Krishnan Padmanabhan (SBN 254220)
kpadmanabhan@winston.com
WINSTON & STRAWN LLP
200 Park Avenue
New York, NY 10166-4193
Telephone: (212) 294-3564
Facsimile: (212) 294-4700

David Enzminger (SBN 137065)
denzminger@winston.com
WINSTON & STRAWN LLP
333 S. Grand Avenue
Los Angeles, CA 90071
Telephone: (213) 615-1700
Facsimile: (213) 615-1750

William M. Logan (*pro hac vice*)
wlogan@winston.com
WINSTON & STRAWN LLP
800 Capitol Street, Suite 2400
Houston, TX 77002
Telephone: (713) 651-2600
Facsimile: (713) 651-2700

Attorneys for Defendant Cisco Systems, Inc.

Terry Ahearn (SBN 216543)
twahearn@duanemorris.com
DUANE MORRIS LLP
260 Homer Avenue, Suite 202
Palo Alto, CA 94301
Telephone: (650) 847-4150
Facsimile: (650) 847-4151

Matthew C. Gaudet (*pro hac vice*)
mcgaudet@duanemorris.com
David C. Dotson (*pro hac vice*)
dcdotson@duanemorris.com
Alice E. Snedeker (*pro hac vice*)
aesnedeker@duanemorris.com
DUANE MORRIS LLP
1075 Peachtree Street NE, Suite 1700
Atlanta, GA 30309
Telephone: (404) 253-6900
Facsimile: (404) 253-6901

Attorneys for Defendant Fortinet, Inc.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

INFOEXPRESS INC., Plaintiff, v. **CISCO SYSTEMS, INC.**, Defendant.	**Case No. 4:23-cv-02698-YGR** **DEFENDANTS CISCO SYSTEMS, INC. AND FORTINET, INC.'S RESPONSIVE CLAIM CONSTRUCTION BRIEF**
INFOEXPRESS INC., Plaintiff, v. **FORTINET, INC.**, Defendant.	**Case No. 4:23-cv-04389-YGR** **DEFENDANTS CISCO SYSTEMS, INC. AND FORTINET, INC.'S RESPONSIVE CLAIM CONSTRUCTION BRIEF**

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 1 of 1144
INFOEXPRESS, INC. - EX2572

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. THE ASSERTED PATENTS 2

III. LEGAL STANDARD 3

IV. ARGUMENT 3

A. InfoExpress has long been on notice of Defendants' indefiniteness arguments, and InfoExpress's waiver arguments are baseless. 3

B. "gatekeeper" ('484 Patent, claims 1–5, 11–13, 15–20, 23–25, 27, 28, 41, 43, 56, 57, 68; '460 Patent, claims 1, 5, 16, 20, 22; '444 Patent, claim 22) 8

C. "access to the restricted subset of the protected network [is / being] responsive to a VLAN configured to communicate with the protected network subject to the access control list" ('484 Patent, claim 56;'460 Patent, claim 30) 14

D. "a wireless access point configured to support an 802.1x standard" ('484 Patent, claim 17) / "an access point configured to use an 802.1x protocol" ('444 Patent, claim 22) 15

E. "audit data" ('350 Patent, claims 1, 6, 8, 9, 10, 13, 18, 19; '460 Patent, claim 1; '444 Patent, claim 22)) 18

F. "audit/auditing" ('484 Patent, claims 1, 13, 39, 42; '350 Patent, claims 1, 6, 8, 9, 10, 13, 18, 19; '450 Patent, claims 16, 22, 23, 25; '444 Patent, claim 22) 18

V. CONCLUSION 23

TABLE OF AUTHORITIES

Page(s)

Cases

Acacia Media Techs. Corp. v. New Destiny Internet Grp.,
405 F. Supp. 2d 1127 (N.D. Cal. 2005) 10, 13

ACQIS LLC v. Samsung Elecs. Co., Ltd.,
No. 2:20-cv-00295-JRG (E.D. Tex. Sept. 26, 2021) 17

Advanced Cardiovascular Sys., Inc. v. SciMed Life Sys., Inc.,
989 F. Supp. 1237 (N.D. Cal. 1997) 7

Apple, Inc. v. Samsung Elecs. Co.,
932 F. Supp. 2d 1076 (N.D. Cal. 2013) 5

BillJCo, LLC v. Cisco Sys., Inc.,
No. 2:21-cv-00181-JRG, ECF No. 68 (E.D. Tex. Jan. 20, 2022) 2, 16, 17

BillJCo, LLC v. Cisco Sys.,
No. 2:21-cv-00183-JRG, 2022 WL 782740 (E.D. Tex. Mar. 14, 2022) 16

Bombardier Recreational Prods. Inc. v. Arctic Cat Inc.,
785 F. App'x 858 (Fed. Cir. 2019) 11

Broadcom Corp. v. Qualcomm Inc.,
543 F.3d 683 (Fed. Cir. 2008) 5

Cap. Sec. Sys., Inc. v. NCR Corp.,
725 F. App'x 952 (Fed. Cir. 2018) 13

Conoco, Inc. v. Energy & Env't Int'l, L.C.,
460 F.3d 1349 (Fed. Cir. 2006) 5

Elec. Scripting Prods., Inc. v. HTC Am. Inc.,
No. 17-CV-05806-RS (RMI), 2021 WL 2530210 (N.D. Cal. June 21, 2021) 7

ePlus, Inc. v. Lawson Software, Inc.,
700 F.3d 509 (Fed. Cir. 2012) 3

Finjan, Inc. v. Proofpoint, Inc.,
No. 13-cv-05808-HSG, 2015 WL 9460295 (N.D. Cal. Dec. 23, 2015) 6

Fundamental Innovation Sys. Int'l LLC v. Samsung Elecs. Co.,
No. 2:17-cv-145-JRG-RSP, 2018 WL 647734 (E.D. Tex. Jan. 31, 2018) 17, 18

Google LLC v. EcoFactor, Inc.,
92 F.4th 1049 (Fed. Cir. 2024) 10

Huawei Techs., Co. v. Samsung Elecs. Co.,
340 F. Supp. 3d 934 (N.D. Cal. 2018) 5

Info-Hold, Inc. v. Applies Media Techs. Corp.,
783 F.3d 1262 (Fed. Cir. 2015) 16

Interval Licensing LLC v. AOL, Inc.,
766 F.3d 1364 (Fed. Cir. 2014) 3

IQASR LLC v. Wendt Corp.,
825 F. App'x 900 (Fed. Cir. 2020) 8, 9, 11, 13

Lazare Kaplan Intern., Inc. v. Photoscribe Techs., Inc.,
628 F.3d 1359 (Fed. Cir. 2010) 5

llumina Inc. v. BGI Genomics Co., Ltd.,
No. 20-CV-01465-WHO, 2020 WL 6891818 (N.D. Cal. Nov. 24, 2020) 6

Mantissa Corp. v. First Fin. Corp.,
No. 2022-1963, 2024 WL 607717 (Fed. Cir. Feb. 14, 2024) 3

Markman v. Westview Instruments, Inc.,
517 U.S. 370 (1996) 3, 5, 10

Nautilus, Inc. v. Biosig Instruments, Inc.,
572 U.S. 898 (2014) 3, 8, 18

NobelBiz, Inc. v. LiveVox, Inc.,
No. 13-CV-1773-YGR, 2015 WL 225223 (N.D. Cal. Jan. 16, 2015) 6

O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.,
521 F.3d 1351 (Fed. Cir. 2008) 3

Oatey Co. v. IPS Corp.,
514 F.3d 1271 (Fed. Cir. 2008) 10

ON24, Inc. v. webinar.net, Inc.,
698 F. Supp. 3d 1154 (N.D. Cal. 2023) 3

Paragon Sols., LLC v. Timex Corp.,
566 F.3d 1075 (Fed. Cir. 2009) 14

Persawvere, Inc. v. Milwaukee Elec. Tool Corp.,
No. C.A. No. 21-400-GBW, 2023 WL 2140033 (D. Del. Feb. 21, 2023) 6

Phillips v. AWH Corp.,
415 F.3d 1303 (Fed. Cir. 2005) 16

Schering Corp. v. Amgen Inc.,
222 F.3d 1347 (Fed. Cir. 2000) 16

Silicon Laboratories, Inc. v. Cresta Technology Corporation,
No. 14-CV-03227-PSG, 2016 WL 791792 (N.D. Cal. Mar. 1, 2016).....6

SuperGuide Corp. v. DirecTV Enters.,
358 F.3d 870 (Fed. Cir. 2004).....15

Takeda Pharm. Co. v. Handa Pharms., LLC,
No. C-11-00840 JCS, 2012 WL 1243109 (N.D. Cal. Apr. 11, 2012) 5

Teva Pharm. USA, Inc. v. Sandoz, Inc.,
574 U.S. 318 (2015).....10

Trs. of Columbia Univ. in City of N.Y. v. Symantec Corp.,
811 F.3d 1359 (Fed. Cir. 2016).....15

Uniloc USA, Inc. v. Apple, Inc.,
Case No. 19-cv-1692, 2021 WL 432183 (N.D. Cal. Jan. 15, 2021).....16

United Carbon Co. v. Binney & Smith Co.,
317 U.S. 228 (1942).....3

Statutes

35 U.S.C. § 112.....3

Other Authorities

https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/ 16

Kenneth Ingham and Stephanie Forrest, A HISTORY AND SURVEY OF NETWORK FIREWALLS (2002).....12

I. INTRODUCTION

There are five terms that the parties propose for construction, and InfoExpress has proposed the plain and ordinary meaning for all five. Defendants offer specific constructions for two of those terms—"audit data" and "audit/auditing"—and challenge two as indefinite: "gatekeeper" and "access to the restricted subset of the protected network [is / being] responsive to a VLAN configured to communicate with the protected network subject to the access control list." For the final dispute—"a wireless access point configured to support an 802.1x standard"—Defendants seek to clarify that this refers to the 802.1x protocol as it existed on or before September 24, 2003, and contend that InfoExpress's contrary plain-and-ordinary-meaning position would render the term indefinite. For the reasons demonstrated below, the Court should find in favor of Defendants for each of these constructions.

In its opening claim construction brief, InfoExpress raised concerns for the first time that Defendants did not timely disclose their indefiniteness positions. That assertion is unfounded. For the past five months, InfoExpress has been fully aware of Defendants' indefiniteness positions. During this period, the parties engaged in numerous discussions where these issues were thoroughly addressed, including multiple email exchanges and at least two video conferences. At no point during these interactions did InfoExpress express any confusion regarding Defendants' positions.

Contrary to InfoExpress's assertions, they received all the evidence supporting Defendants' indefiniteness challenges. This includes Dr. Narasimha Reddy's expert declaration, which provided detailed opinions supporting Defendants' positions. And yet, despite having the opportunity, InfoExpress chose not to depose Dr. Reddy. This strategy by InfoExpress appears to be a deliberate attempt to sidestep the merits of the indefiniteness arguments. By feigning surprise and failing to fully engage with the evidence and expert testimony, InfoExpress is attempting to undermine the substance of Defendants' indefiniteness challenges without addressing the core issues those challenges raise. The Court should disregard InfoExpress's transparent attempts to avoid engaging substantively with the arguments advanced by Defendants, and instead consider the merits of those arguments that conclusively demonstrate the indefiniteness of those terms.

II. THE ASSERTED PATENTS

InfoExpress asserts U.S. Patent Nos. 7,523,484 (the "'484 Patent") (ECF No. 109-2)[1]; 8,051,460 (the "'460 Patent") (ECF No. 1-2); 8,677,450 (the "'450 Patent") (ECF No. 1-3); 8,578,444 (the "'444 Patent") (ECF No. 1-4); and 8,347,350 (the "'350 Patent") (ECF No. 1-5) (collectively, the "Asserted Patents"). The Asserted Patents claim priority to Provisional Application Nos. 60/513,080 (filed on October 21, 2003) and 60/505,582 (filed on September 24, 2003). They are directed to network security and seek to limit authorized users' access to a network by ensuring that access devices connecting to the network comply with security policies to protect the network from viruses and other "malicious computing code." ECF No. 109-2 at 1:19–20, 23–27, 53–63. To accomplish this goal, the Asserted Patents utilize a "gatekeeper" to manage network security by ensuring "that [an] Access Device 160 conforms to a predetermined security policy," (e.g., virus software and encryption protocols) before granting access to the network. *Id.* at 2:17–22. In the prior art, after "gatekeeper" determines that an access device conforms to a security policy, the access device may connect to the network by communicating through the "gatekeeper." *Id.* at 2:22–25. The Asserted Patents claim that prior art "gatekeepers" were problematic because every instance of an access device connecting to a network would pass through a "gatekeeper," burdening the bandwidth of the network. *Id.* at 2:31–39.

The Asserted Patents purportedly improve on the prior art by not requiring that each access device be assigned an individual "gatekeeper" to gain access to the network. *Id.* at 2:59–61. Rather, they logically divide a protected network into a restricted subset and one or more less-restricted subsets. *Id.* at 2:48–50. An access device initially requests access to the network via "gatekeeper," which sits in a "restricted subset" of the network (i.e., the portion of the network with more restrictions, like a quarantine). After "gatekeeper" determines that the access device satisfies a security policy, *id.* at 2:52–54, "gatekeeper" grants the access device access to the less-restricted subset by configuring or reconfiguring the communication port of the access device (i.e., authorizing the access device to leave quarantine). *Id.* at 2:54–59.

[1] This brief is the same in both the *Cisco* and *Fortinet* matters, and the ECF citations herein are to the docket in the *Cisco* matter (Case No. 4:23-cv-02698).

III. LEGAL STANDARD

Claim construction is an issue of law for the Court to decide. *Markman v. Westview Instruments, Inc.*, 517 U.S. 370, 390–91 (1996). "When the parties present a fundamental dispute regarding the scope of a claim term, it is the court's duty to resolve it." *O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1362 (Fed. Cir. 2008). Under 35 U.S.C. § 112, "a patent must be precise enough to afford clear notice of what is claimed, thereby 'appris[ing] the public of what is still open to them' . . . in a manner that avoids '[a] zone of uncertainty which enterprise and experimentation may enter only at the risk of infringement claims[.]'" *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 909 (2014) (quoting *Markman*, 517 U.S. at 373; *United Carbon Co. v. Binney & Smith Co.*, 317 U.S. 228, 236 (1942)); *see also Mantissa Corp. v. First Fin. Corp.*, No. 2022-1963, 2024 WL 607717, at *4 (Fed. Cir. Feb. 14, 2024). A claim term is indefinite when, considering the intrinsic record, it fails to "inform those skilled in the art about the scope of the invention with reasonable certainty." *Nautilus*, 572 U.S. at 910. A claim term's indefiniteness renders the claim invalid. *Id.* at 901. "[I]ndefiniteness is a question of law and in effect part of claim construction." *ON24, Inc. v. webinar.net, Inc.*, 698 F. Supp. 3d 1154, 1161 (N.D. Cal. 2023) (quoting *ePlus, Inc. v. Lawson Software, Inc.*, 700 F.3d 509, 517 (Fed. Cir. 2012)). "The claims, when read in light of the specification and the prosecution history, must provide objective boundaries for those of skill in the art." *Interval Licensing LLC v. AOL, Inc.*, 766 F.3d 1364, 1371 (Fed. Cir. 2014) (citations omitted).

IV. ARGUMENT

A. InfoExpress has long been on notice of Defendants' indefiniteness arguments, and InfoExpress's waiver arguments are baseless.

InfoExpress first indicated that it believed Defendants' indefiniteness arguments were untimely or waived in its opening claim construction brief. ECF No. 109 at 6. This allegation comes as a total surprise to Defendants because InfoExpress has long been on notice of Defendants' indefiniteness positions, and the parties extensively met and conferred on claim construction issues, as required by the Court's Local Rules. InfoExpress's attempt at raising a waiver argument in the eleventh hour is nothing more than litigation by surprise and should not be entertained. InfoExpress's Opening Brief identifies five terms for which indefiniteness is supposedly waived (Op. Br. at 8), but that dispute is only live with respect to the

term "gatekeeper" and "access to the restricted subset of the protected network [is/being] responsive to a VLAN configured to communicate with the protected network subject to an access control list."[2]

Some relevant facts are indisputable.

On March 25, 2024—nearly five months ago—Defendants served InfoExpress with notice of the terms they contended should be found indefinite through the claim construction process. Exs. A; B at 4. The parties met-and-conferred on Defendants' proposed constructions by video conference at least twice, on April 17, 2024, and May 1, 2024. Exs. C, D. During those sessions, Defendants explained in detail their indefiniteness positions to InfoExpress, and InfoExpress confirmed that it disagreed with Defendants' position. Logan Decl. ¶ 1. But InfoExpress never stated (or even suggested) during those conferences that it did not understand the bases for Defendants' indefiniteness positions, nor did it ever suggest that it believed those positions were inadequately disclosed. *Id.* ¶ 2. Following these conferences, the parties exchanged several emails concerning various claim construction disputes, but InfoExpress never expressed any confusion about Defendants' positions in those emails. Exs. E–H. The parties also extended the claim construction schedule numerous times, during which, if InfoExpress truly believed that it was prejudiced, it could have simply flagged the issue, or sought any discovery that it wanted on Defendants' indefiniteness positions. ECF No. 81 (extending claim construction deadlines by two weeks); ECF No. 97 (extending claim construction deadlines by five weeks); ECF No. 104 (extending claim construction deadlines by two weeks); ECF No. 106 (extending claim construction deadlines by one week); ECF No. 108 (extending claim construction deadlines by one week); Exs. E–H – (parties' email correspondence agreeing to several claim construction schedule extensions).

On June 28, 2024—nearly two months before InfoExpress's opening claim construction brief, and consistent with the parties' agreed upon schedule—Defendants served a declaration from Dr. Reddy providing expert opinions explaining that a person of ordinary skill in the art ("POSITA") would not understand the meaning of the terms it had identified as indefinite with any reasonable certainty. Ex. F at 8–9; Ex. L at 10. On that same day, InfoExpress served a declaration from its own expert, Dr. Aaron

[2] The parties have resolved their dispute for "policy auditor" and "the protected network." For the claim terms that contain "802.1x," Defendants' proposed a construction, and have contended that InfoExpress's "plain meaning" would render the claim term indefinite. Accordingly, the only terms for which the waiver dispute plausibly remains is "gatekeeper" and "access to the restricted subset of the protected network [is/being] responsive to a VLAN configured to communicate with the protected network subject to an access control list."

Striegel, that addressed Defendants' indefiniteness positions, including a combined 42 paragraphs supporting his opinion that "gatekeeper" and "access to the restricted subset of the protected network [is/being] responsive to a VLAN configured to communicate with the protected network subject to an access control list" are sufficiently definite (ECF No. 109-36 ¶¶ 50–84, 108-116), . That opinion analyzed the specification, claims, prosecution history, and prior art, and confirmed that Dr. Striegel and InfoExpress understood the parties' dispute. It is therefore difficult to reconcile Defendants' history of disclosure here with InfoExpress's assertion that Defendants "never suppl[ied] any reasoning, basis, or rationale" for their indefiniteness challenges, ECF No. 109 at 1; that "[t]o date, Defendants have not shared their rationale for why these terms might be indefinite," *id.* at 8; and that "it is not clear why Defendants believe these terms are indefinite," *id.* As demonstrated above, those statements are simply wrong.

InfoExpress's position is contrary to Federal Circuit precedent. As the Federal Circuit has "repeatedly explained, 'litigants waive their right to present new claim construction disputes if they are waived for the first time after trial.'" *Lazare Kaplan Intern., Inc. v. Photoscribe Techs., Inc.*, 628 F.3d 1359, 1376 (Fed. Cir. 2010) (quoting *Broadcom Corp. v. Qualcomm Inc.*, 543 F.3d 683, 694 (Fed. Cir. 2008); *Conoco, Inc. v. Energy & Env't Int'l, L.C.*, 460 F.3d 1349, 1359 (Fed. Cir. 2006) ("[A] district court may engage in claim construction during various phases of litigation, not just in a *Markman* order. We have recognized that district courts may engage in rolling claim construction, in which the court revisits and alters its interpretation of the claim terms as its understanding of the technology evolves."). This District is in accord with the Federal Circuit and has held that raising indefiniteness for the first time at claim construction does not constitute waiver—"[F]ailure to seek construction of a term during claim construction does not constitute waiver of an indefiniteness argument." *Apple, Inc. v. Samsung Elecs. Co.*, 932 F. Supp. 2d 1076, 1079 (N.D. Cal. 2013); *id.* at 1084 (concluding that the plaintiff was on notice of the defendant's indefiniteness challenge even though the defendant did not propose the disputed term for construction when indefiniteness was raised in the defendant's answer, invalidity contentions, summary judgment briefing, and trial); *Huawei Techs., Co. v. Samsung Elecs. Co.*, 340 F. Supp. 3d 934, 997–98 (N.D. Cal. 2018) (deciding that the plaintiff was not prejudiced and that the defendant did not waive its indefiniteness challenge even though indefiniteness was not asserted at claim construction); *Takeda Pharm. Co. v. Handa Pharms., LLC*, No. C-11-00840 JCS, 2012 WL 1243109, at *16 (N.D. Cal.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 10 of 1144
INFOEXPRESS, INC. - EX2572

Apr. 11, 2012) ("Due to the largely factual nature of [the indefiniteness] inquiry, the [c]ourt concludes that th[e] question is more suitable for determination on summary judgment than at the claim construction phase of the case."). Indeed, in a factually similar case, a court held that the defendant did not waive its indefiniteness argument when it was first disclosed in the joint claim construction chart, rejecting a similar argument raised by InfoExpress. *See, e.g.*, *Persawvere, Inc. v. Milwaukee Elec. Tool Corp.*, No. C.A. No. 21-400-GBW, 2023 WL 2140033, at *6 n.5 (D. Del. Feb. 21, 2023) (determining that the defendant did not waive its indefiniteness argument when the argument was not raised in its invalidity contentions but raised in the joint claim construction chart). But here, Defendants disclosed their indefiniteness positions more than one month before the parties filed their joint claim construction statement. *Compare* Exs. A; B at 4 (disclosure of Cisco's preliminary claim constructions and evidence on March 25, 2024), *with* ECF No. 89-1 at 9 (joint claim construction statement filed on May 3, 2024). And now, InfoExpress has been on notice of Defendant's indefiniteness positions for nearly five months.

Furter, none of InfoExpress's cited cases found exclusion appropriate in light of such detailed disclosure as was provided by Defendants here. In *llumina Inc. v. BGI Genomics Co., Ltd.*, for instance, there was one potential disclosure during a single meet-and-confer. No. 20-CV-01465-WHO, 2020 WL 6891818, at *8 (N.D. Cal. Nov. 24, 2020). Likewise, *NobelBiz, Inc. v. LiveVox, Inc.*, considered a situation where the disclosures that were made "strongly suggests that defendants viewed the whole of [a] longer phrase indefinite," instead of the specific phrase that the defendants advanced in their claim-construction brief. No. 13-CV-1773-YGR, 2015 WL 225223, at *9 (N.D. Cal. Jan. 16, 2015). Even in *Silicon Laboratories, Inc. v. Cresta Technology Corporation*, the indefiniteness challenges that the defendant raised were later abandoned when constructions were proposed in the joint claim construction statement. No. 14-CV-03227-PSG, 2016 WL 791792, at *3 (N.D. Cal. Mar. 1, 2016). Finally, in *Finjan, Inc. v. Proofpoint, Inc.*, defendants raised indefiniteness challenges for the first time in their expert report ***after*** claim construction. No. 13-cv-05808-HSG, 2015 WL 9460295, at *3 (N.D. Cal. Dec. 23, 2015).

Here, InfoExpress has been on notice of Defendants' contention that these exact terms are indefinite for at least five months (Exs. A; B at 4); has conferred with Defendants about these terms on multiple occasions (Exs. C–I; Logan Decl. ¶ 1); and received an expert declaration from Defendants' expert well before the opening claim-construction brief (Ex. L ¶¶ 34–40). InfoExpress even declined to

depose Dr. Reddy (Ex. F at 6), presumably because it had a sufficient understanding of Defendants' indefiniteness positions. InfoExpress cites no relevant authority finding waiver is appropriate in the face of such clear and substantial notice.

InfoExpress is wrong that the Court should penalize Defendants for not moving for leave to supplement their invalidity contentions to include these indefiniteness challenges. Except for claim construction, this case has been stayed for more than two months, *see* ECF No. 101, so Defendants cannot currently file a motion for leave.[3] But if the Court were to allow Defendants to file such a motion, there would be good cause. For example, Defendants told InfoExpress in their invalidity contentions that additional indefiniteness positions might be disclosed as facts developed during claim construction. Ex. M at 2, 5. Defendants' indefiniteness position on "gatekeeper" is just such a situation. Initially, the parties agreed that various "gatekeeper" limitations required construction, Exs. N at 4; O at 4–6, which suggested a common understanding that those terms have no plain and ordinary meaning and would need to be construed. InfoExpress presented various "gatekeeper" terms requiring constructions through a first two sets of amended lists of claim terms for construction, Exs. O at 4–6; P at 4–6; Q at 4; R at 3, before ultimately changing its position in contending that those terms had a plain and ordinary meaning, Ex. S at 6, 14, 28). To evaluate InfoExpress's position, Defendants sought the opinion of Dr. Reddy, who concluded that "gatekeeper" could not be construed because a POSITA would not have understood it with reasonable certainty. Ex. L ¶¶ 34–40. Defendants promptly notified InfoExpress of that position, Ex. F at 8–9, and provided a declaration from Dr. Reddy, Ex. L at 10. Likewise, Defendants have proposed a construction for the 802.1X terms and have only raised indefiniteness based on InfoExpress's counter position. Given those disclosures, InfoExpress suffered no plausible prejudice, and leave to amend the invalidity contentions would have been warranted (were the case not stayed). *See Elec. Scripting Prods., Inc. v. HTC Am. Inc.*, No. 17-CV-05806-RS (RMI), 2021 WL 2530210, at *3 (N.D. Cal. June 21, 2021) (finding amendment appropriate and no prejudice when "[Plaintiff] already knew of the facts and legal theory underlying [Defendant's proposed amendment to its invalidity contentions]" (quoting *Advanced Cardiovascular Sys., Inc. v. SciMed Life Sys., Inc.*, 989 F. Supp. 1237, 1247 (N.D. Cal. 1997))).

[3] If Defendants should have moved to amend their contentions, InfoExpress should have similarly moved to strike the allegedly untimely positions, which would have required it to confer with Defendants and address the relevant factors, including prejudice. Tellingly, InfoExpress filed no such motion.

InfoExpress's waiver argument is of no moment, and the Court should not give it any consideration.

B. "gatekeeper" ('484 Patent, claims 1–5, 11–13, 15–20, 23–25, 27, 28, 41, 43, 56, 57, 68; '460 Patent, claims 1, 5, 16, 20, 22; '444 Patent, claim 22)

Defendants' Construction	Plaintiff's Construction
Indefinite	Plain and ordinary meaning; no construction necessary

The term "gatekeeper" has no ordinary and customary meaning. Ex. L ¶ 34. When a claim term has no ordinary and customary meaning in the art, its definiteness turns on "whether the intrinsic evidence provides objective boundaries." *IQASR LLC v. Wendt Corp.*, 825 F. App'x 900, 904 (Fed. Cir. 2020) (citation omitted). Here, neither the claims nor the specification provides any such objective boundaries for determining what constitutes a "gatekeeper." Ex. L ¶ 35. Instead, the patent suggests that "gatekeeper" is not defined by the type of hardware, by its functions, or where it resides in the network. Instead, the specification indicates that a "gatekeeper" can be implemented in any number of (and contradictory) ways, without any objective boundaries regarding what does, and does not, constitute a "gatekeeper." Accordingly, the claims—read in light of the specification and prosecution history—fail to inform, with reasonable certainty, a POSITA about the scope of "gatekeeper." *See Nautilus*, 572 U.S. at 901.

The Asserted Patents do not clearly define what a "gatekeeper" is. The Asserted Patents refer to a wide variety of examples that "gatekeeper" ***may be*** or components that "gatekeeper" ***may have***, but these examples are insufficient to inform a POSITA about the scope of "gatekeeper" with reasonable certainty. Ex. L ¶ 35. First, the intrinsic record shows that "gatekeeper" ***may be*** multiple firewalls. Ex. L ¶ 35. For example, in the background of the Asserted Patents, "gatekeeper" is located between the secure network and the access device. *See* ECF No. 109-2 at 1:53–55. Thus, at least based on this disclosure, a separate "gatekeeper" is used for each instance of an access device or access point. *See* ECF No. 109-2 at 2:37–39. Put another way, the concept of a "gatekeeper" appears to at least encompass an array of firewalls for a plurality of access points.

Second, "gatekeeper" ***may also*** include the functionality of a network switch, a software-defined network router, and/or a generic authentication device. Ex. L ¶ 38. For example, a network switch "is programmed to grant access to a secure network only after proper authentication is achieved." ECF No.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 13 of 1144
INFOEXPRESS, INC. - EX2572

109-2 at 1:31–40; *id.* at 2:62–3:4 ("[T]he less-restricted subset of the protected network and the restricted subset of the protected network are characterized by [VLANs] defined within the access point and optionally by access control lists (ACL) of a router, firewall, or switch situated between the VLAN and the protected network."). But "gatekeeper" is similarly programmed to regulate access based on an access device's compliance with a security policy—"GateKeeper 110 is configured to control access to Secure Network 100. In addition to authenticating users who wish to access Secure Network 100 using an Access Device 160, GateKeeper 110 is configured to ensure that Access Device 160 conforms to a predetermined security policy, before granting access to Secure Network 100." *Id.* at 2:14–19.

Third, "gatekeeper" ***may also be*** a generic "single computing device" or a "server." *Compare id.* at 6:14–16 ("[A] single computing device [is] configured to function as both Update Module 255 and GateKeeper 225."); *with id.* at 6:11–14 ("Restricted Subset 205 includes a server configured to function as DHCP 260 and a server configured to function as GateKeeper 225.").

Fourth, "gatekeeper" ***may also*** partially include an access point—which is the very device a "gatekeeper" could supposedly reconfigure to admit or restrict an access device from the network. *Id.* at 15:32–34 ("In some embodiments, ***various aspects of GateKeeper 225 may be incorporated into Access Point 215*** and/or Router 220.") (emphasis added).

Fifth, "gatekeeper" ***may also*** store security policies, which may be stored in several other locations within the restricted subset, including on the policy manager. *Id.* at 6:59–61 ("Security policies may be stored on GateKeeper **225**, on Policy Manager **250**, or elsewhere accessible to Restricted Subset **205**.").

In sum, although the specification lists numerous components that could possibly be part of "gatekeeper," none of these components are limiting examples of what "gatekeeper" must include. But "[n]on-limiting examples do not on their own expressly define the bounds—the limits—of the claim." *IQASR*, 825 F. App'x at 906 (citation omitted). Even the figures provided by the Asserted Patents fail to provide limiting examples. For instance, Figures 3A and 3B depict "gatekeeper" as a block, which contains four sub-blocks: "Security Policy 330A," "Security Policy 330B," "Policy Auditor," and "Access Control." ECF No. 109-2 at Figs. 3A, 3B. Notably, "policy auditor" and "access control" are themselves abstract concepts that describe what "gatekeeper" should do ***but not what it is***. *Id.* at 9:31–38, 9:40–43, 11:31–33, 11:39–42, 11:56–59 (describing only what "policy auditor" does); *id.* at 9:20–25, 9:38–40,

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 14 of 1144
INFOEXPRESS, INC. - EX2572

9:43–45, 10:45–47, 10:55–57, 12:33–35, 12:53–56, 13:3–6 (describing only what "access control" does); s*ee Acacia Media Techs. Corp. v. New Destiny Internet Grp.*, 405 F. Supp. 2d 1127, 1140 (N.D. Cal. 2005) ("Claiming an apparatus using only a block diagram with functional description is indefinite when the patentee names the device using a coined term and the various functions could be performed by an indefinite variety of devices."). The intrinsic record therefore fails to limit the objective boundaries of the "gatekeeper" to specific components.

Curiously, the testimony of InfoExpress's expert only amplifies the confusion. When asked if an access point could be a "gatekeeper," Dr. Striegel answered, "in the invented gatekeeper, an access point would not be a gatekeeper." Ex. T at 87:12–15. However, this opinion directly contradicts the specification, which provides that "[i]n some embodiments, various aspects of GateKeeper 225 may be incorporated into Access Point 215 and/or Router 220." ECF No. 109-2 at 15:32–34. Of course, Dr. Striegel's opinion that a "gatekeeper" must exclude the "access point" is incorrect as a matter of law because it excludes an embodiment: "We normally do not interpret claim terms in a way that excludes embodiments disclosed in the specification." *Google LLC v. EcoFactor, Inc.*, 92 F.4th 1049, 1058 (Fed. Cir. 2024) (quoting *Oatey Co. v. IPS Corp.*, 514 F.3d 1271, 1276 (Fed. Cir. 2008)). Accordingly, Dr. Striegel's opinions regarding the definiteness of "gatekeeper" should be given little weight. *Teva Pharm. USA, Inc. v. Sandoz, Inc.*, 574 U.S. 318, 326–27 (2015) ("[I]n patent construction, subsidiary factfinding is sometimes necessary . . . [S]ometimes courts may have to make 'credibility judgments' about witnesses . . . [and] may have to resolve subsidiary factual disputes." (quoting *Markman*, 517 U.S. at 389)).

The Asserted Patents do not clearly define how "gatekeeper" works. InfoExpress's expert, Dr. Striegel, does not offer a definition for "gatekeeper" that provides objective boundaries. Instead, he opines that "gatekeeper" (1) "could refer to a device that would assist in determining whether an endpoint (that is, an 'Access Device') complied with a security policy, before granting that endpoint access to network resources"; (2) "can gather information to assess the Access Device's compliance with a security policy. However, it is not limited to only performing these functions"; and (3) "had the ability to . . . request audit information . . . communicate with the server filter . . . [and] return a failure response." ECF No. 109-36 ¶¶ 51, 60–62. Dr. Striegel's descriptions provide no objective boundaries concerning how "gatekeeper" works, but rather, he merely restates the functions "gatekeeper" ***could perform***—this cannot

save "gatekeeper" from indefiniteness. *See Bombardier Recreational Prods. Inc. v. Arctic Cat Inc.*, 785 F. App'x 858, 867 (Fed. Cir. 2019) (even "if a claim term's definition can be reduced to words, the claim is still indefinite if a [POSITA] cannot translate the definition into meaningfully precise claim scope") (citation omitted)); *IQASR*, 825 F. App'x at 907 ("A claim term does not become reasonably certain simply because a skilled artisan, when pressed, managed to articulate a definition for it.").

Does a device that "would assist in determining whether an endpoint complied with a security policy" constitute the claimed "gatekeeper?" Ex. T at 59:14–21, 64:16–22. The answer to that question is uncertain even to InfoExpress's expert—when asked whether this exemplary functionality defined a "gatekeeper," Dr. Striegel could only answer that a POSITA would understand what "gatekeeper" is by reading the specification and the claims. *Id.* at 59:23–66:19. In addition, Dr. Striegel testified that "[the gatekeeper] would need to be able to obtain . . . th[e] audit data . . . and then apply[] an appropriate security policy as being one of the embodiments that's present in the respective inventions." *Id.* at 80:20–81:4. When asked more specifically whether "gatekeeper" must include a "policy auditor," Dr. Striegel testified that it "would depend upon the security policies that would be in play with regard[] to the device and the type of access . . . ." *Id.* at 76:9–12. Yet, the Asserted Patents show that "policy auditor" is the only auditing component within "gatekeeper." *See* ECF No. 109-2 at Figs. 3A, 3B. Each of these contradictions and inconsistencies, caused by the open-endedness and imprecision of the claim language, demonstrates that "gatekeeper" is indefinite and fails to provide any objective boundaries to a POSITA. *IQASR*, 825 F. App'x at 904.

InfoExpress responds that "gatekeeper" is subject to its plain and ordinary meaning because extrinsic evidence provides "examples of 'gatekeeper' in the technological field from the time of the invention." ECF No. 109 at 15. But setting aside that these "examples" provide no objective boundary for the term, the extrinsic references cited by InfoExpress each recite the concept of an "in-line "gatekeeper," whereas InfoExpress explicitly distinguishes such "in-line" configuration from the "out-of-band" "gatekeeper" claimed by the Asserted Patents. *Compare* ECF No. 109 at 16 ("***By 'in-line'*** it is meant that all traffic 30 must pass through the entrance sentry 42 before entering the protected network 14." (quoting U.S. Patent No. 7,359,962 at 6:27–29 (LeMair) (emphasis added)); *and id.* at 16 ("If the traffic was [sic] allowed, gatekeeper then sent the traffic on to the destination machine. No traffic was

allowed to pass directly from the local machine to the remote machine." (quoting Kenneth Ingham and Stephanie Forrest, A HISTORY AND SURVEY OF NETWORK FIREWALLS at 10 (2002))); *with id.* at 3 ("While the ***in-line configuration*** ensured a degree of security, it had its own disadvantages: cost, efficiency, unworkability. Indeed, such a configuration required a gatekeeper with each instance of an access point, which would be quite costly. As to efficiency, the ***in-line gatekeeper*** was a bottleneck on communications between the endpoint and the network." (emphasis added)); *and id.* at 3 ("The Asserted Patents solved these problems with a novel and non-obvious approach that relieved computer resources . . . [which] used an ***out-of-band*** gatekeeper (located in the more restricted subset)." (emphasis in original)). According to InfoExpress, after the "out-of-band" "gatekeeper" grants access to an access device, further data no longer passes through the "out-of-band gatekeeper." *Id.* at 4 ("By configuring the access point in response to approval of the device by the gatekeeper, network traffic for previously approved devices passes to the less-restricted subset without passing through and being evaluated by the gatekeeper.").

InfoExpress therefore fails to explain how a POSITA would understand the claimed "out-of-band gatekeeper" to work with any reasonable certainty, particularly because the claimed "gatekeeper" may step aside and stop its gatekeeping function—a fundamental ***difference*** from prior art "in-line gatekeepers." Indeed, prior art gatekeepers cannot tell us what the term means in the recited claims because the entire purpose of the invention is to distinguish how the claimed "gatekeeper" operates over those prior art gatekeepers. Ultimately, InfoExpress cannot reconcile the two self-contradictory positions—that the claimed "out-of-band gatekeeper" is novel and different from prior art "in-line gatekeepers" while arguing that the "out-of-band gatekeeper" borrows the plain and ordinary meaning of prior art from "in-line gatekeepers." The only logical conclusion is that the claimed "gatekeeper" is a unique aspect of the purported invention that requires a ***specific definition*** (i.e., there is no plain meaning), which the specification fails to provide.

The Asserted Patents do not clearly define where "gatekeeper" is located. Critically, the amorphous nature of "gatekeeper's" components results in contradictory disclosures of where it should be in the claimed invention. For example, the specification provides a first location where "gatekeeper" is ***between*** the secure network and the access device. ECF No. 109-2 at 1:53–55. The specification provides a second location where the "gatekeeper" ***resides on*** the restricted subset of the network, defined by

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 17 of 1144
INFOEXPRESS, INC. - EX2572

VLANs, and "gatekeeper" is supposed to "send[] commands to the access point" that resides at a different location, i.e., the less-restricted subset of the network. *See, e.g., id.* at 4:10–24, 5:42–45, Fig. 2. At this second location, "gatekeeper" is not strictly between the secure network and access device in the sense that once access is granted, further data can bypass "gatekeeper" and go directly to the protected network. *Id.* at Fig. 2, 10:3–8 ("Once Port 305A has been reconfigured to be associated with VLAN 310A, future general network traffic between Access Device 230 and Less-Restricted Subset 210 may pass through Ports 305A, 305D and 335A without passing through GateKeeper 225 or other elements of Restricted Subset 205."). The specification provides a third location where "gatekeeper" may be partially incorporated as part of an access point while also partially residing somewhere else, i.e., within the restricted subset. *Id.* at 15:32–34 ("In some embodiments, various aspects of GateKeeper 225 may be incorporated into Access Point 215 and/or Router 220."). The specification therefore causes confusion regarding the specific location or function of "gatekeeper."

"Gatekeeper" is indefinite. As demonstrated above, "gatekeeper" is indefinite because the intrinsic record provides no objective indicia by which to determine what does, and does not, qualify as a "gatekeeper." Courts have repeatedly found terms indefinite in similar circumstances. *IQASR*, 825 F. App'x at 904 (finding the term "magnetic fuzz" indefinite where the patent neither defines nor provides enough explanation that an artisan may infer reasonably certain, objective boundaries of the term); *Cap. Sec. Sys., Inc. v. NCR Corp.*, 725 F. App'x 952, 958–59 (Fed. Cir. 2018) (finding the term "transactional operator" indefinite because there is no "rationale supporting the seemingly arbitrary definition of 'transactional operator' as a microprocessor and keyboard, while excluding the associated display and keypads"); *Acacia Media Techs. Corp. v. New Destiny Internet Grp.*, 405 F. Supp. 2d 1127, 1139–41 (N.D. Cal. 2005) (holding that a POSITA would not understand the scope or bounds of the structure of the term "identification encoder" when that term is read in light of the specification, rendering the claim term "identification encoder" indefinite). Here, the specification provides no guidance regarding what a "gatekeeper" is, what a "gatekeeper" does, or where a "gatekeeper" is located. Accordingly, "gatekeeper" should be found indefinite for at least this reason.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 18 of 1144
INFOEXPRESS, INC. - EX2572

C. "access to the restricted subset of the protected network [is / being] responsive to a VLAN configured to communicate with the protected network subject to the access control list" ('484 Patent, claim 56;'460 Patent, claim 30)

Defendants' Construction	Plaintiff's Construction
Indefinite	Plain and ordinary meaning; no construction necessary

The Asserted Patents fail to inform a POSITA with reasonable certainty what it means for "access" to be "responsive to" a VLAN (which stands for virtual local area network) or how access could be "responsive to" a VLAN. Ex. L ¶ 51. In certain parts of the specification, the term "responsive to" aligns with its plain and ordinary meaning, namely, taking an action after receiving a request or a command. Ex. L ¶¶ 52, 53. For instance, the specification describes "a gatekeeper, applying a security policy to the access device, responsive to the request and reconfiguring the communication port for communicating between the access device and the less-restricted subset of the protected network, if requirements of the security policy are satisfied." ECF No. 109-2 at 4:17–23. Here, "responsive to" indicates that "gatekeeper's" action of "applying a security policy" is a direct response to an action—i.e., the access request sent from the access device. *Id.* at 4:10–19; Ex. L ¶ 52. Also, the specification states that "configuration of the communication port including association of the communication port alternatively with the first VLAN or the second VLAN, configuration of the communication port being responsive to the commands issued by the gatekeeper" and "means for allowing communication to the less-restricted subset, responsive to the enforcement of the security policy." ECF No. 109-2 at 3:55–59, 4:50–51. In this example, "responsive to" signifies that the adjustments to the communication port are made following another action—i.e., commands from "gatekeeper." In stark contrast, this claim language requires being "responsive to" a ***thing*** (i.e., a VLAN) instead of an ***action***, which is nonsensical.

The plain and ordinary meaning of "responsive to" in the context of the term "access to the restricted subset . . . responsive to a VLAN" is not reasonably certain. The same terms appearing in different parts of a patent are presumed to have the same meaning, "unless it is clear from the specification and prosecution history that the terms have different meanings at different portions of the claims." *Paragon Sols., LLC v. Timex Corp.*, 566 F.3d 1075, 1087 (Fed. Cir. 2009). In this context, the plain and ordinary meaning cannot apply because "access" would not be described as being "responsive to" a

VLAN, and the specification lacks any explanation as to how "access" would be "responsive to" a thing (i.e., a VLAN). Further there is no explanation as to how a VLAN would, for example, function in a manner such that "access" would be "responsive to" it. Thus, the term "access to the restricted subset . . . responsive to a VLAN" must be found indefinite because it does not identify any request or command (i.e., some action) that would be "responsive to a VLAN." Ex. L ¶ 53. Any attempt by InfoExpress to impute the plain and ordinary meaning of "responsive to" to this term is nonsensical and nothing more than an apples to oranges comparison. *See, e.g., Trs. of Columbia Univ. in City of N.Y. v. Symantec Corp.*, 811 F.3d 1359, 1367 (Fed. Cir. 2016) ("The claims are nonsensical in the way a claim to extracting orange juice from apples would be, and are thus indefinite.").

InfoExpress's attempts to show the contrary fail because InfoExpress merely recites portions of the Asserted Patents that do not show any request or command that would cause a response to a VLAN. ECF No. 109 at 22–23. InfoExpress repeats two portions of the Asserted Patents—(1) "***Ports 305A-305C are associated with VLAN***," and (2) "***These communication ports are configured to be associated with VLAN*** 310C such that any data (e.g., communications) they receive from external devices are directed to Port 305F and, thus, to subject to ACL 340C." *Id.* (quoting ECF No. 109-2 at 8:51–63, 10:55–61, 11:1–9 (emphasis added)). However, these quotes refer to what a VLAN is associated with and not what is "responsive to" a VLAN. InfoExpress attempts to rewrite its specification and claim language, arguing that "access to the ***less*** restricted subset of the network is determined by a VLAN," ECF No. 109 at 23 (emphasis in original), but InfoExpress simply cites additional portions of the specification that discuss a VLAN's association, not its operation or functionality. *SuperGuide Corp. v. DirecTV Enters.*, 358 F.3d 870, 875 (Fed. Cir. 2004) ("The written description, however, is not a substitute for, nor can it be used to rewrite, the chosen claim language. Specifications teach. Claims claim." (citation omitted)).

D. "a wireless access point configured to support an 802.1x standard" ('484 Patent, claim 17) / "an access point configured to use an 802.1x protocol" ('444 Patent, claim 22)

Defendants' Construction	Plaintiff's Construction
"802.1x protocol as it existed on or before September 24, 2003"; Otherwise, indefinite	Plain and ordinary meaning; no construction necessary

The specification contemplates "the ***existing*** 802.1x protocol implementation" at the time of the purported invention. ECF No. 109-2 at 13:1–3 (emphasis added); *see also* U.S. Provisional Application No. 60/513,080 (Ex. U) at 4 ("Existing System 1c: 802.1x"); *id.* at 6 ("The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol."). Consistent with the specification, Defendants' proposed construction seeks to give the terms "802.1x standard" and "802.1x protocol" their "ordinary and customary meaning as understood by a person of ordinary skill in the art at the time of the invention." *Info-Hold, Inc. v. Applies Media Techs. Corp.*, 783 F.3d 1262, 1265 (Fed. Cir. 2015) (citing *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005)). Divorced from the specification, the terms "802.1x standard" and "802.1x protocol" embrace an evolving communications technology that include "a variety of enhancements that would not have been known, let alone predicted, by a POSITA at the time of the alleged priority date." Ex. L ¶ 45 (citing Ex. 5 of Dr. Reddy's Decl. (https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/)). The terms "802.1x standard" and "802.1x protocol" must therefore be limited to what they meant at the time of the alleged priority date—to find otherwise would improperly "enlarge the scope of the patent to embrace technology arising after its filing." *See Schering Corp. v. Amgen Inc.*, 222 F.3d 1347, 1352–54 (Fed. Cir. 2000). And limiting those terms in this way—to reflect the issued standards that existed at the time of the invention—has been a consistent practice of the courts, particularly where, as here, evolving communication standard technology is at issue. *See, e.g., BillJCo, LLC v. Cisco Sys.,* No. 2:21-cv-00183-JRG, 2022 WL 782740, at *7–11, 18 (E.D. Tex. Mar. 14, 2022) (limiting "a Bluetooth communications interface" to "a communications interface using Bluetooth standards that existed at the time of the claimed invention")[4]; *Uniloc USA, Inc. v. Apple, Inc.*, Case No.

[4] Coincidentally, counsel for both parties litigated this exact issue in the Eastern District of Texas just two years ago, and InfoExpress's counsel, previously representing BillJCo, LLC against Cisco, advances the same defunct argument that several courts have previously rejected. *Compare* ECF No. 109 at 24, 25 ("The claim language does not limit 802.1x to any particular version. Neither does the specification . . . . Accordingly, pursuant to Dr. Striegel's technical analysis of each version of 802.1x and the consistency of the 802.1x versions as they relate to the claims, there would be no reason to construe the claim with a time-bar."); *with BillJCo, LLC v. Cisco Sys., Inc.*, No. 2:21-cv-00181-JRG, ECF No. 68 at 1 (E.D. Tex. Jan. 20, 2022) (Ex. V) ("Defendants' claim construction for 'Bluetooth,' which is part of the disputed phrase 'Bluetooth communication interface,' is that the use 'Bluetooth' requires incorporation of the entirety of promulgated industry standards that existed as of the priority date for the asserted patent. This argument lacks any support in the intrinsic evidence, which does not mention any industry standard."). Nevertheless, the *BillJCo* court agreed with Cisco (the same position that it maintains in this case): "In short, ***the Court agrees with Defendants***. In the claims, 'a Bluetooth communications interface' means

19-cv-1692, 2021 WL 432183, at *8 (N.D. Cal. Jan. 15, 2021) (holding that claim terms "Bluetooth messaging" and "Bluetooth protocols" should be limited to functionality described in the Bluetooth Core Specification "as it existed at the time of the claimed invention"); *ACQIS LLC v. Samsung Elecs. Co., Ltd.,* No. 2:20-cv-00295-JRG, at 32–33 (E.D. Tex. Sept. 26, 2021)) (stating "the term 'Universal Serial Bus (USB) protocol' must be interpreted as of the priority date" and limiting the scope of the term to USB Rev. 2 and earlier versions); *Fundamental Innovation Sys. Int'l LLC v. Samsung Elecs. Co.*, No. 2:17-cv-145-JRG-RSP, 2018 WL 647734, at *11 (E.D. Tex. Jan. 31, 2018) (citation omitted); ("The term 'USB' in the patents-in-suit should be limited to the Universal Serial Bus standards that existed at the time of the claimed invention.").

Here, InfoExpress contends that the earliest claimed priority date is September 24, 2003. Ex. W at 12. Based on this contention, "802.1x standard" and "802.1x protocol" should be construed to have the same meaning it did as of September 24, 2003. InfoExpress relies extensively on Dr. Striegel to suggest that the "802.1x" standard or protocol InfoExpress claimed nearly two decades ago has not changed much at all. Indeed, Dr. Striegel contends that "802.1x standard" and "802.1x protocol" should not be temporally limited up to the claimed priority date of the patent because "the 802.1x standard/protocol has been interoperable and consistent over the years" and has remained "substantially the same." ECF No. 109-36 ¶ 117. But when asked if future 802.1x protocols will "use the same port access control from now until 2027" (which is when the patents will expire), Dr. Striegel answered that "I don't have a crystal ball, and I couldn't say exactly what might go in or even if there will be a new revision of the standard before 2027." Ex. T at 113:9–114:1. And for the question, "Do you know whether the use of EAP will change in future versions of 802.1x?" *Id.* at 114:17–18. Dr. Striegel answered, "In its very nature, EAP is extensible," and "EAP dictates that framework. It was very intentionally meant to be extensible." *Id.* at 115:20–23, 116:11–13. By "extensible," Dr. Striegel meant that "[a] POSITA, who would have known 802.1X, would have already seen at the time different variations of EAP that were already running on that." *Id.* at 116:13–16. This testimony demonstrates the problem with InfoExpress's position: Dr. Striegel's testimony demonstrates that the 802.1x standard/protocol has continued to evolve over time, that a POSITA has no idea what the standard will look like in the future, and the only thing that a POSITA

'a communications interface using Bluetooth standards that existed at the time of the claimed invention.'" *BillJCo*, 2022 WL782740, at *5 (emphasis added).

can ascertain for certain is that the standard is going to change. *See Fundamental Innovation*, 2018 WL 647734, at *9 (finding that "[a]n invention cannot comply with standards not yet in existence").

To the extent the phrases "a wireless access point configured to support an 802.1x standard" and "an access point configured to use an 802.1x protocol" are not limited to then-existing technology as reflected in Defendant's proposed construction, those phrases are indefinite because these terms, as claimed, encompass versions of the 802.1x protocol or standard that a POSITA reading the specification at the time of the invention (September 2003) could not possibly have predicted. Ex. L ¶¶ 43-45; *Nautilus*, 572 U.S. at 901; *Fundamental Innovation*, 2018 WL 647734, at *9 (finding that "[a]n invention cannot comply with standards not yet in existence"). Moreover, as Dr. Striegel acknowledged, even a POSITA today cannot ascertain what the bounds of the claims will be through the expiration of the patents. InfoExpress suggests that Defendants' position is waived, but it provides no relevant authority that suggests Defendants are precluded from arguing that InfoExpress's claim-construction position would render the term indefinite. Accordingly, the term should be limited to "802.1x protocol as it existed on or before September 24, 2003" or otherwise found indefinite.

E. "audit data" ('350 Patent, claims 1, 6, 8, 9, 10, 13, 18, 19; '460 Patent, claim 1; '444 Patent, claim 22))

Defendants' Construction	Plaintiff's Construction
Information about a device used in determining compliance of the device with a security policy	Data relating to compliance for a security policy

F. "audit/auditing" ('484 Patent, claims 1, 13, 39, 42; '350 Patent, claims 1, 6, 8, 9, 10, 13, 18, 19; '450 Patent, claims 16, 22, 23, 25; '444 Patent, claim 22)

Defendants' Construction	Plaintiff's Construction
Evaluat[e/ing] information about [a device / the access device] for determining its compliance with a security policy	To evaluate the compliance of a security policy

Defendants are unsure as to what InfoExpress disputes about their proposed constructions for these terms. InfoExpress's brief proceeds as though it is arguing in favor of Defendants' proposals, and against its own proposals. Indeed, InfoExpress and Defendants are in absolute agreement on the fundamental understanding of the invention, as InfoExpress described in its brief. ECF No. 109 at 6–7. The only

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 23 of 1144
INFOEXPRESS, INC. - EX2572

purported issues that InfoExpress raised with Defendants' proposal are (1) that the proposal is purportedly "overbroad" because it "potentially would include all 'information about [a device / the access device]'"; and (2) the proposal "risks conflating" authentication of a user and auditing of a device. *Id.* at 7. As set forth below, InfoExpress is wrong on both points, and it is actually ***InfoExpress's*** proposal that exhibits these two problems.

By way of background, the specification teaches a specific way to restrict access to a secure network—by authenticating the user, and by separately auditing the security of the very device through which the user is attempting to access the secure network. ECF No. 109-2 at 2:15–19 ("In addition to ***authenticating users*** who wish to access Secure Network 100 using an Access Device 160, GateKeeper 110 is configured to ensure that ***Access Device*** 160 conforms to a predetermined security policy, before granting access to Secure Network 100." (emphasis added)). "Auditing" and "audit data" relate to only one of those two concepts—auditing the access device. "Auditing" is done by evaluating information about the access device (e.g., "operating system status (version, updates, etc.), antivirus software status, information concerning devices connected to Access Device 230, Windows registry information, MAC address, IP addresses, cookies, status of applications executing on Access Device 230," *id.* at 11:44–49)) to determine if the device complies with the requirements set forth in a security policy. For example, a network administrator may want to ensure that the device attempting to access the secure network has the latest security patches installed and the most up-to-date anti-virus signatures enabled. *Id.* at 2:19–25. This is because even if the *user* is properly authenticated, that does not mean the ***device*** through which the user is attempting to access the secure network is free of viruses that could spread to the secure network or weak security settings that could place the secure network at risk. *See id.* at 1:41–44 ("Reliance on mere user authentication includes several disadvantages. For example, there are no provisions to assure that an access device used by the authenticated user meets network security policies."). Only once it is determined that the access device itself is not problematic and complies with the security policy will that device be permitted to access the less-restricted subset of the secure network. Therefore, this device auditing process is decidedly distinct from the separate "authentication" of a "user." Again, InfoExpress's brief acknowledges that this is the thrust of the invention. *See* ECF No. 109 at 6–7.

In view of this shared understanding of the claimed invention, InfoExpress's gripes regarding

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 24 of 1144
INFOEXPRESS, INC. - EX2572

Defendants' proposal fall flat. Regarding issue (1)—where InfoExpress claims that Defendants' proposal construction is "overbroad" because it "potentially would include all 'information about [a device / the access device]'"—Defendants' proposal does not require "all" information about a device. Indeed, Defendants' proposal does not even use the word "all." Instead, it simply requires that information about a device/access device be evaluated to determine compliance with the "security policy." Whatever information about the access device is sufficient for evaluating compliance with the security policy is sufficient under Defendants' construction. Moreover, Defendants' proposal is actually *narrower* than InfoExpress's proposal, given that InfoExpress's proposal is untethered to the invention described in the specification.

Regarding issue (2)—where InfoExpress claims that Defendants' proposed construction "risks conflating" "authentication" of a "user" with "auditing" of a "device"—InfoExpress's argument proceeds as if InfoExpress has confused its own construction with Defendants' construction. Defendants' construction plainly requires that "auditing" be "about [a device / the access device]" to "determin[e] its [i.e., *the device's*] compliance with a security policy." It has nothing to do with the separate concept of "authenticating" a "user," and there is no ambiguity in Defendants' proposal. InfoExpress also made this clear to the PTAB in a July 24, 2024 filing. '484 Patent, Patent Owner Preliminary Response ("POPR") (Ex. X) at 10 ("The specification also establishes 'auditing' and 'authentication' are two different evaluations."); *id.* at 9 ("***[T]he claimed audit*** and determination that the device meets the requirement of a security policy means the device's ***hardware/software meets network device requirements***. Notably, 'auditing' is not authentication." (emphasis added)).

InfoExpress's proposal, in contrast, creates the very problem that InfoExpress argues it is trying to avoid, i.e., InfoExpress's proposal is not tailored to the "device" or "access device" (depending on the claim at issue), but instead, generically addresses "compliance of a security policy." InfoExpress acknowledges that "compliance of a security policy" could be related to "authentication" of a user instead of "auditing" a device. ECF No. 109 at 6 (arguing that a "security policy" can include "authentication data," which is "information about the user"). Thus, InfoExpress's construction (which simply requires evaluating compliance with a "security policy") is ambiguous as to whether the "compliance of a security policy" relates to authentication of a user or auditing of a device. InfoExpress's proposal could be

interpreted as evaluating the compliance of anything, based on anything. But the claims and specification are clear that "auditing" is of the ***device***, not the ***user***.

The Claims. The claims themselves support Defendants' proposal. They require, e.g., "audit[ing] the access device." ECF No. 109-2 at cl. 1. For example, claim 1 of the '484 Patent requires "a policy auditor configured to audit ***the access device*** using the at least one security policy," and taking certain action "if the audit results in a determination that ***the access device*** meets the requirements of the at least one security policy." *Id.* at cl. 1 (emphasis added). Therefore, the claims themselves make clear that "auditing" is done to the ***device*** seeking access, which must be based on information about the device.

The Specification. From the outset of the Asserted Patents, the specification makes clear that auditing is done to a device: "The gatekeeper is configured to enforce a security policy ***against the external device*** before granting it access." *Id.* at Abstract (emphasis added). The specification explains how this is done: the "gatekeeper" contains a "policy auditor" that "is configured to receive a request for access to Less-Restricted Subset 210 from Access Device 230, to determine which of Security Policy 330A or optional Security Policy 330B applies to the current request, ***to perform a security audit of Access Device*** 230 based on the appropriate member of Security Policies 330A-330B, and to notify Access Control 320 if the audit is passed." *Id.* at 9:31–38 (emphasis added). Figure 4 depicts this approach, in which the gatekeeper "authenticates a user, obtains audit data, and applies a security policy in an Authenticate User Step 440, an Obtain Audit Data Step 450 and an Apply Security Policy Step 460, respectively." *Id.* at 10:34–37. In the "Obtain Audit Data" step, "Policy Auditor 325 collects further data to perform a security audit of Access Device 230 responsive to Security Policy 330A or Security Policy 330B." *Id.* at 39–42. "Policy Auditor 325," which does the auditing, is part of the "GateKeeper 225" in Figure 3A. *Id.* at Fig. 3A. The "audit data" is information from the Access Device that "may include, for example, operating system status (version, updates, etc.), antivirus software status, information concerning devices connected to Access Device 230, Windows registry information, MAC address, IP addresses, cookies, status of applications executing on Access Device 230, or the like." *Id.* at 11:45–50.

The specification further explains that the "audit data" may be retrieved by "an agent running on Access Device 230" that is "configured to monitor local security and to report results of this monitoring

to Policy Auditor 325" to allow Policy Auditor 325 in the GateKeeper to audit the Access Device. *Id.* at 11:51–55. "The security audit typically includes determining if Access Device 230 satisfies requirements of the security policy." *Id.* at 11:63–65. It can "optionally include[] active probing, scanning, and/or collection of third party data regarding Access Device 230." *Id.* at 11:66–67. That is to say, the audit may be performed based on information about the Access Device provided by a third party. But the common thread is that in every instance the audit is performed on the *device* based on information about the device. InfoExpress recently made the same representations to the PTAB. '444 Patent POPR (Ex. Y) at 4–5 ("[T]he patent teaches an agent on the device to receive requests for and to send audit data pertaining to the device ***so the gatekeeper can apply the security policy to the device***." (emphasis added)); (Ex. X) at 9 ("***[T]he claimed audit*** and determination that the device meets the requirement of a security policy ***means*** the device's hardware/software ***meets network device requirements***." (emphasis added)).

Other Problems with InfoExpress's Proposal. InfoExpress's proposal also suffers from other infirmities. Namely, it is nonsensical on its face. There is no concept of evaluating the compliance "***of*** a security policy" in the Asserted Patents. Instead, a "compliance policy" is used to evaluate the compliance ***of*** something else—e.g., a device attempting to access the network. Further, InfoExpress's proposal is not clear about with what "the compliance of a security policy" would be evaluated. In other words, what is a security policy supposed to comply with? The specification does not address these issues.

Additional Issues Specific to "Audit Data." As set forth above, InfoExpress acknowledges that "audit data" is "information about a device." ECF No. 109 at 6 ("compliance with this 'security policy' can include . . . audit data (i.e., information about the device)."); *id.* ("'Audit data' is specifically directed to ensuring that the ***device*** that is attempting to access the protected network meet certain software and/or hardware criteria." (emphasis added)). In contrast to that acknowledgement, InfoExpress's construction is untethered from the device.

InfoExpress argues that a "security policy" can include "authentication data," which InfoExpress states is "information about the user," ECF No. 109 at 6, while simultaneously proposing a construction for "audit data" (which InfoExpress says is "information about a device") in a way that could cover either "authentication data" (i.e., for a ***user***) or "audit data" (i.e., for a ***device***). InfoExpress's proposed construction is therefore inconsistent with even its own argument, to say nothing of the specification and

claim language described above. "Audit data" is not simply any "data relating to compliance for a security policy" (as InfoExpress proposes) because that definition would cover "authentication data" as well (which InfoExpress acknowledges is different data that serves a different purpose—authentication of a ***user***).

Defendants' proposal, on the other hand, is consistent with the claim language, specification, and even InfoExpress's arguments, as described above. For example, the specification describes an "obtain audit data" step that sends "system data requests to Access Device 230, Router 220, or Access Point 215. The requested system data may include, for example, operating system status (version, updates, etc.), antivirus Software status, information concerning devices connected to Access Device 230, Windows registry information, MAC address, IP addresses, cookies, status of applications executing on Access Device 230, or the like." ECF No. 109-2 at 11:43–50. The claims are consistent with this discussion. *See, e.g.,* ECF No. 109-6 at cl. 6 ("wherein an agent running ***on the device*** collects the audit data" (emphasis added)); ECF No. 109-5 at cl. 22 ("sending a request for audit data to an agent running ***on the device***." (emphasis added)). Thus, "audit data" is not just any data relating to compliance with a security policy (e.g., including data relating to user authentication). Rather, "audit data" is information about a ***device*** and is used to determine the device's compliance with a security policy.

V. CONCLUSION

Based on the foregoing, Defendants respectfully request that the Court adopt Defendants' proposed constructions for the disputed terms.

Dated: August 23, 2024

Winston & Strawn LLP

By: */s/ Krishnan Padmanabhan*

Krishnan Padmanabhan (SBN 254220)

Attorney for Defendant Cisco Systems, Inc.

Dated: August 23, 2023

DUANE MORRIS LLP

By: */s/Terry Ahearn*

Terry Ahearn (SBN 216543)

Attorney for Defendant Fortinet, Inc.

Krishnan Padmanabhan (SBN 254220)
kpadmanabhan@winston.com
WINSTON & STRAWN LLP
200 Park Avenue
New York, NY 10166-4193
Telephone: (212) 294-3564
Facsimile: (212) 294-4700

David Enzminger (SBN 137065)
denzminger@winston.com
WINSTON & STRAWN LLP
333 S. Grand Avenue
Los Angeles, CA 90071
Telephone: (213) 615-1700
Facsimile: (213) 615-1750

William M. Logan (*pro hac vice*)
wlogan@winston.com
WINSTON & STRAWN LLP
800 Capitol Street, Suite 2400
Houston, TX 77002
Telephone: (713) 651-2600
Facsimile: (713) 651-2700

Attorneys for Defendant Cisco Systems, Inc.

Terry Ahearn (SBN 216543)
twahearn@duanemorris.com
DUANE MORRIS LLP
260 Homer Avenue, Suite 202
Palo Alto, CA 94301
Telephone: (650) 847-4150
Facsimile: (650) 847-4151

Matthew C. Gaudet (*pro hac vice*)
mcgaudet@duanemorris.com
David C. Dotson (*pro hac vice*)
dcdotson@duanemorris.com
Alice E. Snedeker (*pro hac vice*)
aesnedeker@duanemorris.com
DUANE MORRIS LLP
1075 Peachtree Street NE, Suite 1700
Atlanta, GA 30309
Telephone: (404) 253-6900
Facsimile: (404) 253-6901

Attorneys for Defendant Fortinet, Inc.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

INFOEXPRESS INC., Plaintiff, v. **CISCO SYSTEMS, INC.**, Defendant.	**Case No. 4:23-cv-02698-YGR** **DECLARATION OF WILLIAM M. LOGAN IN SUPPORT OF DEFENDANTS CISCO SYSTEMS, INC. AND FORTINET, INC.'S RESPONSIVE CLAIM CONSTRUCTION BRIEF**
INFOEXPRESS INC., Plaintiff, v. **FORTINET, INC.**, Defendant.	**Case No. 4:23-cv-04389-YGR** **DECLARATION OF WILLIAM M. LOGAN IN SUPPORT OF DEFENDANTS CISCO SYSTEMS, INC. AND FORTINET, INC.'S RESPONSIVE CLAIM CONSTRUCTION BRIEF**

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 30 of 1144
INFOEXPRESS, INC. - EX2572

I, William Logan, hereby declare, under penalty of perjury, that the following statements are true and correct:

1. I am an associate attorney at Winston & Strawn LLP and counsel of record for Defendant Cisco Systems, Inc. ("Cisco") in the above-captioned matter. I am a member in good standing of the State Bar of Texas and appear in this case *pro hac vice*. Except as otherwise noted, I have personal knowledge of the facts stated herein and, if called as a witness, I could and would competently testify thereto.

2. This declaration is made in support of Defendants Cisco Systems, Inc. ("Cisco") and Fortinet, Inc.'s ("Fortinet") Responsive Claim Construction Brief.

3. Attached as Exhibit A is a true and correct copy of the email from Ms. Vickie Kennedy serving Defendant Cisco Systems, Inc.'s Identification of Preliminary Claim Construction and Evidence to Counsel date March 25, 2024.

4. Attached as Exhibit B is a true and correct copy of Defendant Cisco Systems, Inc.'s Patent L.R. 4-2 Identification of Preliminary Claim Constructions and Evidence, served on March 25, 2024.

5. Attached as Exhibit C is a true and correct copy of the Microsoft Outlook invitation of Zoom meeting from Andrew Schwerin to counsel regarding Patent L.R. 4-2(c) Meet-and-Confer dated April 17, 2024. During this meeting, the parties conferred on proposed constructions, including Defendants' indefiniteness positions. InfoExpress never suggested during this meeting that it did not understand the bases for Defendants' indefiniteness positions and confirmed that it disagreed with Defendants' positions.

6. Attached as Exhibit D is a true and correct copy of the Microsoft Outlook invitation of Teams meeting from myself to counsel regarding Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement dated May 1, 2024. During this meeting, the parties conferred on proposed constructions, including Defendants' indefiniteness positions. InfoExpress never suggested during this meeting that it did not understand the bases for Defendants' indefiniteness positions and confirmed that it disagreed with Defendants' positions.

7. Attached as Exhibit E is a true and correct copy of the email from Mr. Andrew Schwerin to Counsel dated May 3, 2024.

8. Attached as Exhibit F is a true and correct copy of the email from Mr. Andrew Schwerin to Counsel dated July 26, 2024.

9. Attached as Exhibit G is a true and correct copy of the email from Mr. Andrew Schwerin to Counsel dated May 9, 2024

10. Attached as Exhibit H is a true and correct copy of the email from Mr. Andrew Schwerin to Counsel dated May 9, 2024.

11. Attached as Exhibit I is a true and correct copy of an email from Ms. Vickie Kennedy to counsel, serving Cisco's Notice of Deposition of Dr. Aaron Striegel, dated July 9, 2024.

12. Attached as Exhibit J is a true and correct copy of Cisco's Notice of Deposition of Dr. Aaron Striegel, served on July 9, 2024.

13. Attached as Exhibit K is a true and correct copy of the Declaration of Dr. A.L. Narasimha Reddy in Support of Defendants' Claim Constructions, served on June 28, 2024.

14. Attached as Exhibit L is a true and correct copy of an excerpt of Cisco's Amended Invalidity Contentions, served on March 1, 2024.

15. Attached as Exhibit M is a true and correct copy of Cisco's Identification of Proposed Claim Terms for Construction, served on November 30, 2023.

16. Attached as Exhibit N is a true and correct copy of Plaintiff InfoExpress, Inc.'s ("InfoExpress") Proposed Patent Claim Terms for Construction, served on November 30, 2023.

17. Attached as Exhibit O is a true and correct copy of InfoExpress's Proposed patent Claim Terms for Construction, served on March 4, 2024.

18. Attached as Exhibit P is a true and correct copy of InfoExpress's Amended Proposed patent Claim Terms for Construction, served on March 15, 2024.

19. Attached as Exhibit Q is a true and correct copy of InfoExpress's Second Amended Proposed Patent Claim Terms for Construction, served on March 22, 2024.

20. Attached as Exhibit R is a true and correct copy of InfoExpress's Preliminary Claim Constructions and Extrinsic Evidence, served on March 25, 2024.

21. Attached as Exhibit S is a true and correct copy of the transcript of the deposition of Dr. Aaron Striegel taken on August 1, 2024.

22. Attached as Exhibit T is a true and correct copy of U.S. Provisional Patent Application No. 60/513,080, titled "Gatekeeper Inventions for Controlling Access to a Corporate Network Using 802.1x" and filed on October 21, 2003.

23. Attached as Exhibit U is a true and correct copy of BillJCo, LLC's Reply Claim Construction Brief, ECF No. 68, filed in *BillJCo, LLC v. Cisco Sys., Inc.*, No. 2:21-cv-00181-JRG; 2:21-cv-00183-JRG. (E.D. Tex. Jan. 27, 2022).

24. Attached as Exhibit V is a true and correct copy of InfoExpress's Disclosure of Asserted Claims and Infringement Contentions Per Patent L.R. 3-1 and 3-2 with exhibits, served on October 2, 2023.

25. Attached as Exhibit W is a true and correct copy of the Patent Owner Preliminary Response, *Cisco Sys., Inc. v. InfoExpress, Inc.,* IPR2024-00675 for U.S. Patent No. 7,523,484 filed publicly, dated July 25, 2024.

26. Attached as Exhibit X is a true and correct copy of the Patent Owner Preliminary Response, *Cisco Sys., Inc. v. InfoExpress, Inc.,* IPR2024-00677 for U.S. Patent No. 8,578,444 filed publicly, dated July 17, 2024.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 23rd day in August in The Woodlands, Texas.

By: */s/ William M. Logan*
William M. Logan

EXHIBIT A

From:	Kennedy, Vickie
To:	Tosti, Jacob A.; Michalek, Brian R.; Grabenstein, Casey; Schwerin, Andrew; Kuo, Joseph M.; mflynnobrien@bdiplaw.com; bentzminger@bdiplaw.com
Cc:	WS-Cisco-InfoExpress
Subject:	InfoExpress Inc. v. Cisco Systems, Inc. (4:23-cv-02698-YGR) Cisco"s Identification of Preliminary Claim Constructions
Date:	Monday, March 25, 2024 5:57:23 PM
Attachments:	2024-03-25 Cisco Identification of Prelim Claim Constructions and Evidence per PLR 4-2.pdf

Counsel,
Attached please find Cisco System, Inc.'s Patent L.R. 4-2 Identification of Preliminary Claim Constructions and Evidence.

Vickie Kennedy

Senior Paralegal

Winston & Strawn LLP
35 W. Wacker Drive
Chicago, IL 60601-9703

D: +1 312-558-5940

F: +1 312-558-5700

VCard | Email | winston.com

EXHIBIT B

Krishnan Padmanabhan (SBN 254220)
WINSTON & STRAWN LLP
200 Park Avenue
New York, NY 10166-4193
Telephone: (212) 294-6700
Facsimile: (212) 294-4700
KPadmanabhan@winston.com

David Enzminger (SBN: 137065)
WINSTON & STRAWN LLP
333 S. Grand Avenue
Los Angeles, CA 90071
Telephone: (213) 615-1700
Facsimile: (213) 615-1750
DEnzminger@winston.com

William Logan (*pro hac vice*)
WINSTON & STRAWN LLP
800 Capitol Street, Suite 2400
Houston, TX 77002-2925
Telephone: (713) 651-2600
Facsimile: (713) 651-2700
WLogan@winston.com

Patrick Clark (*pro hac vice*)
WINSTON & STRAWN LLP
2121 N. Pearl St., Suite 900
Dallas, TX 75201
Telephone: (214) 453-6492
Facsimile: (214) 453-6400
PClark@winston.com

Attorneys for Defendant
CISCO SYSTEMS, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INFOEXPRESS INC.,

Plaintiff,

v.

CISCO SYSTEMS, INC.,

Defendant.

Case No. 4:23-cv-02698-YGR

DEFENDANT CISCO SYSTEMS, INC.'S PATENT L.R. 4-2 IDENTIFICATION OF PRELIMINARY CLAIM CONSTRUCTIONS AND EVIDENCE

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 37 of 1144
INFOEXPRESS, INC. - EX2572

I. INTRODUCTION

Pursuant to Patent L.R. 4-2, and the Amended Scheduling Order (ECF No. 63), Defendant Cisco Systems, Inc. ("Cisco" or "Defendant") hereby submits its identification of preliminary Claim constructions and extrinsic evidence.

II. ASSERTED PATENTS AND CLAIMS

Plaintiff InfoExpress Inc. ("InfoExpress" or "Plaintiff") currently asserts the following Patents, Claims, and priority dates:

Asserted Patents	Asserted Claims	Asserted Priority Dates
U.S. Patent No. 7,523,484 (the "'484 Patent")	1–5, 11–13, 15–19, 23–25, 28, 38–39, 41–43, 53, 57–59, 61–63, 65–66, and 68	September 24, 2003 / October 21, 2003
U.S. Patent Nos. 8,347,350 (the "'350 Patent")	1–2, 4–10, 13, and 18–19	September 24, 2003 / October 21, 2003
U.S. Patent No. 8,051,460 (the "'460 Patent")	1–6, 10–12, 16–22, and 27	September 24, 2003 / October 21, 2003
U.S. Patent No. 8,677,450 (the "'450 Patent")	1–4, 7–9, 14, 16, 22–23, 25, and 27	September 24, 2003 / October 21, 2003
U.S. Patent No. 8,578,444 (the "'444 Patent")	1–6, 10, 12, 17, and 22	September 24, 2003 / October 21, 2003
U.S. Patent No. 8,117,645 (the "'645 Patent")	1–2 and 5–6	September 24, 2003 / October 21, 2003

III. PRELIMINARY STATEMENT AND RESERVATION OF RIGHTS

Cisco's Preliminary Claim Constructions are based upon its investigation and discovery received to date, including InfoExpress Inc.'s ("InfoExpress") Preliminary Infringement Contentions. Cisco reserves the right to amend these constructions to address any additional discovery, including any clarification, additional understanding, or amendment of InfoExpress's Preliminary Infringement

Contentions. Cisco further reserves the right to amend its Preliminary Claim Constructions as necessary in response to any proposed constructions provided by InfoExpress or pursuant to the meet-and-confer process contemplated in Patent L.R. 4-2(c).

Cisco reserves the right to refine this list to construe any portion of any identified term or element, additional language surrounding any identified term or element, or any term or element similar to an identified term or element found in any additional Claim limitations within any of the Asserted Claims. If the Claim terms or elements set forth herein include particular terms or elements appropriate for separate constructions, such terms or elements are deemed part of this disclosed list. Similarly, to the extent additional Claim language provides appropriate context to construe terms or elements listed herein, such additional language is deemed part of this disclosure.

Cisco has grouped certain terms below for ease of reference when conferring. Cisco may adjust or eliminate the groupings over the course of the meet and confer process.

IV. IDENTIFICATION OF PRELIMINARY CLAIM CONSTRUCTIONS

Subject to the foregoing, Cisco identifies the following claim constructions below.

Dated: March 25, 2024

WINSTON & STRAWN LLP

By: */s/ Krishnan Padmanabhan*

Krishnan Padmanabhan (SBN 254220)
WINSTON & STRAWN LLP
200 Park Avenue
New York, NY 10166-4193
Telephone: 212-294-6700
Facsimile: 212-294-4700
KPadmanabhan@winston.com

David Enzminger (SBN: 137065)
WINSTON & STRAWN LLP
333 S. Grand Avenue
Los Angeles, CA 90071
Telephone: (213) 615-1700
Facsimile: (213) 615-1750
DEnzminger@winston.com

William Logan (*pro hac vice*)
WINSTON & STRAWN LLP
800 Capitol Street, Suite 2400
Houston, TX 77002-2925
Telephone: (713) 651-2600
Facsimile: (713) 651-2700
WLogan@winston.com

Patrick Clark (*pro hac vice*)
WINSTON & STRAWN LLP
2121 N. Pearl St., Suite 900
Dallas, TX 75201
Telephone: (214) 453-6492
Facsimile: (214) 453-6400
PClark@winston.com

Attorneys for Defendant
CISCO SYSTEMS, INC.

Cisco's Preliminary Claim Constructions and Evidence

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
1.	access control	'484 Patent: Claim 1C '350 Patent: Claim 1PRE '645 Patent: Claims 1PRE, 2, 5, 6	indefinite	Expert Declaration and Testimony of Dr. Narasimha Reddy that this term is indefinite Intrinsic Evidence from U.S. Patent No. 7,523,484: 1:26-30. The need for access control has grown with users' demands for accessing secure networks over the Internet and from personal devices such as laptop computers and personal digital assistants. 1:31-32. A first level of access control is achieved by requiring authentication of a user. 1:53-55. A greater level of access control may be achieved by including a gatekeeper between the secure network and the access device. 3:60-4:9. Various embodiments of the invention include a network gatekeeper comprising at least one security policy including requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network, a policy auditor configured to audit an access device using the at least one security policy, in response to a request to access the less-restricted subset of the protected network, the request being sent from the access device to the gatekeeper via a communication device, and an access control configured to reconfigure the communication device such that data sent from the access device can be received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit results in a determination that the access device meets the requirements of the at least one security policy, the restricted subset of the protected network including the gatekeeper.

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				9:20-21. Switch Logic 317 is controlled by an Access Control 320 included in GateKeeper 225. 9:21-23. Access Control 320 is configured to send commands to Switch Logic 317 in order to reconfigure members of Ports 305A-305G. 9:26-29. In some embodiments, as described further herein, Access Control 320 is also configured to read a status of members of Ports 305A-305G and/or device identification data from Switch Logic 317. 9:30-31. Access Control 320 is responsive to a Policy Auditor 325 included in GateKeeper 225. 9:31-38. Policy Auditor 325 is configured to receive a request for access to Less-Restricted Subset 210 from Access Device 230, to determine which of Security Policy 330A or optional Security Policy 330B applies to the current request, to perform a security audit of Access Device 230 based on the appropriate member of Security Policies 330A-330B, and to notify Access Control 320 if the audit is passed. 9:38-40. This notice typically causes Access Control 320 to reconfigure a member of Ports 305A-305G using Switch Logic 317. 9:40-43. For example, in some embodiments, if Security Policy 330A applies and if Access Device 230 satisfies requirements of Security Policy 330A, then Policy Auditor 325 provides a notice to Access Control 320. 9:43-45. In response, Access Control 320 sends appropriate commands to Switch Logic 317. 10:45-47. In Update Port Log Step 410, Access Control 320 reads port configuration data from Access Point 215

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				to determine the current configuration of Ports 305A-305G. 10:55-57. In Restrict Port Step 420, Access Control 320 configures those members of Ports 305A-305G that may be accessed by external devices, such as Access Device 230. 12:33-35. In typical embodiments, reconfiguration of Port 305A is accomplished by sending commands from Access Control 320 to Switch Logic 317. 12:53-56. Access Control 320 may selectively grant access to different parts of Protected Network 200 if ACL 340B is configured to allow access to different elements within Protected Network 200 than ACL 340A is configured. 13:3-5. A selection between granting access to a first or second part of Protected Network 200 can, therefore, be made using Access Control 320.
2.	access control list	'484 Patent: Claims 2, 59 '450 Patent: Claim 3 '444 Patent: Claim 3	indefinite	Expert Declaration and Testimony of Dr. Narasimha Reddy that this term is indefinite Intrinsic Evidence from U.S. Patent No. 7,523,484: 2:62-67. Typically, the less-restricted subset of the protected network and the restricted subset of the protected network are characterized by Virtual Local Area Networks (e.g., VLANs) defined within the access point and optionally by access control lists (ACL) of a router, firewall, or switch situated between the VLAN and the protected network. 6:24-27. In this case, as described further herein, access control lists within Router 220 are optionally used to

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				independently control access to specific devices within Less-Restricted Subset 210. 6:65-7:2. As is described further herein, management of Access Point 215 is accomplished by configuring and reconfiguring one or more communication ports within Access Point 215, and optionally setting access control lists within Router 220. 8:38-42. Data passed through members of Ports 305D-305G are received by Router 220 and may be communicated to other elements of Protected Network 200 responsive to access control lists (ACL 340A-340D) associated with Ports 335A-335D of Router 220. 8:45-48. For example, ACL 340C may be an access control list that specifically allows communication to network addresses used by GateKeeper 225 and DHCP 260, and blocks communication to all other network addresses. 12:44-48 While access control lists (ACL 340A-340D) within Router 220 are typically configured prior to Receive Access Request Step 430, in some embodiments, Reconfigure Port Step 470 further includes configuring one or more members of ACL 340A-340D.
3.	gatekeeper	'484 Patent Claims: 1PRE, 1B, 1C, 2, 3, 4, 5, 11, 12, 13, 15, 16, 17, 18, 19, 20, 23, 24, 25, 27A, 27C, 28A, 28C, 41A, 41C, 43, 57A, 57B, 68, 71, 82A, 82C '460 Patent: Claims 1A, 1C, 1D, 5, 16A, 16C, 20, 22 '450 Patent: Claims 1C, 2	indefinite	Expert Declaration and Testimony of Dr. Narasimha Reddy that this term is indefinite Intrinsic Evidence from U.S. Patent No. 7,523,484: Abstract. A new approach to network security includes manipulating an access point such that an initial communication from an external device is passed to a restricted subset of a computing network including a gatekeeper.

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
		’444 Patent: Claims 1C, 1D, 7, 17, 22C, 22D ’645 Patent: Claims 1[B-i], 1[C-ii], 2		Abstract. The gatekeeper is configured to enforce a security policy against the external device before granting access to a less-restricted subset of the computing network. Abstract. If requirements of the security policy are satisfied, then the gatekeeper reconfigures the access point such that further communication from the external device may be received by elements of the less-restricted subset. 1:53-55. A greater level of access control may be achieved by including a gatekeeper between the secure network and the access device. 1:55-56. The gatekeeper is configured to ensure that the access device conforms to a predetermined security policy. 1:57-59. FIG. 1 is a block diagram of a Secure Network, generally designated 100, including two instances of a Gatekeeper 110 each associated with a different instance of an Access Point 120. 1:65-2:1. These ports are used to connect through GateKeeper 110 to other elements within Secure Network 100 such as File Server 130 or LAN 125. 2:1-4. Large corporate networks may include many instances of Access Point 120, each including hundreds of individual communication ports and being associated with an instance of GateKeeper 110. 2:14-15. GateKeeper 110 is configured to control access to Secure Network 100. 2:15-19. In addition to authenticating users who wish to access Secure Network 100 using an Access Device 160,

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				GateKeeper 110 is configured to ensure that Access Device 160 conforms to a predetermined security policy, before granting access to Secure Network 100. 2:19-22. For example, GateKeeper 110 may make certain that Access Device 160 has up-to-date virus software and encryption protocols as proscribed by the security policy. 2:22-25. Once GateKeeper 110 has verified that Access Device 160 satisfies the security policy, Access Device 160 is allowed to communicate through GateKeeper 110 to LAN 125. 2:26-28. A disadvantage of the use of GateKeeper 110, as practiced in the prior art, is that all communications between Access Device 160 and LAN 125 pass through GateKeeper 110. 2:31-34. The use of one instance of GateKeeper 110 to support numerous instances of Access Device 160 is limited by bandwidth and required sophistication (e.g., cost) of GateKeeper 110. 2:34-37. It is undesirable for GateKeeper 110 to become a limiting factor on the bandwidth of communication between instances of Access Device 160 and Secure Network 100. 2:37-39. Further, the use of a separate GateKeeper 110 for each instance of Access Device 160 or Access Point 120 is often prohibitively expensive. 2:39-42. Even if a separate GateKeeper is used for each Access Point 120, there is no isolation between compliant and non-compliant Access Devices 160 which are attached to the same Access Point 120.

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				2:52-56. Elements (e.g., a gatekeeper) of the restricted subset are then used to apply security policies to the access device and if security policies are satisfied, the access device is granted access to a less-restricted subset of the protected network. 3:16-20. For example, the restricted VLAN allows traffic to pass to a gatekeeper configured to receive requests for access to the less-restricted VLAN, and to determine if, and to what extent, access may be allowed. 3:20-22. To grant access, the gatekeeper sends commands to the access point in order to reconfigure a communication port to which the access device is connected. 3:29-30. This network traffic need not pass through the gatekeeper. 3:30-34. Thus, in various embodiments of the invention a gatekeeper is used to grant access to the less-restricted subset, and after access has been granted, most network traffic does not need to pass through the gatekeeper. 3:34-37. For example, in some embodiments, the gatekeeper only receives requests to access the less-restricted network and data regarding access to and security of the protected network. 3:39-42. These limited communications with gatekeeper occur both before and after reconfiguration of the communication port, and eliminate a significant disadvantage associated with the use of prior art gatekeepers. 3:43-59. Various embodiments of the invention include a computing network comprising a less-restricted subset of the computing network, access to the less-restricted

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				subset being responsive to a first VLAN, a restricted subset of the computing network including a gatekeeper, the gatekeeper configured to receive requests for access to the less-restricted subset from an access device and to issue commands configured to allow access to the less-restricted subset, access to the restricted subset of the computing network being responsive to a second VLAN, and at least one access point including a communication port configurable for communication with the less-restricted subset or alternatively for communication with only the restricted subset, configuration of the communication port including association of the communication port alternatively with the first VLAN or the second VLAN, configuration of the communication port being responsive to the commands issued by the gatekeeper. 3:60-4:9. Various embodiments of the invention include a network gatekeeper comprising at least one security policy including requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network, a policy auditor configured to audit an access device using the at least one security policy, in response to a request to access the less-restricted subset of the protected network, the request being sent from the access device to the gatekeeper via a communication device, and an access control configured to reconfigure the communication device such that data sent from the access device can be received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit results in a determination that the access device meets the requirements of the at least one security policy, the restricted subset of the protected network including the gatekeeper. 4:10-22. Various embodiments of the invention include a method of granting access to a protected network, the

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				method comprising receiving a request for access to a less-restricted subset of the protected network from an access device external to the protected network, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper, applying a security policy to the access device, responsive to the request, and reconfiguring the communication port for communicating between the access device and the less-restricted subset of the protected network, if requirements of the security policy are satisfied. 4:24-43. Various embodiments of the invention include a method of granting access to a protected network, the method comprising receiving a first communication from an access device at a communication port, the communication port being configured to pass the first communication to a restricted subset of the protected network, the restricted subset including a gatekeeper configured to enforce security policy for access to a less-restricted subset of the protected network, receiving a command from the gatekeeper, the command being responsive to the received first communication and being configured to reconfigure the communication port to communicate data to the less-restricted subset of the protected network, configuring the communication port to communicate data to the less-restricted subset of the protected network rather than merely the restricted subset of the protected network, responsive to the received command, and receiving a second communication from the access device at the communication port, the communication port now being configured to pass the second communication to the less-restricted subset of the protected network.

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				5:33-36. This restricted subset includes a gatekeeper configured to administer a security policy governing access to those parts of the protected computing network that are not part of the restricted subset. 5:41-44. If the device requesting access satisfies requirements of the security policy, then the gatekeeper sends commands to the access point in order to reconfigure the communication port through which the access request was received. 5:57-58. As is described further herein this access is under the control of a GateKeeper 225. 5:58-60. GateKeeper 225 is configured to enforce a security policy against one or more Access Device 230 requesting access to Less-Restricted Subset 210. 6:5-6. Restricted Subset 205 is a subset of Protected Network 200 including at least GateKeeper 225. 6:11-14. For example, in one embodiment, Restricted Subset 205 includes a server configured to function as DHCP 260 and a server configured to function as GateKeeper 225. 6:14-16. In one embodiment, Restricted Subset 205 includes a single computing device configured to function as both Update Module 255 and GateKeeper 225. 6:34-36. GateKeeper 225 is configured to enforce one or more security policies against an instance of Access Device 230 attempting to access Protected Network 200. 6:41-47. For example, in one embodiment GateKeeper 225 is configured to enforce a security policy that requires a user of Access Device 230 to provide a username and password, requires Access Device 230 to

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				be running an operating system with specific security patches installed, requires that Access Device 230 not be connected to any insecure devices, and requires that Access Device 230 have current antivirus software installed. 6:49-55. In some embodiments, GateKeeper 225 is configured to enforce several alternative security policies having different levels of requirements, and to determine which security policy to enforce based on the identity of Access Device 230, the identity of a user of Access Device 230, those elements of Less-Restricted Subset 210 to which access is requested, and/or the like. 6:59-61. Security policies may be stored on GateKeeper 225, on Policy Manager 250, or elsewhere accessible to Restricted Subset 205. 6:62-65. In some embodiments, a single instance of GateKeeper 225 is configured to manage access through more than one Access Point 215 and/or to manage access to more than one Protected Network 200. 7:2-4. In some embodiments Protected Network 200 includes a plurality of Access Point 215, a plurality of GateKeeper 225 and/or a plurality of Restricted Subset 205. 7:4-6. Further details of GateKeeper 225 and Access Point 215 are discussed below. 7:17-19. In some embodiments, Access Device 230 is configured to execute a software and/or hardware agent for communicating with GateKeeper 225. 7:19-22. For example, in one embodiment, Access Device 230 includes an agent configured to monitor code

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				running on Access Device 230 and report any suspicious code to GateKeeper 225. 7:22-26. In another example, Access Device 230 may include software and/or hardware configured to monitor other devices connected to Access Device 230 and to report information about these devices (e.g., their security statuses or MAC addresses) to GateKeeper 225. 7:27-29. Policy Manager 250 is configured to centrally create, update, and distribute security policies enforced by one or more GateKeeper 225. 7:46-50. Update Module 255 is optionally included in Less-Restricted Subset 210 or external to Protected Network 200. Update Module 255 optionally operates responsive to a security policy and/or to GateKeeper 225. 7:51-53. FIG. 3A is a block diagram showing further details of Access Point 215, Router 220 and GateKeeper 225, according to various embodiments of the invention. 8:24-25. As is discussed further below, the commands received by Switch Logic 317 may be generated by GateKeeper 225. 8:25-30. This communication between GateKeeper 225 and Switch Logic 317 may be accomplished using SNMP (Simple Network Management Protocol), telnet, SSH (Secure Shell), RADIUS (Remote Authentication User Dial-In Service), EAP (Extensible Authentication Protocol), or the like. 8:45-52. For example, ACL 340C may be an access control list that specifically allows communication to network addresses used by GateKeeper 225 and DHCP 260, and blocks communication to all other network addresses. In this case, communication through Port

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				335C of Router 220 would only be allowed to reach these elements of Restricted Subset 205 and would not be allowed to reach elements of Less-Restricted Subset 210. 9:20-21. Switch Logic 317 is controlled by an Access Control 320 included in GateKeeper 225. 9:30-31. Access Control 320 is responsive to a Policy Auditor 325 included in GateKeeper 225. 9:53-58. FIG. 3B is a block diagram showing further details of Access Point 215, Router 220 and GateKeeper 225 of FIG. 2, after access has been granted to elements of Less-Restricted Subset 210, according to various embodiments of the invention. 10:3-8. Once Port 305A has been reconfigured to be associated with VLAN 310A, future general network traffic between Access Device 230 and Less-Restricted Subset 210 may pass through Ports 305A, 305D and 335A without passing through GateKeeper 225 or other elements of Restricted Subset 205. 10:8-10. Further, communication related to access to security of Protected Network 200 may still be received by GateKeeper 225 via Port 305A. 10:10-14. For example, GateKeeper 225 may still receive control traffic such as DNS lookups or DHCP requests, or requests to access additional elements of Protected Network 200, or requests to continue to access the Less-Restricted Subset 210. 10:18-20. For example, ACL 340B may be configured to grant access to File Server 235, Policy Manager 250 and GateKeeper 225.

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				10:33-37. In response, GateKeeper 225 authenticates a user, obtains audit data, and applies a security policy in an Authenticate User Step 440, an Obtain Audit Data Step 450 and an Apply Security Policy Step 460, respectively. 10:37-40. If the security policy is satisfied, then in a Reconfigure Port Step 470, GateKeeper 225 reconfigures the communication port of Access Point 215 to which Access Device 230 has connected. 10:51-53. Typically, the read configuration data is stored in a port configuration table, for example within GateKeeper 225. 10:61-62. ACL 340C is configured to allow communication to, for example, DHCP 260 and GateKeeper 225. 11:10-13. In Receive Access Request Step 430, a request for access to Less-Restricted Subset 210 is received at one of Ports 305A-305C configured to pass data to DHCP 260 and Gatekeeper 225. 11:14-23. Because Port 305A, Port 305B and Port 305C are configured to pass data to DHCP 260 and Gatekeeper 225, the received access request passes through Access Point 215 and is received by either DHCP 260 or Gatekeeper 225 In typical embodiments, an initial access request is first acknowledged by DHCP 260 which assigns a dynamic network address (e.g., IP address) to Access Device 230 and returns, to Access Device 230, a network address associated with GateKeeper 225 or more specifically Policy Auditor 325. 11:23-25. Using this network address, Access Device 230 may engage in further communication with GateKeeper 225 or Policy Auditor 325.

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				11:25-30. In some embodiments, DHCP 260 and instances of GateKeeper 225 are associated with a local domain name service configured to provide network addresses associated with a particular instance of GateKeeper 225 configured to manage (reconfigure) the particular Access Point 215 to which Access Device 230 is connected. 12:20-24. This communication port is reconfigured such that data received by the communication port is passed to one or more elements of Less-Restricted Subset 210 rather than merely elements of Restricted Subset 205 (e.g., GateKeeper 225). 13:32-34. However, in some embodiments, ACL 340A is configured to allow access to GateKeeper 225 as well as Less-Restricted Subset 210. 13:34-37. Thus, general network traffic does not need to pass through GateKeeper 225, while communication regarding security of Protected Network 200 is optionally received by GateKeeper 225. 13:37-38. Further communication between Access Device 230 and GateKeeper 225 may provide a variety of advantages. 13:38-42. For example, further communication between GateKeeper 225 and an agent executing on Access Device 230 may allow for continuing audits of security aspects of Access Devices 230. 13:46-49. Further communication between GateKeeper 225 and an agent executing on Access Device 230 may also allow for a user of Access Device 230 to explicitly logoff Protected Network 200.

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				13:55-14:1. According to embodiments like that disclosed in U.S. Provisional Patent Application No. 60/513,080, the disclosure of which has been incorporated herein by reference, an AP (e.g., a switch or wireless access point (WAP) which is used to connect end points to the corporate network) may be programmed to prohibit access by the PC (e.g., notebook, desktop PC, PDA, or similar computing device) to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK (e.g., software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria) passes, while still supporting the existing encryption and authentication functionality. 15:32-34. In some embodiments, various aspects of GateKeeper 225 may be incorporated into Access Point 215 and/or Router 220. 15:34-36. GateKeeper 225 and Policy Manager 250 are each optionally implemented on a plurality of computing devices within Restricted Subset 205. 15:37-40. In some embodiments, GateKeeper 225 uses DHCP 260 to assign IP addresses from a restricted IP address range depending on the compliance of Access Device 230 to security policies 330A-330B. 15:40-45. GateKeeper 225 inserts DHCP options and/or modifies the IP source addresses of DHCPDISCOVER and DHCPREQUEST packets, based on the compliance of the Access Device 230 to security policies 330A-330B. 15:45-49. DHCP 260 is configured to provide an address from the restricted address range or the less-restricted address range based on the source address and/or options

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				present in the DHCP request or discover packets that have been modified by GateKeeper 225.
4.	policy auditor	'484 Patent: Claims 1A, 6	indefinite	Expert Declaration and Testimony of Dr. Narasimha Reddy that this term is indefinite Intrinsic Evidence from U.S. Patent No. 7,523,484: 3:60-4:9. Various embodiments of the invention include a network gatekeeper comprising at least one security policy including requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network, a policy auditor configured to audit an access device using the at least one security policy, in response to a request to access the less-restricted subset of the protected network, the request being sent from the access device to the gatekeeper via a communication device, and an access control configured to reconfigure the communication device such that data sent from the access device can be received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit results in a determination that the access device meets the requirements of the at least one security policy, the restricted subset of the protected network including the gatekeeper. 9:30-31. Access Control 320 is responsive to a Policy Auditor 325 included in GateKeeper 225. 9:31-38. Policy Auditor 325 is configured to receive a request for access to Less-Restricted Subset 210 from Access Device 230, to determine which of Security Policy 330A or optional Security Policy 330B applies to the current request, to perform a security audit of Access Device 230 based on the appropriate member of Security Policies 330A-330B, and to notify Access Control 320 if the audit is passed.

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				9:40-45. For example, in some embodiments, if Security Policy 330A applies and if Access Device 230 satisfies requirements of Security Policy 330A, then Policy Auditor 325 provides a notice to Access Control 320. In response, Access Control 320 sends appropriate commands to Switch Logic 317. 9:48-50. In alternative embodiments, Security Policies 330A-330B are stored elsewhere in Protected Network 200 accessible to Policy Auditor 325. 11:18-23. In typical embodiments, an initial access request is first acknowledged by DHCP 260 which assigns a dynamic network address (e.g., IP address) to Access Device 230 and returns, to Access Device 230, a network address associated with GateKeeper 225 or more specifically Policy Auditor 325. 11:23-25. Using this network address, Access Device 230 may engage in further communication with GateKeeper 225 or Policy Auditor 325. 11:31-33. In optional Authenticate User Step 440, Policy Auditor 325 authenticates the identity of Access Device 230 and/or a user of Access Device 230. 11:39-42. In optional Obtain Audit Data Step 450, Policy Auditor 325 collects further data to perform a security audit of Access Device 230 responsive to Security Policy 330A or Security Policy 330B. 11:52-55. For example, Access Device 230 may include a software agent configured to monitor local security and to report results of this monitoring to Policy Auditor 325. 11:56-59. In Apply Security Policy Step 460, a security audit of Access Device 230 is performed by Policy

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				Auditor 325 responsive to a member of Security Policy 330A or Security Policy 330B.
5.	authentication module	'645 Patent: Claims 1[B-i], 1[C-ii], 2	indefinite	Expert Declaration and Testimony of Dr. Narasimha Reddy that this term is indefinite Intrinsic Evidence from U.S. Patent No. 7,523,484: 14:20-23. There may be one or more instances of the CF and SF, which correspond to the separate EAP Authentication Modules (EAPM) that are supported.
6.	server filter / SF	'645 Patent: Claims 2, 5	indefinite	Expert Declaration and Testimony of Dr. Narasimha Reddy that this construction is indefinite Intrinsic Evidence from U.S. Patent No. 7,523,484: 14:11-13. The EAP server then calls a server filter which sends the responses to the GK for evaluation. 14:18-20. According to an exemplary embodiment, client filters (CF) and server filters (SF) are added along with an agent and GK to perform audits, as highlighted in FIG. 5.
7.	code segment	'484 Patent: Claims 82A, 82B, 82C, 82D, 82E	indefinite	Expert Declaration and Testimony of Dr. Narasimha Reddy that this term is indefinite Intrinsic Evidence from U.S. Patent No. 7,523,484: The term does not appear in the specification.
8.	element	'484 Patent: Claim 20	indefinite	Expert Declaration and Testimony of Dr. Narasimha Reddy that this term is indefinite Intrinsic Evidence from U.S. Patent No. 7,523,484: Abstract. If requirements of the security policy are satisfied, then the gatekeeper reconfigures the access point such that further communication from the external

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				device may be received by elements of the less-restricted subset. 1:65-2:1. These ports are used to connect through GateKeeper 110 to other elements within Secure Network 100 such as File Server 130 or LAN 125. 2:52-56. Elements (e.g., a gatekeeper) of the restricted subset are then used to apply security policies to the access device and if security policies are satisfied, the access device is granted access to a less-restricted subset of the protected network. 3:7-13. The restricted VLAN allows network traffic to pass to the restricted subset of the protected network and is typically restricted in the sense that it only allows access to elements of the protected network that are configured to communicate with an access device whose security characteristics are unknown or questionable. 3:13-16. In contrast, the less-restricted VLAN allows access to the less-restricted subset of the protected network and, in typical embodiments, to elements of both the less-restricted subset and the restricted subset. 3:26-29. Subsequent to reconfiguration of the communication port, network traffic can pass from the access device through the less-restricted VLAN to elements of both the less-restricted subset and (optionally) the restricted subset. 3:59. Other elements are optional. 4:9. Other elements are optional. 4:54. Other elements are optional. 4:55-60. In various embodiments of the invention the restricted subset of a computing network includes

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 60 of 1144
INFOEXPRESS, INC. - EX2572

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				elements configured to communicate with access devices having an unknown or questionable security status, and the less-restricted subset of the computing network includes those elements of the computing network not included in the restricted subset. 5:39-41. The less-restricted subset being less restricted relative to the restricted subset in terms of what elements may be included in each subset. 6:17-18. Less-Restricted Subset 210 includes those elements of Protected Network 200 not included in Restricted Subset 205. 6:21-22. In some embodiments, Protected Network 200 includes elements having a hierarchy of access restrictions. 6:49-55. In some embodiments, GateKeeper 225 is configured to enforce several alternative security policies having different levels of requirements, and to determine which security policy to enforce based on the identity of Access Device 230, the identity of a user of Access Device 230, those elements of Less-Restricted Subset 210 to which access is requested, and/or the like. 7:35-38. For example, a security policy may be selected for use responsive to a device type of Access Device 230 and/or the elements of Protected Network 200 to which access has been requested. 8:38-42. Data passed through members of Ports 305D-305G are received by Router 220 and may be communicated to other elements of Protected Network 200 responsive to access control lists (ACL 340A-340D) associated with Ports 335A-335D of Router 220.

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				8:42-45. ACL 340A through 340D are each communication filters that deny or allow communication to be passed to specific elements or sets of elements within Protected Network 200. 8:48-52. In this case, communication through Port 335C of Router 220 would only be allowed to reach these elements of Restricted Subset 205 and would not be allowed to reach elements of Less-Restricted Subset 210. 8:53-55. ACL 340A-340D of Router 220 may be used to limit communication from Access Device 230 to specific elements of Protected Network 200. 8:63-9:2. As is discussed further herein, by reconfiguring a member of Ports 305A-305C to be associated with a different member of VLANs 310A-310D, not subject to the filtering of ACL 340C, communications from Access Device 230 can be directed to elements within Less-Restricted Subset 210, and optionally Restricted Subset 205, rather than merely to Restricted Subset 205. 9:45-48. These commands cause changes in Port 305A, such that communication from Access Device 230 is no longer blocked by ACL 340C and can now be received by elements of Less-restricted Subset 310. 9:53-57. FIG. 3B is a block diagram showing further details of Access Point 215, Router 220 and GateKeeper 225 of FIG. 2, after access has been granted to elements of Less-Restricted Subset 210, according to various embodiments of the invention. 9:62-67. If ACL 340A allows communication to network addresses associated with one or more elements of Less-Restricted Subset 210, the above reconfiguration of Port 305A results in a granting of access to Less-Restricted Subset 210 from Access Device 230.

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				10:3-8. Once Port 305A has been reconfigured to be associated with VLAN 310A, future general network traffic between Access Device 230 and Less-Restricted Subset 210 may pass through Ports 305A, 305D and 335A without passing through GateKeeper 225 or other elements of Restricted Subset 205. Further, communication related to access to security of Protected Network 200 may still be received by GateKeeper 225 via Port 305A. 10:10-14. For example, GateKeeper 225 may still receive control traffic such as DNS lookups or DHCP requests, or requests to access additional elements of Protected Network 200, or requests to continue to access the Less-Restricted Subset 210. 10:40-43. Finally, the reconfigured communication port is used to pass communication between Access Device 230 and one or more element of Less-Restricted Subset 210 in a Communicate Step 480. 10:63-66. As a result, any requests for access received from external devices are prevented from reaching Less-Restricted Subset 210 and instead are received by elements of Restricted Subset 205. 11:6-9. Restrict Port Step 420 is optional, for example when members of Ports 305A-305C have been configured to communicate data to elements of Restricted Subset 205 by an administrator of Access Point 215. 12:20-24. This communication port is reconfigured such that data received by the communication port is passed to one or more elements of Less-Restricted Subset 210 rather than merely elements of Restricted Subset 205 (e.g., GateKeeper 225).

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				12:48-52. In alternative embodiments, reconfiguring of members of ACL 340A-340D may be used to grant access to elements of Less-Restricted Subset 210 as an alternative to associating members of Ports 305A-305G to different members of VLANs 310A-310D. 12:53-56. Access Control 320 may selectively grant access to different parts of Protected Network 200 if ACL 340B is configured to allow access to different elements within Protected Network 200 than ACL 340A is configured. 12:61-66. When Port 305A is associated with VLAN 310A, as in FIG. 3B, communication from Access Device 230 is directed through Port 335A of Router 220 subject to ACL 340A and, thus, may access only those elements of Protected Network 200 allowed by ACL 340A. 12:66-13:3. When Port 305A is associated with VLAN 310B, communication from Access Device 230 is instead passed through Port 335B subject to ACL 340B and may access only those elements of Protected Network 200 permitted by ACL 340B. 13:29-32. In Communicate Step 480, communication occurs between Access Device 230 and elements of Less-Restricted Subset 210 via the communication port reconfigured in Reconfigure Port Step 470.
9.	EAP Protocol	'444 Patent: Claims 1A, 8 '450 Patent: Claim 7 '645 Patent: Claims 1C, 1[C-i], 2, 6	Indefinite, or limited to time of invention, otherwise indefinite	Expert Declaration and Testimony of Dr. Narasimha Reddy that this construction is indefinite, or is limited to time of invention, otherwise indefinite Intrinsic Evidence from U.S. Patent No. 7,523,484: 8:24-30. As is discussed further below, the commands received by Switch Logic 317 may be generated by

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				GateKeeper 225. This communication between GateKeeper 225 and Switch Logic 317 may be accomplished using SNMP (Simple Network Management Protocol), telnet, SSH (Secure Shell), RADIUS (Remote Authentication User Dial-In Service), EAP (Extensible Authentication Protocol), or the like. 12:35-40. These commands or responses to requests from Switch Logic 317 are optionally sent via SNMP, telnet, SSH, RADIUS, EAP, or the like, and are responsive to data received in Authenticate User Step 440 and Obtain Audit Data Step 450, and/or to the security audit performed in Apply Security Policy Step 460. 14:9-11. A client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP which relays them to the EAP server. 14:11-13. The EAP server then calls a server filter which sends the responses to the GK for evaluation. 14:20-23. There may be one or more instances of the CF and SF, which correspond to the separate EAP Authentication Modules (EAPM) that are supported. 14:27-28. The CF and SF APIs have APIs which correspond to the EAPM APIs. 14:28-31. Therefore, the EAP Client Layer (ECL) or EAP Server Layer (ESL) can call the CF and SF instances corresponding to a particular authentication method as shown in FIGS. 6A and 6B. 14:31-34. To the ECL and ESL, each instance of the CF and SF appears to be an EAPM which incorporates the functionality of the original EAPM prior to completion of the success response by the server EAPM.

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				14:39-41. This authentication method corresponds to an authentication method supported by one of the EAPMs. 14:42-44. The ECL calls the corresponding CF to perform authentication, which at first calls the appropriate EAPM to obtain the proper authentication response. 14:44-46. The authentication response is returned by the CF to the ESL, which sends the response to the server's ESL, SF, and EAPM. 14:46-49. This process continues until the authentication either succeeds or fails, at which time the server's authentication EAPM returns a success or failure response to the SF. 14:50-53. If the SF receives a success response from the server EAPM as shown in FIG. 7, the SF changes to the audit state and calls GK to obtain audit requests to send back to the client. 14:57-58. On the client, audit requests are passed to the agent API instead of to the client EAPM. 14:63-65. The ECL and ESL continue to communicate with the CF and SF, but instead of calling the EAPM, the CF and SF call the agent and GK respectively, to perform this exchange.
10.	monitor	'460 Patent: Claim 22	indefinite	Expert Declaration and Testimony of Dr. Narasimha Reddy that this term is indefinite Intrinsic Evidence from U.S. Patent No. 7,523,484: 7:19-22. For example, in one embodiment, Access Device 230 includes an agent configured to monitor code

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 66 of 1144
INFOEXPRESS, INC. - EX2572

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				running on Access Device 230 and report any suspicious code to GateKeeper 225. 7:22-26. In another example, Access Device 230 may include software and/or hardware configured to monitor other devices connected to Access Device 230 and to report information about these devices (e.g., their security statuses or MAC addresses) to GateKeeper 225. 11:52-55. For example, Access Device 230 may include a software agent configured to monitor local security and to report results of this monitoring to Policy Auditor 325.
11.	update the access device	'460 Patent: Claim 27	indefinite	Expert Declaration and Testimony of Dr. Narasimha Reddy that this term is indefinite Intrinsic Evidence from U.S. Patent No. 7,523,484: 6:6-11. In some embodiments, Restricted Subset 205 further includes a DHCP (dynamic host configuration protocol service) 260 configured to assign and manage network addresses, and/or an Update Module 255 configured for providing security updates to Access Device 230. 6:14-16. In one embodiment, Restricted Subset 205 includes a single computing device configured to function as both Update Module 255 and GateKeeper 225. 7:39-41. Update Module 255 is configured for remotely modifying Access Device 230, or a device connected to Access Device 230, in order to improve compliance with a security policy. 7:41-45. For example, if it is found that Access Device 230 includes out-of-date antivirus software, then Update Module 255 may facilitate updating of the antivirus software on Access Device 230.

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				7:45-46. In some embodiments, Update Module 255 is configured to update an agent executing on Access Device 230. 7:46-50. Update Module 255 is optionally included in Less-Restricted Subset 210 or external to Protected Network 200. Update Module 255 optionally operates responsive to a security policy and/or to GateKeeper 225. 12:13-16. For example, in one embodiment, Apply Security Policy Step 460 includes updating antivirus software on Access Device 230 in response to a security audit that determined that the current antivirus software is out-of-date.
12.	and that concerns antivirus software	'350 Patent: Claim 9	indefinite	Expert Declaration and Testimony of Dr. Narasimha Reddy that this term is indefinite Intrinsic Evidence from U.S. Patent No. 7,523,484: 6:41-48. For example, in one embodiment GateKeeper 225 is configured to enforce a security policy that requires a user of Access Device 230 to provide a username and password, requires Access Device 230 to be running an operating system with specific security patches installed, requires that Access Device 230 not be connected to any insecure devices, and requires that Access Device 230 have current antivirus software installed. 7:42-45. For example, if it is found that Access Device 230 includes out-of-date antivirus software, then Update Module 255 may facilitate updating of the antivirus software on Access Device 230. 11:44-50. The requested system data may include, for example, operating system status (version, updates, etc.),

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				antivirus software status, information concerning devices connected to Access Device 230, Windows registry information, MAC address, IP addresses, cookies, status of applications executing on Access Device 230, or the like. 12:12-16. For example, in one embodiment, Apply Security Policy Step 460 includes updating antivirus software on Access Device 230 in response to a security audit that determined that the current antivirus software is out-of-date.

InfoExpress's Preliminary Claim Construction

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
1.	"configured to reconfigure the communication device" "reconfiguring [an/the] access point" "wherein the access point is reconfigured" "configuring [an/the] access point"	'484 Patent: Claim 1 '350 Patent: Claims 1, 18 '350 Patent: Claim 4 '450 Patent: Claims 1, 3, 4, 22; '444 Patent: Claims 2, 3, 4, 5, 7, 22; '645 Patent: Claim 1	plain and ordinary meaning	Expert Declaration and Testimony of Dr. Narasimha Reddy that this construction is plain and ordinary Intrinsic Evidence from U.S. Patent No. 7,523,484: Abstract: A new approach to network security includes manipulating an access point such that an initial communication from an external device is passed to a restricted subset of a computing network including a gatekeeper. **The gatekeeper is configured to enforce a security policy against the external device before granting access to a less-restricted subset of the computing network. If requirements of the security policy are satisfied, then the gatekeeper reconfigures the access point such that further communication from the external device may be received by elements of the less-restricted subset**. Enforcement of the security policy optionally includes performing a security audit of the external device. 3:60-4:9: Various embodiments of the invention include a network gatekeeper comprising at least one security policy including requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network, a policy auditor configured to audit an access device using the at least one security policy, in response to a request to access the less-restricted subset of the

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				protected network, the request being sent from the access device to the gatekeeper via a communication device, and **an access control configured to reconfigure the communication device such that data sent from the access device can be received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected** network, if the audit results in a determination that the access device meets the requirements of the at least one security policy, the restricted subset of the protected network including the gatekeeper. Other elements are optional. 11:10-30: In Receive Access Request Step 430, a request for access to Less-Restricted Subset 210 is received at one of Ports 305A-305C configured to pass data to DHCP 260 and Gatekeeper 225. Typically, this request is received from an external device such as Access Device 230. Because Port 305A, Port 305B and Port 305C are configured to pass data to DHCP 260 and Gatekeeper 225, the received access request passes through Access Point 215 and is received by either DHCP 260 or Gatekeeper 225 In typical embodiments, an initial access request is first acknowledged by DHCP 260 which assigns a dynamic network address (e.g., IP address) to Access Device 230 and returns, to Access Device 230, a network address associated with GateKeeper 225 or more specifically Policy Auditor 325. Using this network address, Access Device 230 may engage in further communication with GateKeeper 225 or Policy Auditor 325. **In some embodiments, DHCP 260 and instances of GateKeeper 225 are associated with a local domain name service**

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				configured to provide network addresses associated with a particular instance of GateKeeper 225 configured to manage (reconfigure) the particular Access Point 215 to which Access Device 230 is connected.
2.	"reconfiguring a port on the communication device" "reconfiguring the communication port" "configuring the communication port" "configured to reconfigure the communication port" "configured for reconfiguring the communication port"	'484 Patent: Claim 20 '484 Patent: Claims 27, 28, 41, 71; '460 Patent: Claims 1, 16, 22 '484 Patent: Claims 57, 58 '484 Patent: Claim 57 '484 Patent: Claim 82	plain and ordinary meaning	Expert Declaration and Testimony of Dr. Narasimha Reddy that this construction is plain and ordinary Intrinsic Evidence from U.S. Patent No. 7,523,484: 2:48-61: Systems and methods of the invention include a protected network physically or logically divided into a restricted subset and one or more less-restricted subsets. Requests from an access device for access to the less-restricted subset are first passed to the restricted subset. Elements (e.g., a gatekeeper) of the restricted subset are then used to apply security policies to the access device and if security policies are satisfied, the access device is granted access to a less-restricted subset of the protected network. **The passing of access requests to the restricted subset and granting of access are accomplished by configuring and reconfiguring a communication port of an access point.** After access is granted, further communication between the access device and the protected network can include access to the less restricted subset. 5:29-50: Access to a protected computing network is controlled by manipulating a communication port

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				within an access point. **When an access request is first received, the communication port is configured to pass the request to a restricted subset of a protected computing network**. This restricted subset includes a gatekeeper configured to administer a security policy governing access to those parts of the protected computing network that are not part of the restricted subset. Those parts of the protected computing network that are not part of the restricted network are considered to be in a less-restricted subset. The less-restricted subset being less restricted relative to the restricted subset in terms of what elements may be included in each subset. If the device requesting access satisfies requirements of the security policy, then the gatekeeper sends commands to the access point in order to reconfigure the communication port through which the access request was received. **The communication port is reconfigured such that further communication from the access device is passed to the less-restricted subset as well as, optionally, the restricted subset**. In some embodiments, the less-restricted subset and the restricted subset are characterized by VLANs defined within the protected network. 6:62-7:6: In some embodiments, a single instance of GateKeeper 225 is configured to manage access through more than one Access Point 215 and/or to manage access to more than one Protected Network 200. **As is described further herein, management**

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				of Access Point 215 is accomplished by configuring and reconfiguring one or more communication ports within Access Point 215, and optionally setting access control lists within Router 220. In some embodiments Protected Network 200 includes a plurality of Access Point 215, a plurality of GateKeeper 225 and/or a plurality of Restricted Subset 205. Further details of GateKeeper 225 and Access Point 215 are discussed below. 10:26-46: FIG. 4 is a flowchart illustrating a method of granting access to Less-Restricted Subset 210 (FIG. 2), according to various embodiments of the invention. In these embodiments, an Update Port Log Step 410 and a Restrict Port Step 420 are used to prepare an open (unused) communication port on Access Point 215 for receiving a request for access to Less-Restricted Subset 210. This request is received from Access Device 230 in a Receive Access Request Step 430. In response, GateKeeper 225 authenticates a user, obtains audit data, and applies a security policy in an Authenticate User Step 440, an Obtain Audit Data Step 450 and an Apply Security Policy Step 460, respectively. If the security policy is satisfied, then in a Reconfigure Port Step 470, **GateKeeper 225 reconfigures the communication port of Access Point 215 to which Access Device 230 has connected**. Finally, the reconfigured communication port is used to pass communication between Access Device 230 and one

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				or more element of Less-Restricted Subset 210 in a Communicate Step 480. Further details of these steps are discussed herein. 10:55-11:9: In Restrict Port Step 420, Access Control 320 configures those members of Ports 305A-305G that may be accessed by external devices, such as Access Device 230. **These communication ports are configured to be associated with VLAN 310C such that any data (e.g., communications) they receive from external devices are directed to Port 305F** and, thus, to subject to ACL 340C. ACL 340C is configured to allow communication to, for example, DHCP 260 and GateKeeper 225. As a result, any requests for access received from external devices are prevented from reaching Less-Restricted Subset 210 and instead are received by elements of Restricted Subset 205. Restrict Port Step 420 results in a configuration such as that illustrated in FIG. 3A. In this configuration, those members of Ports 305A-305G that may be accessed by external devices include Port 305A, Port 305B and Port 305C. As a result of Restrict Port Step 420, these members of Ports 305A-305G are associated with VLAN 310C and communicatively coupled to Protected Network 200 through ACL 340C. Restrict Port Step 420 is optional, for example when members of Ports 305A-305C have been configured to communicate data to elements of Restricted Subset 205 by an administrator of Access Point 215.

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				12:17-32: In Reconfigure Port Step 470, the communication port of Access Point 215, to which Access Device 230 is communicatively connected, is reconfigured responsive to a successful security audit in Apply Security Policy Step 460. **This communication port is reconfigured such that data received by the communication port is passed to one or more elements of Less-Restricted Subset 210 rather than merely elements of Restricted Subset 205 (e.g., GateKeeper 225).** For example, FIG. 3A shows Port 305A prior to execution of Reconfigure Port Step 470 and FIG. 3B shows Port 305A following execution of Reconfigure Port Step 470. In FIG. 3B, Port 305A is associated with VLAN 310A and, thus, communicatively coupled through Port 305D to Protected Network 200 subject to the restrictions of ACL 340A. The restrictions of ACL 340A allow access to all or part of Less-Restricted Subset 210, as well as optionally all or part of Restricted Subset 205. 13:10-28: As illustrated in the above example, a member of Ports 305A-305G, through which Access Device 230 is requesting access, may be reconfigured to more than one alternative setting in Reconfigure Port Step 470. **For example, in various embodiments a communication port may be reconfigured to a prior administrator specified configuration previously read in Update Port Log Step 410**, reconfigured to be linked to a specific port

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				responsive to the request received in Receive Access Request Step 430, reconfigured to grant access to a particular part of Less-Restricted Subset 210, reconfigured to a default setting, and/or the like. By reading administrator specified port configurations in Update Port Log Step 410 and **reconfiguring communication ports back to these read configurations in Reconfigure Port Step 470**, an administrator may reconfigure Protected Network 200 without concern that their specifications will be lost or permanently overwritten by methods of the invention. In embodiments wherein a communication port is not reconfigured to a previous administrator specified configuration, Update Port Log Step 410 is optional.
3.	"access point"	'484 Patent: Claims 16, 17, 27, 28, 33, 34, 35, 41, 48, 49, 50, 62, 82; '460 Patent: Claims 1, 10, 11, 12, 16; '450 Patent: Claims 1, 3, 4, 16, 22; '444 Patent: Claims 1–5, 7, 22; '350 Patent: Claim 1, 4, 18; '645 Patent: Claim 1	plain and ordinary meaning	Expert Declaration and Testimony of Dr. Narasimha Reddy that this construction is plain and ordinary Intrinsic Evidence from U.S. Patent No. 7,523,484: 1:64-2:13: **Each instance of Access Point 120 may include a large number of individual communication ports**. These ports are used to connect through GateKeeper 110 to other elements within Secure Network 100 such as File Server 130 or LAN 125. Large corporate networks may include many instances of Access Point 120, each including hundreds of

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				individual communication ports and being associated with an instance of GateKeeper 110. **Some instances of Access Point 120 are capable of supporting virtual local area networks (VLANs).** VLANs are generated by associating communication ports within Access Point 120 with separate virtual networks. For example, one Access Device 160 may be placed on a different VLAN than another Access Device 160 by assigning the communication ports of Access Point 120 to separate VLANs. From the point of view of these devices, the effect of a VLAN is equivalent to having a separate hardwired network. 2:26-42: A disadvantage of the use of GateKeeper 110, as practiced in the prior art, is that all communications between Access Device 160 and LAN 125 pass through GateKeeper 110. **For large networks including many instances of Access Point 120, each of which may include many communication ports, this can be a significant burden**. The use of one instance of GateKeeper 110 to support numerous instances of Access Device 160 is limited by bandwidth and required sophistication (e.g., cost) of GateKeeper 110. It is undesirable for GateKeeper 110 to become a limiting factor on the bandwidth of communication between instances of Access Device 160 and Secure Network 100. Further, the use of a separate GateKeeper 110 for each instance of Access Device 160 or Access Point 120 is often prohibitively expensive. Even if a separate

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				GateKeeper is used for each Access Point 120, there is no isolation between compliant and non-compliant Access Devices 160 which are attached to the same Access Point 120. 5:51-67: FIG. 2 is a block diagram of a Protected Network 200, according to various embodiments of the invention. Protected Network 200 is either physically or logically divided into a Restricted Subset 205 and a Less-Restricted Subset 210. **Access to Protected Network 200 is possible through an Access Point 215 (a communication device) and an optional Router 220**. As is described further herein this access is under the control of a GateKeeper 225. GateKeeper 225 is configured to enforce a security policy against one or more Access Device 230 requesting access to Less-Restricted Subset 210. **Typically, Less-Restricted Subset 210 and Restricted Subset 205 are characterized by VLAN settings within Access Point 215**. Access Device 230 and Access Point 215 are connected by a communication channel such as a cable, the Internet, a telephone network, other computing network, and/or the like. **In some embodiments, a network access server (not shown) is included between Access Device 230 and Access Point 215**. 7:51-61: **FIG. 3A is a block diagram showing further details of Access Point 215, Router 220 and GateKeeper 225, according to various**

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				embodiments of the invention. Access Point 215 is, for example, a network switch, a wireless access point, a remote access virtual private network (VPN), secure socket layer VPN, firewall, or the like. When embodied in a network switch, Access Point 215 includes a series of communication ports, designated Ports 305A-305G and configured for communication with devices such as Access Device 230, Router 220, Less-Restricted Subset 210 and/or Restricted Subset 205. 9:3-19: **When Access Point 215 is embodied in a wireless access point, some or all of Ports 305A-305G may be wireless connections rather than physical ports**. In these embodiments, Lines 315 may represent logical associations used to control data flow between wireless connections to Access Point 215 and/or members of Ports 305A-305G that are physical communication ports. For example, in some embodiments, MAC addresses are used to distinguish wireless communications from different instances of Access Device 230 and the logical associations (represented by Lines 315) are used to direct these communications to various output channels. The output channels may be other wireless connections or physical members of Ports 305A-305G. These logical associations may be altered by Switch Logic 317 just as associations with members of VLANs 310A-310D are modified. **Therefore, the teachings herein that use a network switch as an**

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				example of Access Point 215, apply equally to wireless access points. 10:26-11:50: FIG. 4 is a flowchart illustrating a method of granting access to Less-Restricted Subset 210 (FIG. 2), according to various embodiments of the invention. **In these embodiments, an Update Port Log Step 410 and a Restrict Port Step 420 are used to prepare an open (unused) communication port on Access Point 215 for receiving a request for access to Less-Restricted Subset 210**. This request is received from Access Device 230 in a Receive Access Request Step 430. In response, GateKeeper 225 authenticates a user, obtains audit data, and applies a security policy in an Authenticate User Step 440, an Obtain Audit Data Step 450 and an Apply Security Policy Step 460, respectively. If the security policy is satisfied, then in a Reconfigure Port Step 470, **GateKeeper 225 reconfigures the communication port of Access Point 215 to which Access Device 230 has connected**. Finally, the reconfigured communication port is used to pass communication between Access Device 230 and one or more element of Less-Restricted Subset 210 in a Communicate Step 480. Further details of these steps are discussed herein. **In Update Port Log Step 410, Access Control 320 reads port configuration data from Access Point 215 to determine the current configuration of Ports 305A-305G**. If any of Ports 305A-305G have been configured by an administrator of Access Point

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				215, then in Update Port Log Step 410 the administrator specified configuration(s) are stored for later use during Reconfigure Port Step 470. Typically, the read configuration data is stored in a port configuration table, for example within GateKeeper 225. Update Port Log Step 410 is optional, as discussed further herein. In Restrict Port Step 420, Access Control 320 configures those members of Ports 305A-305G that may be accessed by external devices, such as Access Device 230. These communication ports are configured to be associated with VLAN 310C such that any data (e.g., communications) they receive from external devices are directed to Port 305F and, thus, to subject to ACL 340C. ACL 340C is configured to allow communication to, for example, DHCP 260 and GateKeeper 225. As a result, any requests for access received from external devices are prevented from reaching Less-Restricted Subset 210 and instead are received by elements of Restricted Subset 205. Restrict Port Step 420 results in a configuration such as that illustrated in FIG. 3A. In this configuration, those members of Ports 305A-305G that may be accessed by external devices include Port 305A, Port 305B and Port 305C. As a result of Restrict Port Step 420, these members of Ports 305A-305G are associated with VLAN 310C and communicatively coupled to Protected Network 200 through ACL 340C. **Restrict Port Step 420 is optional, for example when members of Ports 305A-305C have been configured to communicate**

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				data to elements of Restricted Subset 205 by an administrator of Access Point 215. In Receive Access Request Step 430, a request for access to Less-Restricted Subset 210 is received at one of Ports 305A-305C configured to pass data to DHCP 260 and Gatekeeper 225. Typically, this request is received from an external device such as Access Device 230. Because Port 305A, **Port 305B and Port 305C are configured to pass data to DHCP 260 and Gatekeeper 225, the received access request passes through Access Point 215** and is received by either DHCP 260 or Gatekeeper 225 In typical embodiments, an initial access request is first acknowledged by DHCP 260 which assigns a dynamic network address (e.g., IP address) to Access Device 230 and returns, to Access Device 230, a network address associated with GateKeeper 225 or more specifically Policy Auditor 325. Using this network address, Access Device 230 may engage in further communication with GateKeeper 225 or Policy Auditor 325. In some embodiments, **DHCP 260 and instances of GateKeeper 225 are associated with a local domain name service configured to provide network addresses associated with a particular instance of GateKeeper 225 configured to manage (reconfigure) the particular Access Point 215 to which Access Device 230 is connected.** 15:21-36: Several embodiments are specifically illustrated and/or described herein. However, it will be

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				appreciated that modifications and variations are covered by the above teachings and within the scope of the appended claims without departing from the spirit and intended scope thereof. For example, the teachings herein may be applied to embodiments **wherein Access Point 215 is a wireless access point and MAC addresses, or the like, are used instead of VLANs to separate traffic from different instances of Access Device 230**. It is, thus, anticipated that network management techniques other than VLANs may be used to distinguish Less-Restricted Subset 210 from Restricted Subset 205. In some embodiments, **various aspects of GateKeeper 225 may be incorporated into Access Point 215 and/or Router 220**. GateKeeper 225 and Policy Manager 250 are each optionally implemented on a plurality of computing devices within Restricted Subset 205.
4.	"associating the communication port with a VLAN" "wherein configuring the access point includes assigning a VLAN"	'484 Patent: Claim 58 '450 Patent: Claim 4; '444 Patent: Claim 4	plain and ordinary meaning	Expert Declaration and Testimony of Dr. Narasimha Reddy that this construction is plain and ordinary Intrinsic Evidence from U.S. Patent No. 7,523,484: 3:43-59: Various embodiments of the invention include a computing network comprising a less-restricted subset of the computing network, access to the less-restricted subset being responsive to a first VLAN, a restricted subset of the computing network including a gatekeeper, the gatekeeper configured to receive requests for access to the less-restricted subset from an access device and to issue commands configured

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				to allow access to the less-restricted subset, access to the restricted subset of the computing network being responsive to a second VLAN, and at least one access point including a communication port configurable for communication with the less-restricted subset or alternatively for communication with only the restricted subset, **configuration of the communication port including association of the communication port alternatively with the first VLAN or the second VLAN, configuration of the communication port being responsive to the commands issued by the gatekeeper**. Other elements are optional. 5:51-67: FIG. 2 is a block diagram of a Protected Network 200, according to various embodiments of the invention. Protected Network 200 is either physically or logically divided into a Restricted Subset 205 and a Less-Restricted Subset 210. Access to Protected Network 200 is possible through an Access Point 215 (a communication device) and an optional Router 220. As is described further herein this access is under the control of a GateKeeper 225. GateKeeper 225 is configured to enforce a security policy against one or more Access Device 230 requesting access to Less-Restricted Subset 210. Typically, **Less-Restricted Subset 210 and Restricted Subset 205 are characterized by VLAN settings within Access Point 215**. Access Device 230 and Access Point 215 are connected by a communication channel such as a cable, the Internet,

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				a telephone network, other computing network, and/or the like. In some embodiments, a network access server (not shown) is included between Access Device 230 and Access Point 215. 7:62-8:23: Communication received at one member of Ports 305A-305G is directed internally to another member of Ports 305A-305G via a member of VLANs 310A-310D. **VLANs 310A-310D are logical associations between members of Ports 305A-305G**. **Typically, any members of Ports 305A-305G that are configured to be associated with the same member of VLANs 310A-310D are in bi-directional communication with each other**. These associations are illustrated in FIGS. 3A and 3B by Lines 315. For example, with Ports 305A-305G configured as shown in FIG. 3A, **communication from Access Device 230 and received at Port 305A is directed to Port 305F because Port 305A and Port 305F are both associated with VLAN 310C**. (In some embodiments of Access Point 215, a member of VLANs 310A-310D may be configured such that some members of Ports 305A-305G, even if associated with the same VLAN, are hidden from each other. For example, in these embodiments, both Ports 305A and 305B may be in communication with Port 305F but not with each other.) **The associations between members of Ports 305A-305G and VLANs 310A-310D are controlled by Switch Logic 317 which is accessible to other devices, for example through**

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				Port 305G. Switch Logic 317 is configured for configuring and reconfiguring members of Ports 305A-305G responsive to received commands. For example, by receiving an appropriate command, Switch Logic 317 is configured to reconfigure Port 305A to be associated with VLAN 310A, as illustrated in FIG. 3B below. In this configuration, data received at Port 305A is directed to Port 305D via VLAN 310A, rather than to Port 305F. 8:53-9:2: ACL 340A-340D of Router 220 may be used to limit communication from Access Device 230 to specific elements of Protected Network 200. For example, in the embodiments illustrated by FIG. 3A, if ACL 340C is configured to restrict communication to Restricted Subset 205, **and Ports 305A-305C are associated with VLAN 310C as indicated by Lines 315, then communication via these members of Ports 305A-305G will be restricted to Restricted Subset 205**. In typical embodiments, at least one member of ACL 340A-340D is configured to allow communication to Restricted Subset 205 but not to Less-Restricted Subset 210. As is discussed further herein, by reconfiguring a member of Ports 305A-305C to be associated with a different member of VLANs 310A-310D, not subject to the filtering of ACL 340C, communications from Access Device 230 can be directed to elements within Less-Restricted Subset 210, and optionally Restricted Subset 205, rather than merely to Restricted Subset 205.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 87 of 1144
INFOEXPRESS, INC. - EX2572

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				9:53-10:25: FIG. 3B is a block diagram showing further details of Access Point 215, Router 220 and GateKeeper 225 of FIG. 2, after access has been granted to elements of Less-Restricted Subset 210, according to various embodiments of the invention. **Port 305A has been reconfigured to be associated with VLAN 310A rather than VLAN 310C**. Because VLAN 310A is communicatively coupled to Port 305D and Port 335A (of Router 220) via ACL 340A, any communication received at Port 305A from Access Device 230 is now subject to the filtering effects of ACL 340A rather than ACL 340C. If ACL 340A allows communication to network addresses associated with one or more elements of Less-Restricted Subset 210, the above reconfiguration of Port 305A results in a granting of access to Less-Restricted Subset 210 from Access Device 230. In some embodiments, if ACL 340A is configured to allow access to members of Less-Restricted Subset 210 it is also configured to allow access to members of Restricted Subset 205. Once Port 305A has been reconfigured to be associated with VLAN 310A, future general network traffic between Access Device 230 and Less-Restricted Subset 210 may pass through Ports 305A, 305D and 335A without passing through GateKeeper 225 or other elements of Restricted Subset 205. Further, communication related to access to security of Protected Network 200 may still be received by GateKeeper 225 via Port 305A. For example, GateKeeper 225 may still receive control traffic such as DNS lookups or

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				DHCP requests, or requests to access additional elements of Protected Network 200, or requests to continue to access the Less-Restricted Subset 210. In some embodiments, members of VLAN 310A-310D and ACL 340A-340D are optionally used to grant or bar access to different subsets of Protected Network 200, Less-Restricted Subset 210, or Restricted Subset 205. For example, ACL 340B may be configured to grant access to File Server 235, Policy Manager 250 and GateKeeper 225. **In this case, associating a member of Ports 305A-305C with VLAN 310B may provide access to these devices from an instance of Access Device 230**. Granting of access to a specific region of Less-Restricted Subset 210 is optionally responsive to which member of Security Policies 330A-330B has been satisfied. 10:55-11:9: In Restrict Port Step 420, Access Control 320 configures those members of Ports 305A-305G that may be accessed by external devices, such as Access Device 230. **These communication ports are configured to be associated with VLAN 310C such that any data (e.g., communications) they receive from external devices are directed to Port 305F** and, thus, to subject to ACL 340C. ACL 340C is configured to allow communication to, for example, DHCP 260 and GateKeeper 225. As a result, any requests for access received from external devices are prevented from reaching Less-Restricted Subset 210 and instead are received by elements of

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				Restricted Subset 205. Restrict Port Step 420 results in a configuration such as that illustrated in FIG. 3A. In this configuration, those members of Ports 305A-305G that may be accessed by external devices include Port 305A, Port 305B and Port 305C. **As a result of Restrict Port Step 420, these members of Ports 305A-305G are associated with VLAN 310C and communicatively coupled to Protected Network 200 through ACL 340C**. Restrict Port Step 420 is optional, for example when members of Ports 305A-305C have been configured to communicate data to elements of Restricted Subset 205 by an administrator of Access Point 215. 12:17-13:9: In Reconfigure Port Step 470, the communication port of Access Point 215, to which Access Device 230 is communicatively connected, is reconfigured responsive to a successful security audit in Apply Security Policy Step 460. This communication port is reconfigured such that data received by the communication port is passed to one or more elements of Less-Restricted Subset 210 rather than merely elements of Restricted Subset 205 (e.g., GateKeeper 225). For example, FIG. 3A shows Port 305A prior to execution of Reconfigure Port Step 470 and FIG. 3B shows Port 305A following execution of Reconfigure Port Step 470**. In FIG. 3B, Port 305A is associated with VLAN 310A and, thus, communicatively coupled through Port 305D to Protected Network 200 subject to the restrictions of ACL 340A**. The restrictions of ACL

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				340A allow access to all or part of Less-Restricted Subset 210, as well as optionally all or part of Restricted Subset 205. In typical embodiments, reconfiguration of Port 305A is accomplished by sending commands from Access Control 320 to Switch Logic 317. These commands or responses to requests from Switch Logic 317 are optionally sent via SNMP, telnet, SSH, RADIUS, EAP, or the like, and are responsive to data received in Authenticate User Step 440 and Obtain Audit Data Step 450, and/or to the security audit performed in Apply Security Policy Step 460. **In response to these commands, Switch Logic 317 configures Port 305A to be associated with VLAN 310A and, thus, communicate through Port 305D.** While access control lists (ACL 340A-340D) within Router 220 are typically configured prior to Receive Access Request Step 430, in some embodiments, Reconfigure Port Step 470 further includes configuring one or more members of ACL 340A-340D. **In alternative embodiments, reconfiguring of members of ACL 340A-340D may be used to grant access to elements of Less-Restricted Subset 210 as an alternative to associating members of Ports 305A-305G to different members of VLANs 310A-310D.** Access Control 320 may selectively grant access to different parts of Protected Network 200 if ACL 340B is configured to allow access to different elements within Protected Network 200 than ACL 340A is configured. For example, in one

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				embodiment, Access Device 230 will receive access to all of Less-Restricted Subset 210 if Port 305A is associated with VLAN 310A, or alternatively Access Device 230 will receive access to only a part of Less-Restricted Subset 210 if Port 305A is associated with VLAN 310B. When Port 305A is associated with VLAN 310A, as in FIG. 3B, communication from Access Device 230 is directed through Port 335A of Router 220 subject to ACL 340A and, thus, may access only those elements of Protected Network 200 allowed by ACL 340A. **When Port 305A is associated with VLAN 310B, communication from Access Device 230 is instead passed through Port 335B subject to ACL 340B and may access only those elements of Protected Network 200 permitted by ACL 340B**. A selection between granting access to a first or second part of Protected Network 200 can, therefore, be made using Access Control 320. The selection is optionally responsive to the security policy used in Apply Security Policy Step 460, to whether the security policy was fully or partially satisfied, to data obtained in Authenticate User Step 440 or Obtain Audit Data Step 450, or the like.
5.	"the applying of the security policy taking place under control of the gatekeeper" "a gatekeeper stored in memory and executable to: . . .	'444 Patent: Claim 1, 22 '645 Patent: Claim 1 '484 Patent: Claims 27, 28, 41, 43, 66, 68, 82; '460 Patent: Claims 1, 3, 5, 16, 18, 20; '450	plain and ordinary meaning	Expert Declaration and Testimony of Dr. Narasimha Reddy that this construction is plain and ordinary Intrinsic Evidence from U.S. Patent No. 7,523,484: 1:53-63: A greater level of access control may be achieved by including a gatekeeper between the secure network

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
	evaluate device information received from the device in response to the audit request" "applying a security policy" "application of the security policy"	Patent: Claims 1, 2, 16, 22; '444 Patent: Claims 1, 2, 22 '450 Patent: Claims 1, 16, 22		and the access device. **The gatekeeper is configured to ensure that the access device conforms to a predetermined security policy**. FIG. 1 is a block diagram of a Secure Network, generally designated 100, including two instances of a Gatekeeper 110 each associated with a different instance of an Access Point 120. Secure Network 100 further includes, as an illustrative example, a network File Server 130, a Network PC (personal computer) 140 and a Printer 150 included in and connected via, a local area network designated LAN 125. 2:14-25: GateKeeper 110 is configured to control access to Secure Network 100. In addition to authenticating users who wish to access Secure Network 100 using an Access Device 160, **GateKeeper 110 is configured to ensure that Access Device 160 conforms to a predetermined security policy, before granting access to Secure Network 100**. For example, GateKeeper 110 may make certain that Access Device 160 has up-to-date virus software and encryption protocols as proscribed by the security policy. Once GateKeeper 110 has verified that Access Device 160 satisfies the security policy, Access Device 160 is allowed to communicate through GateKeeper 110 to LAN 125. 4:10-23: Various embodiments of the invention include a method of granting access to a protected network,

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				the method comprising receiving a request for access to a less-restricted subset of the protected network from an access device external to the protected network, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and **a restricted subset of the protected network, the restricted subset including a gatekeeper, applying a security policy to the access device, responsive to the request, and reconfiguring the communication port for communicating between the access device and the less-restricted subset of the protected network**, if requirements of the security policy are satisfied. Other steps are optional. 5:51-67: FIG. 2 is a block diagram of a Protected Network 200, according to various embodiments of the invention. Protected Network 200 is either physically or logically divided into a Restricted Subset 205 and a Less-Restricted Subset 210. Access to Protected Network 200 is possible through an Access Point 215 (a communication device) and an optional Router 220. As is described further herein this access is under the control of a GateKeeper 225. **GateKeeper 225 is configured to enforce a security policy against one or more Access Device 230 requesting access to Less-Restricted Subset 210**. Typically, Less-Restricted Subset 210 and Restricted Subset 205 are characterized by VLAN settings within Access Point 215. Access Device 230

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				and Access Point 215 are connected by a communication channel such as a cable, the Internet, a telephone network, other computing network, and/or the like. In some embodiments, a network access server (not shown) is included between Access Device 230 and Access Point 215. 6:34-48: **GateKeeper 225 is configured to enforce one or more security policies against an instance of Access Device 230 attempting to access Protected Network 200**. The security polices may include requirements for user identification such as user names and passwords, configuration requirements relating to the configuration of Access Device 230, application requirements relating to applications running on Access Device 230, or the like. **For example, in one embodiment GateKeeper 225 is configured to enforce a security policy that requires a user of Access Device 230 to provide a username and password, requires Access Device 230 to be running an operating system with specific security patches installed**, requires that Access Device 230 not be connected to any insecure devices, and requires that Access Device 230 have current antivirus software installed. 10:26-44: FIG. 4 is a flowchart illustrating a method of granting access to Less-Restricted Subset 210 (FIG. 2), according to various embodiments of the invention. In these embodiments, an Update Port

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				Log Step 410 and a Restrict Port Step 420 are used to prepare an open (unused) communication port on Access Point 215 for receiving a request for access to Less-Restricted Subset 210. This request is received from Access Device 230 in a Receive Access Request Step 430. In response, **GateKeeper 225 authenticates a user, obtains audit data, and applies a security policy in an Authenticate User Step 440, an Obtain Audit Data Step 450 and an Apply Security Policy Step 460, respectively.** If the security policy is satisfied, then in a Reconfigure Port Step 470, GateKeeper 225 reconfigures the communication port of Access Point 215 to which Access Device 230 has connected. Finally, the reconfigured communication port is used to pass communication between Access Device 230 and one or more element of Less-Restricted Subset 210 in a Communicate Step 480. Further details of these steps are discussed herein. 11:56-12:43: **In Apply Security Policy Step 460, a security audit of Access Device 230 is performed by Policy Auditor 325 responsive to a member of Security Policy 330A or Security Policy 330B**. The particular member of Security Policy 330A or Security Policy 330B used to perform the audit may be responsive to the identity of Access Device 230, an identity of a user of Access Device 230, a part of Less-Restricted Subset 210 to which access is requested, or the like. The security audit typically includes determining if Access Device 230 satisfies

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				requirements of the security policy. The security audit optionally includes active probing, scanning, and/or collection of third party data regarding Access Device 230. In some embodiments, Authenticate User Step 440 is considered part of the security policy audit. As is discussed further herein, in some embodiments, satisfaction of all the requirements of a particular security policy results in access to Less-Restricted Subset 210, while satisfaction of a subset of the requirements associated with the particular security policy is considered partial satisfaction of the security policy and may result in a more limited access to Less-Restricted Subset 210. In some embodiments, **Apply Security Policy Step 460 includes using Update Module 255 (FIG. 2) to overcome deficiencies in the security of Access Device 230**. For example, in one embodiment, Apply Security Policy Step 460 includes updating antivirus software on Access Device 230 in response to a security audit that determined that the current antivirus software is out-of-date. **In Reconfigure Port Step 470, the communication port of Access Point 215, to which Access Device 230 is communicatively connected, is reconfigured responsive to a successful security audit in Apply Security Policy Step 460**. This communication port is reconfigured such that data received by the communication port is passed to one or more elements of Less-Restricted Subset 210 rather than merely elements of Restricted Subset 205

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				(e.g., GateKeeper 225). For example, FIG. 3A shows Port 305A prior to execution of Reconfigure Port Step 470 and FIG. 3B shows Port 305A following execution of Reconfigure Port Step 470. In FIG. 3B, Port 305A is associated with VLAN 310A and, thus, communicatively coupled through Port 305D to Protected Network 200 subject to the restrictions of ACL 340A. The restrictions of ACL 340A allow access to all or part of Less-Restricted Subset 210, as well as optionally all or part of Restricted Subset 205. In typical embodiments, reconfiguration of Port 305A is accomplished by sending commands from Access Control 320 to Switch Logic 317. **These commands or responses to requests from Switch Logic 317 are optionally sent via SNMP, telnet, SSH, RADIUS, EAP, or the like, and are responsive to data received in Authenticate User Step 440 and Obtain Audit Data Step 450, and/or to the security audit performed in Apply Security Policy Step 460**. In response to these commands, Switch Logic 317 configures Port 305A to be associated with VLAN 310A and, thus, communicate through Port 305D. 14:50-67: If the SF receives a success response from the server EAPM as shown in FIG. 7, **the SF changes to the audit state and calls GK to obtain audit requests to send back to the client**. In this state, the SF returns specially formatted audit requests to the ESL which are passed to the ECL, and eventually to the

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				CF which sends back audit responses to the SF requests. **On the client, audit requests are passed to the agent API instead of to the client EAPM**. The agent returns information about the local system, which is converted to audit responses that are sent to the server. During the audit state, the SF and CF **exchange audit requests and responses about the EP** as shown in FIGS. 8A and 8B. The ECL and ESL continue to communicate with the CF and SF, but instead of calling the EAPM, the CF and SF call the agent and GK respectively, to perform this exchange. The audit session continues until the necessary audit information has been passed to the SF.
6.	"system data"	'484 Patent: Claims 4, 5, 43, 66, 68; '460 Patent: Claims 3, 4, 5, 6, 18, 19, 20, 21	plain and ordinary meaning	Expert Declaration and Testimony of Dr. Narasimha Reddy that this construction is plain and ordinary Intrinsic Evidence from U.S. Patent No. 7,523,484: 11:39-50: In optional Obtain Audit Data Step 450, Policy Auditor 325 collects further data to perform a security audit of Access Device 230 responsive to Security Policy 330A or Security Policy 330B. In some embodiments, **Obtain Audit Data Step 450 includes sending system data requests to Access Device 230, Router 220, or Access Point 215**. **The requested system data may include, for example, operating system status (version, updates, etc.), antivirus software status, information concerning devices**

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				connected to Access Device 230, Windows registry information, MAC address, IP addresses, cookies, status of applications executing on Access Device 230, or the like.
7.	"information regarding the device" "information regarding the access device" "device information received from the device in response to the audit request"	'450 Patent: Claim 1 '450 Patent: Claim 23 '645 Patent: Claim 1	plain and ordinary meaning	Expert Declaration and Testimony of Dr. Narasimha Reddy that this construction is plain and ordinary Intrinsic Evidence from U.S. Patent No. 7,523,484: 1:31-40: A first level of access control is achieved by requiring authentication of a user. This may be accomplished by **requiring the user to enter a username and password or by reading a MAC address or other identifying information from an access device**. In some systems, a network switch is programmed to grant access to a secure network only after proper authentication is achieved. Systems capable of using this approach include those using a proprietary VMPS protocol from Cisco Systems, Inc. of San Jose, Calif. or using a IEEE 802.1x standard protocol. 7:17-26: In some embodiments, Access Device 230 is configured to execute a software and/or hardware agent for communicating with GateKeeper 225. For example, in one embodiment, Access Device 230 includes an agent configured to monitor code running on Access Device 230 and report any suspicious code to GateKeeper 225. **In another**

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				example, Access Device 230 may include software and/or hardware configured to monitor other devices connected to Access Device 230 and to report information about these devices (e.g., their security statuses or MAC addresses) to GateKeeper 225. 11:39-50: In optional Obtain Audit Data Step 450, Policy Auditor 325 collects further data to perform a security audit of Access Device 230 responsive to Security Policy 330A or Security Policy 330B. In some embodiments, Obtain Audit Data Step 450 includes sending system data requests to Access Device 230, Router 220, or Access Point 215. **The requested system data may include, for example, operating system status (version, updates, etc.), antivirus software status, information concerning devices connected to Access Device 230, Windows registry information, MAC address, IP addresses, cookies, status of applications executing on Access Device 230, or the like**. 14:4-17: According to an embodiment like that disclosed in U.S. Provisional Patent Application No. 60/513,080, the disclosure of which has been incorporated herein by reference, the auditing protocol takes place between the EP (e.g., end point which can either be a PC or network device) agent software and the GK. **A client filter redirects calls for audit information to an agent on the EP and sends the responses to the**

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				802.1x compliant AP which relays them to the EAP server. The EAP server then calls a server filter which sends the responses to the GK for evaluation. **The GK sends requests for more information on the reverse path and this continues until the audit is completed**. If the audit is successful, the server sends a message to the AP which enables the EP's port allowing access for the PC. If the audit fails, the port on the AP is left disabled. 14:57-67: On the client, audit requests are passed to the agent API instead of to the client EAPM. **The agent returns information about the local system, which is converted to audit responses that are sent to the server.** During the audit state, the SF and CF exchange audit requests and responses about the EP as shown in FIGS. 8A and 8B. The ECL and ESL continue to communicate with the CF and SF, but instead of calling the EAPM, the CF and SF call the agent and GK respectively, to perform this exchange. **The audit session continues until the necessary audit information has been passed to the SF.** 15:14-19: **After the audit has been performed, "keep alives" and updates regarding changes to previous audit information are exchanged**. Changes are reevaluated and if inconsistent with the current state,

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				access to the network is modified appropriately by changing the VLAN used for the EP or by terminating access by the EP by communicating with the AP.
8.	"audit data pertaining to [a/the] device" "audit data"	'350 Patent: Claims 1, 18, 19; '444 Patent: Claims 1, 5, 6, 7, 10, 22 '350 Patent: Claims 1, 6, 8, 9, 10, 13, 18, 19; '444 Patent: Claims 1, 5, 6, 7, 10, 11, 12, 13, 14, 22	plain and ordinary meaning	Expert Declaration and Testimony of Dr. Narasimha Reddy that this construction is plain and ordinary Intrinsic Evidence from U.S. Patent No. 7,523,484: 10:26-44: FIG. 4 is a flowchart illustrating a method of granting access to Less-Restricted Subset 210 (FIG. 2), according to various embodiments of the invention. In these embodiments, an Update Port Log Step 410 and a Restrict Port Step 420 are used to prepare an open (unused) communication port on Access Point 215 for receiving a request for access to Less-Restricted Subset 210. This request is received from Access Device 230 in a Receive **Access Request Step 430. In response, GateKeeper 225 authenticates a user, obtains audit data, and applies a security policy in an Authenticate User Step 440, an Obtain Audit Data Step 450 and an Apply Security Policy Step 460, respectively**. If the security policy is satisfied, then in a Reconfigure Port Step 470, GateKeeper 225 reconfigures the communication port of Access Point 215 to which Access Device 230 has connected. Finally, the reconfigured communication port is used to pass communication between Access Device 230 and one or more element of Less-

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				Restricted Subset 210 in a Communicate Step 480. Further details of these steps are discussed herein. 11:39-55: **In optional Obtain Audit Data Step 450, Policy Auditor 325 collects further data to perform a security audit of Access Device 230 responsive to Security Policy 330A or Security Policy 330B. In some embodiments, Obtain Audit Data Step 450 includes sending system data requests to Access Device 230, Router 220, or Access Point 215**. The requested system data may include, for example, operating system status (version, updates, etc.), antivirus software status, information concerning devices connected to Access Device 230, Windows registry information, MAC address, IP addresses, cookies, status of applications executing on Access Device 230, or the like. In some embodiments, **Obtain Audit Data Step 450 is facilitated by an agent running on Access Device 230**. For example, Access Device 230 may include a software agent configured to monitor local security and to report results of this monitoring to Policy Auditor 325. 12:33-43: In typical embodiments, reconfiguration of Port 305A is accomplished by sending commands from Access Control 320 to Switch Logic 317. These commands or responses to requests from Switch Logic 317 are optionally sent via SNMP, telnet,

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				SSH, RADIUS, EAP, or the like, **and are responsive to data received in Authenticate User Step 440 and Obtain Audit Data Step 450, and/or to the security audit performed in Apply Security Policy Step 460**. In response to these commands, Switch Logic 317 configures Port 305A to be associated with VLAN 310A and, thus, communicate through Port 305D.
9.	"requirements of the security policy are satisfied" "that the access device satisfies the requirements of the security policy" "based on satisfaction of the security policy"	'460 Patent: Claims 1, 16; '484 Patent: Claims 27, 28, 41, and 82 '460 Patent: Claims 3, 5, 18, 20 '450 Patent: Claims 16, 22	plain and ordinary meaning	Expert Declaration and Testimony of Dr. Narasimha Reddy that this construction is plain and ordinary Intrinsic Evidence from U.S. Patent No. 7,523,484: 2: 14-25: GateKeeper 110 is configured to control access to Secure Network 100. In addition to authenticating users who wish to access Secure Network 100 using an Access Device 160, GateKeeper 110 is configured to ensure that Access Device 160 conforms to a predetermined security policy, before granting access to Secure Network 100. For example, GateKeeper 110 may make certain that Access Device 160 has up-to-date virus software and encryption protocols as proscribed by the security policy. **Once GateKeeper 110 has verified that Access Device 160 satisfies the security policy, Access Device 160 is allowed to communicate through GateKeeper 110 to LAN 125.** 5:29-50:

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				Access to a protected computing network is controlled by manipulating a communication port within an access point. When an access request is first received, the communication port is configured to pass the request to a restricted subset of a protected computing network. This restricted subset includes a gatekeeper configured to administer a security policy governing access to those parts of the protected computing network that are not part of the restricted subset. Those parts of the protected computing network that are not part of the restricted network are considered to be in a less-restricted subset. The less-restricted subset being less restricted relative to the restricted subset in terms of what elements may be included in each subset. **If the device requesting access satisfies requirements of the security policy, then the gatekeeper sends commands to the access point in order to reconfigure the communication port through which the access request was received**. The communication port is reconfigured such that further communication from the access device is passed to the less-restricted subset as well as, optionally, the restricted subset. In some embodiments, the less-restricted subset and the restricted subset are characterized by VLANs defined within the protected network. 9:30-52: Access Control 320 is responsive to a Policy Auditor 325 included in GateKeeper 225. Policy Auditor 325 is configured to receive a request for access to Less-

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				Restricted Subset 210 from Access Device 230, to determine which of Security Policy 330A or optional Security Policy 330B applies to the current request, to perform a security audit of Access Device 230 based on the appropriate member of Security Policies 330A-330B, and to notify Access Control 320 if the audit is passed. This notice typically causes Access Control 320 to reconfigure a member of Ports 305A-305G using Switch Logic 317. For example, in some embodiments, if Security Policy 330A applies **and if Access Device 230 satisfies requirements of Security Policy 330A, then Policy Auditor 325 provides a notice to Access Control 320**. In response, Access Control 320 sends appropriate commands to Switch Logic 317. These commands cause changes in Port 305A, such that communication from Access Device 230 is no longer blocked by ACL 340C and can now be received by elements of Less-restricted Subset 310. In alternative embodiments, Security Policies 330A-330B are stored elsewhere in Protected Network 200 accessible to Policy Auditor 325. Restricted Subset 205 optionally includes one, two, or more security policy, such as Security Policies 330A-330B. 10:26-44: FIG. 4 is a flowchart illustrating a method of granting access to Less-Restricted Subset 210 (FIG. 2), according to various embodiments of the invention. In these embodiments, an Update Port Log Step 410 and a Restrict Port Step 420 are used to prepare an open (unused) communication port on

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				Access Point 215 for receiving a request for access to Less-Restricted Subset 210. This request is received from Access Device 230 in a Receive Access Request Step 430. In response, GateKeeper 225 authenticates a user, obtains audit data, and applies a security policy in an Authenticate User Step 440, an Obtain Audit Data Step 450 and an Apply Security Policy Step 460, respectively. **If the security policy is satisfied, then in a Reconfigure Port Step 470, GateKeeper 225 reconfigures the communication port of Access Point 215 to which Access Device 230 has connected**. Finally, the reconfigured communication port is used to pass communication between Access Device 230 and one or more element of Less-Restricted Subset 210 in a Communicate Step 480. Further details of these steps are discussed herein. 11:56-12:9: In Apply Security Policy Step 460, a security audit of Access Device 230 is performed by Policy Auditor 325 responsive to a member of Security Policy 330A or Security Policy 330B. The particular member of Security Policy 330A or Security Policy 330B used to perform the audit may be responsive to the identity of Access Device 230, an identity of a user of Access Device 230, a part of Less-Restricted Subset 210 to which access is requested, or the like. **The security audit typically includes determining if Access Device 230 satisfies requirements of the security policy**. The security audit optionally includes active probing, scanning, and/or collection

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				of third party data regarding Access Device 230. In some embodiments, Authenticate User Step 440 is considered part of the security policy audit. **As is discussed further herein, in some embodiments, satisfaction of all the requirements of a particular security policy results in access to Less-Restricted Subset 210, while satisfaction of a subset of the requirements associated with the particular security policy is considered partial satisfaction of the security policy and may result in a more limited access to Less-Restricted Subset 210**.
10.	"update[e/ing] the access device" "updating the device" "facilitating updates to software on the device" "the updated access device" "software update"	'484 Patent: Claims 3, 24, 38, 41; '460 Patent: Claim 27 '350 Patent: Claim 7 '450 Patent: Claim 2 '450 Patent: Claims 16, 22 '450 Patent: Claims 27, 28	indefinite	Expert Declaration and Testimony of Dr. Narasimha Reddy that this term is indefinite Intrinsic Evidence from U.S. Patent No. 7,523,484: 6:6-11. In some embodiments, Restricted Subset 205 further includes a DHCP (dynamic host configuration protocol service) 260 configured to assign and manage network addresses, and/or an Update Module 255 configured for providing security updates to Access Device 230. 6:14-16. In one embodiment, Restricted Subset 205 includes a single computing device configured to function as both Update Module 255 and GateKeeper 225. 7:39-41. Update Module 255 is configured for remotely modifying Access Device 230, or a device connected to Access Device 230, in order to improve compliance with a security policy. 7:41-45. For example, if it is found that Access Device 230 includes out-of-date antivirus software, then Update

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				Module 255 may facilitate updating of the antivirus software on Access Device 230. 7:45-46. In some embodiments, Update Module 255 is configured to update an agent executing on Access Device 230. 7:46-50. Update Module 255 is optionally included in Less-Restricted Subset 210 or external to Protected Network 200. Update Module 255 optionally operates responsive to a security policy and/or to GateKeeper 225. 12:13-16. For example, in one embodiment, Apply Security Policy Step 460 includes updating antivirus software on Access Device 230 in response to a security audit that determined that the current antivirus software is out-of-date.
11.	"EAP encryption protocol" "receive the authentication information from the device using an EAP encryption protocol"	'645 Patent: Claim 1 '645 Patent: Claim 1	Indefinite, or limited to time of invention, otherwise indefinite	Expert Declaration and Testimony of Dr. Narasimha Reddy that this construction is indefinite, or limited to time of invention, otherwise indefinite Intrinsic Evidence from U.S. Patent No. 7,523,484: 8:24-30. As is discussed further below, the commands received by Switch Logic 317 may be generated by GateKeeper 225. This communication between GateKeeper 225 and Switch Logic 317 may be accomplished using SNMP (Simple Network Management Protocol), telnet, SSH (Secure Shell), RADIUS (Remote Authentication User Dial-In Service), EAP (Extensible Authentication Protocol), or the like. 12:35-40. These commands or responses to requests from Switch Logic 317 are optionally sent via SNMP, telnet, SSH, RADIUS, EAP, or the like, and are responsive to data received in Authenticate User Step 440 and Obtain

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 110 of 1144
INFOEXPRESS, INC. - EX2572

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				Audit Data Step 450, and/or to the security audit performed in Apply Security Policy Step 460. 14:9-11. A client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP which relays them to the EAP server. 14:11-13. The EAP server then calls a server filter which sends the responses to the GK for evaluation. 14:20-23. There may be one or more instances of the CF and SF, which correspond to the separate EAP Authentication Modules (EAPM) that are supported. 14:27-28. The CF and SF APIs have APIs which correspond to the EAPM APIs. 14:28-31. Therefore, the EAP Client Layer (ECL) or EAP Server Layer (ESL) can call the CF and SF instances corresponding to a particular authentication method as shown in FIGS. 6A and 6B. 14:31-34. To the ECL and ESL, each instance of the CF and SF appears to be an EAPM which incorporates the functionality of the original EAPM prior to completion of the success response by the server EAPM. 14:39-41. This authentication method corresponds to an authentication method supported by one of the EAPMs. 14:42-44. The ECL calls the corresponding CF to perform authentication, which at first calls the appropriate EAPM to obtain the proper authentication response. 14:44-46. The authentication response is returned by the CF to the ESL, which sends the response to the server's ESL, SF, and EAPM.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 111 of 1144
INFOEXPRESS, INC. - EX2572

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				14:46-49. This process continues until the authentication either succeeds or fails, at which time the server's authentication EAPM returns a success or failure response to the SF. 14:50-53. If the SF receives a success response from the server EAPM as shown in FIG. 7, the SF changes to the audit state and calls GK to obtain audit requests to send back to the client. 14:57-58. On the client, audit requests are passed to the agent API instead of to the client EAPM. 14:63-65. The ECL and ESL continue to communicate with the CF and SF, but instead of calling the EAPM, the CF and SF call the agent and GK respectively, to perform this exchange.
12.	"EAP server layer (SL)", "ESL"	'645 Patent: Claims 1, 2, 5	Indefinite, or limited to time of invention, otherwise indefinite	Expert Declaration and Testimony of Dr. Narasimha Reddy that this construction is indefinite, or limited to time of invention, otherwise indefinite Intrinsic Evidence from U.S. Patent No. 7,523,484: 14:4-26: > According to an embodiment like that disclosed in U.S. Provisional Patent Application No. 60/513,080, the disclosure of which has been incorporated herein by reference, the auditing protocol takes place between the EP (e.g., end point which can either be a PC or network device) agent software and the GK. A client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP which relays them to the EAP server. **The EAP server then calls a server filter which**

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				sends the responses to the GK for evaluation. The GK sends requests for more information on the reverse path and this continues until the audit is completed. If the audit is successful, the server sends a message to the AP which enables the EP's port allowing access for the PC. If the audit fails, the port on the AP is left disabled.
13.	"SF" "wherein the SF is part of the ESL"	'645 Patent: Claims 2, 5 '645 Patent: Claim 5	indefinite	Expert Declaration and Testimony of Dr. Narasimha Reddy that this construction is indefinite Intrinsic Evidence from U.S. Patent No. 7,523,484: 14: 18-15:13: According to an exemplary embodiment, **client filters (CF) and server filters (SF) are added along with an agent and GK to perform audits, as highlighted in FIG.** 5. There may be one or more instances of the CF and SF, which correspond to the separate EAP Authentication Modules (EAPM) that are supported. Note that the agent and GK are logical components. The functionality of the agent and GK can be embedded into the CF and SF, respectively, or in the case of the GK, may reside on a separate server. The CF and SF APIs have APIs which correspond to the EAPM APIs. Therefore, the EAP Client Layer (ECL) or EAP Server Layer (ESL) can call the CF and SF instances corresponding to a particular authentication method as shown in FIGS. 6A and 6B. **To the ECL and ESL, each instance of the CF and SF appears to be an EAPM which incorporates the**

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				functionality of the original EAPM prior to completion of the success response by the server EAPM. To use the invention as disclosed in U.S. Provisional Patent Application No. 60/513,080, the disclosure of which has been incorporated herein by reference, **the ECL and ESL are configured to use the instance of the CF and SF corresponding to the desired authentication method**. This authentication method corresponds to an authentication method supported by one of the EAPMs. The ECL calls the corresponding CF to perform authentication, which at first calls the appropriate EAPM to obtain the proper authentication response. The authentication response is returned by the CF to the ESL, which sends the response to the server's ESL, SF, and EAPM. **This process continues until the authentication either succeeds or fails, at which time the server's authentication EAPM returns a success or failure response to the SF**. **If the SF receives a success response from the server EAPM as shown in FIG. 7, the SF changes to the audit state and calls GK to obtain audit requests to send back to the client**. In this state, the SF returns specially formatted audit requests to the ESL which are passed to the ECL, and eventually to the CF which sends back audit responses to the SF requests. On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				information about the local system, which is converted to audit responses that are sent to the server. **During the audit state, the SF and CF exchange audit requests and responses about the EP as shown in FIGS. 8A and 8B**. The ECL and ESL continue to communicate with the CF and SF, but instead of calling the EAPM, the CF and SF call the agent and GK respectively, to perform this exchange. The audit session continues until the necessary audit information has been passed to the SF. If the audit indicates the client EP is in compliance, the SF returns a success response. If the VLAN for the EP is specified in the policy, then the VLAN that should be used for this EP is passed back as well. If the GK determines that the EP has failed the audit, GK returns a failure response to SF which causes one of the following: (1) the SF returns a failure to ECL, and the corresponding port on the AP is left disabled, or (2) the SF returns a success response to the ECL but specifies that the EP should be set to a restricted VLAN where the EP has limited network access. In either case, the EP is isolated from the company network until it successfully passes an audit with the GK.
14.	"a wireless access point configured to support an 802.1x standard"	'484 Patent: Claim 17 '444 Patent: Claims 1, 22	limited to time of invention, otherwise indefinite	Expert Declaration and Testimony of Dr. Narasimha Reddy that this construction is limited to time of invention, otherwise indefinite Intrinsic Evidence from U.S. Patent No. 7,523,484:

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
	"an access point configured to use an 802.1x protocol"			7: 51-61: FIG. 3A is a block diagram showing further details of Access Point 215, Router 220 and GateKeeper 225, according to various embodiments of the invention. Access Point 215 is, **for example, a network switch, a wireless access point, a remote access virtual private network (VPN), secure socket layer VPN, firewall, or the like**. When embodied in a network switch, Access Point 215 includes a series of communication ports, designated Ports 305A-305G and configured for communication with devices such as Access Device 230, Router 220, Less-Restricted Subset 210 and/or Restricted Subset 205. 9: 3-19: **When Access Point 215 is embodied in a wireless access point, some or all of Ports 305A-305G may be wireless connections rather than physical ports**. In these embodiments, Lines 315 may represent logical associations used to control data flow between wireless connections to Access Point 215 and/or members of Ports 305A-305G that are physical communication ports. For example, in some embodiments, MAC addresses are used to distinguish wireless communications from different instances of Access Device 230 and the logical associations (represented by Lines 315) are used to direct these communications to various output channels. The output channels may be other wireless connections or physical members of Ports 305A-305G. These logical associations may be altered by Switch Logic 317 just as associations with members of VLANs 310A-310D

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				are modified. **Therefore, the teachings herein that use a network switch as an example of Access Point 215, apply equally to wireless access points.** 13: 55-14:3 According to embodiments like that disclosed in U.S. Provisional Patent Application No. 60/513,080, the disclosure of which has been incorporated herein by reference, **an AP (e.g., a switch or wireless access point (WAP) which is used to connect end points to the corporate network)** may be programmed to prohibit access by the PC (e.g., notebook, desktop PC, PDA, or similar computing device) to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK (e.g., software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria) passes, while still supporting the existing encryption and authentication functionality. **The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol.** 15: 20-36: Several embodiments are specifically illustrated and/or described herein. However, it will be appreciated that modifications and variations are covered by the above teachings and within the scope of the appended claims without departing from the spirit and intended scope thereof. For example, the

No.	Claim Term, Clause, or Phrase	Patent(s) and Claim(s)	Proposed Construction	Evidence
				teachings herein may be applied to embodiments wherein **Access Point 215 is a wireless access point and MAC addresses, or the like, are used instead of VLANs to separate traffic from different instances of Access Device 230**. It is, thus, anticipated that network management techniques other than VLANs may be used to distinguish Less-Restricted Subset 210 from Restricted Subset 205. In some embodiments, various aspects of GateKeeper 225 may be incorporated into Access Point 215 and/or Router 220. GateKeeper 225 and Policy Manager 250 are each optionally implemented on a plurality of computing devices within Restricted Subset 205.

CERTIFICATE OF SERVICE

I am a citizen of the United States employed in the city of Chicago, State of Illinois. I am over the age of 18 and not a party to this action.

On March 25, 204, I served the following document described as:

DEFENDANT CISCO SYSTEMS, INC.'S PATENT L.R. 4-2 IDENTIFICATION OF PRELIMINARY CLAIM CONSTRUCTIONS AND EVIDENCE

on the interested parties in this action listed on the service list below.

X	by electronically transmitting a true and correct copy thereof via email to the following in accordance with their agreement to be served electronically pursuant to Federal Rule of Civil Procedure 5(b)(2)(E).

SERVICE LIST:

Brenda H. Entzminger
bentzminger@bdilaw.com
M. Elizabeth Day
eday@bdilaw.com
Michelle E. Flynn-O'Brien
mflynnobrien@bdilaw.com
BUNSOW DE MORY
701 El Camino Real
Redwood City, CA 94063

Brian R. Michalek
Brian.michalek@saul.com
Casey T. Grabenstein
Casey.crabenstein@saul.com
Joseph M. Kuo
Joseph.kuo@saul.com
SAUL EWING
161 N. Clatk Street, Suite 4200
Chicago, IL 60601

Andrew F. Schwerin
Andrew.schwerin@saul.com
Andrew F. Schwerin, I
SAUL EWING
Center Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on March 25, 2024, at Chicago, Illinois.

/s/ Vickie Kennedy
Vickie Kennedy

EXHIBIT C

Subject: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR, Patent L.R. 4-2(c) Meet-and-Confer
Location: https://saul.zoom.us/j/97430530167?pwd=TVZTK1JteDAvYUV1YkZjNzBuUVlNQT09

Start: Wed 4/17/2024 1:00 PM
End: Wed 4/17/2024 2:00 PM
Show Time As: Tentative

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Schwerin, Andrew

Andrew Schwerin is inviting you to a scheduled Zoom meeting.

Join Zoom Meeting

https://saul.zoom.us/j/97430530167?pwd=TVZTK1JteDAvYUV1YkZjNzBuUVlNQT09

Meeting ID: 974 3053 0167

Passcode: 943138

One tap mobile

+13017158592,,97430530167#,,,,*943138# US (Washington DC)

+13126266799,,97430530167#,,,,*943138# US (Chicago)

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 121 of 1144
INFOEXPRESS, INC. - EX2572

Dial by your location

• +1 301 715 8592 US (Washington DC)

• +1 312 626 6799 US (Chicago)

• +1 646 558 8656 US (New York)

• +1 253 215 8782 US (Tacoma)

• +1 346 248 7799 US (Houston)

• +1 669 900 9128 US (San Jose)

Meeting ID: 974 3053 0167

Passcode: 943138

Find your local number: https://saul.zoom.us/u/aeEOK0lTod

Join by SIP

• 97430530167@zoomcrc.com

Join by H.323

• 162.255.37.11 (US West)

• 162.255.36.11 (US East)

• 115.114.131.7 (India Mumbai)

- 115.114.115.7 (India Hyderabad)
- 213.19.144.110 (Amsterdam Netherlands)
- 213.244.140.110 (Germany)
- 103.122.166.55 (Australia Sydney)
- 103.122.167.55 (Australia Melbourne)
- 149.137.40.110 (Singapore)
- 64.211.144.160 (Brazil)
- 149.137.68.253 (Mexico)
- 69.174.57.160 (Canada Toronto)
- 65.39.152.160 (Canada Vancouver)
- 207.226.132.110 (Japan Tokyo)
- 149.137.24.110 (Japan Osaka)

Meeting ID: 974 3053 0167

Passcode: 943138

"Saul Ewing LLP (saul.com)" has made the following annotations:
+~~~~~~~~~~~~~~~~~~~~~~~~+
This e-mail may contain privileged, confidential, copyrighted, or other legally protected information. If you are not the intended recipient (even if the e-mail address is yours), you may not use, copy, or retransmit it. If you have received this by mistake please notify us by return e-mail, then delete.
+~~~~~~~~~~~~~~~~~~~~~~~~+

EXHIBIT D

Subject: Re: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement
Location: Microsoft Teams Meeting

Start: Wed 5/1/2024 1:00 PM
End: Wed 5/1/2024 2:00 PM

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Logan, William

William Logan
Associate Attorney
Winston & Strawn LLP
D +1 (713) 651-2766

From: Schwerin, Andrew <andrew.schwerin@saul.com>
Sent: Tuesday, April 30, 2024 7:34:15 PM
To: Logan, William <WLogan@winston.com>; Michalek, Brian R. <brian.michalek@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>; Dotson, David C. <DCDotson@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Vinci, Brianna <BVinci@duanemorris.com>
Cc: Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: RE: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

Counsel:

Please see InfoExpress's further edits to the Joint Claim Construction Statement and Exhibit A chart. We have accepted your edits and made our further edits in redline. We look forward to discussing your proposed compromise for "audit/auditing" and "audit data" and the antecedent basis issue with you. Also, we believe that terms #13 and #14 can be combined.

We are available tomorrow 4 pm ET to 5 pm ET and Thursday from 12 pm ET to 2 pm ET. Please let us know if that works.

Regards,

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 125 of 1144
INFOEXPRESS, INC. - EX2572

Office: (215) 972-7184

From: Logan, William <WLogan@winston.com>
Sent: Wednesday, April 24, 2024 6:49 PM
To: Michalek, Brian R. <brian.michalek@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Schwerin, Andrew <andrew.schwerin@saul.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>; Dotson, David C. <DCDotson@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Vinci, Brianna <BVinci@duanemorris.com>
Cc: Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: RE: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

Counsel:

Attached are Cisco's and Fortinet's edits to the draft JCCS and Exhibit A you circulated. In the interest of narrowing disputes, we have withdrawn some terms and agreed on others. We have proposed some potential compromise constructions below for two of the terms that we may be able to live with if InfoExpress agrees, and we can eliminate a dispute for the Court:

- Term 3, "audit data". Potential compromise position: "data used for determining compliance with a security policy"
- Term 19, "audit/auditing". Potential compromise position: "determin[e/ing] compliance of [a device / the access device] with a security policy"

Also, as we discussed on our last call, please let us know InfoExpress's position as to what is the antecedent basis for "the protected network" in claim 16 of the '460 Patent (term 17).

Further, several disputed terms are directed to a single dependent claim (in most cases), including "access control," "monitor," "and that contains antivirus software," "the protected network," "update module," "access to the restricted subset of the protected network . . .," "a wireless access point configured to support an 802.1x standard," and "an access point configured to use an 802.1x protocol." If you drop some or all of the claims associated with these terms, the number of disputed terms would be narrowed, which would streamline claim construction for the Court and the parties. Please let us know if you would be agreeable to this.

Thanks,
William

William Logan
Associate Attorney
Winston & Strawn LLP
T: +1 713-651-2600
D: +1 713-651-2766
F: +1 713-651-2700
Email | winston.com
Pronouns: He, Him, His

From: Michalek, Brian R. <brian.michalek@saul.com>
Sent: Wednesday, April 17, 2024 6:17 PM
To: Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Schwerin, Andrew <andrew.schwerin@saul.com>; Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>; Dotson, David C. <DCDotson@duanemorris.com>; Snedeker, Alice

<AESnedeker@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Vinci, Brianna <BVinci@duanemorris.com>
Cc: Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: RE: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

Cisco and Fortinet Counsel,

As discussed today, please see the joint stipulation. Please let me know if you have any edits or it is good to file.

Additionally, on April 9, 2024, InfoExpress circulated a draft LPR 4.3 statement and chart. Pursuant to rule LPR 4.2(c), Fortinet and Cisco agreed to review the draft statement and chart and supply their edits and comments. Please do so by April 24, 2024 so the parties can continue to make meaningful progress toward narrowing the issues.

Best,

Brian

Brian R. Michalek
Partner
SAUL EWING LLP | Chicago
Office: (312) 876-7836

From: Padmanabhan, Krishnan <KPadmanabhan@winston.com>
Sent: Friday, April 12, 2024 7:51 PM
To: Michalek, Brian R. <brian.michalek@saul.com>; Schwerin, Andrew <andrew.schwerin@saul.com>; Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>; Dotson, David C. <DCDotson@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Vinci, Brianna <BVinci@duanemorris.com>
Cc: Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: Re: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

****EXTERNAL EMAIL** - This message originates from outside our Firm. Please consider carefully before responding or clicking links/attachments.**

Brian,

Let's plan to meet and confer on Wed. at 4 EST (if InfoExpress is available).

Importantly, we think it makes sense to meet and confer pursuant to the Court's Order on Cisco's Rule 12 Motion, which provided additional guidance regarding scheduling issues (including that the Markman Hearing is likely to be taken off calendar), and asked the parties to confer on claim reduction in light of the Court's Order.

Thanks
KP

Krishnan Padmanabhan
(D) 212-294-3564

(M) 415-632-8214

From: Michalek, Brian R. <brian.michalek@saul.com>
Sent: Friday, April 12, 2024 3:38:49 PM
To: Schwerin, Andrew <andrew.schwerin@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>; Dotson, David C. <DCDotson@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Vinci, Brianna <BVinci@duanemorris.com>
Cc: Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: RE: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

Counsel,

Please let us know what times next week work to meet and confer pursuant to LPR 4-2(c) in advance of Friday's deadline to submit its Joint Claim Construction Chart.

In anticipation of that meet and confer, it would be helpful if Defendants could circulate any edits it had to the draft statement and chart provided by InfoExpress on Tuesday, April 9, 2024.

Further to the parties agreement to extend the service of claim construction expert reports to May 17, 2024 and the limited LPR 4-4 extension from May 17, 2024 to May 24, 2024, the parties agreed to follow up on the appropriate procedural mechanism to memorialize that agreement before the Court. InfoExpress believes a joint stipulation among the parties is the appropriate way to do so. Please let us know if you disagree or have other thoughts.

Thanks,

Brian

Brian R. Michalek
Partner
SAUL EWING LLP | Chicago
Office: (312) 876-7836

From: Schwerin, Andrew <andrew.schwerin@saul.com>
Sent: Tuesday, April 9, 2024 5:40 PM
To: Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Logan, William <WLogan@winston.com>; Clark, Patrick <PClark@winston.com>; Dotson, David C. <DCDotson@duanemorris.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Vinci, Brianna <BVinci@duanemorris.com>
Cc: Michalek, Brian R. <brian.michalek@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

Counsel:

Attached is a draft of the Joint Claim Construction Prehearing Statement along with an Exhibit A with term constructions and evidence (as required by Patent Local Rule 4-3(b)).

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 128 of 1144
INFOEXPRESS, INC. - EX2572

Per Rule 4-2(c), we're required to meet and confer. Once you've had an opportunity to review, please let us when you are ready to meet for the purpose of narrowing the issues.

Regards,

Andrew Schwerin
Associate
(215) 972-7184
andrew.schwerin@saul.com
Read my bio >>

Centre Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102-2186

"Saul Ewing LLP (saul.com)" has made the following annotations:
+~~~~~~~~~~~~~~~~~~~~~~~~~~+
This e-mail may contain privileged, confidential, copyrighted, or other legally protected information. If you are not the intended recipient (even if the e-mail address is yours), you may not use, copy, or retransmit it. If you have received this by mistake please notify us by return e-mail, then delete.
+~~~~~~~~~~~~~~~~~~~~~~~~~~+

The contents of this message may be privileged and confidential. If this message has been received in error, please delete it without reading it. Your receipt of this message is not intended to waive any applicable privilege. Please do not disseminate this message without the permission of the author. Any tax advice contained in this email was not intended to be used, and cannot be used, by you (or any other taxpayer) to avoid penalties under applicable tax laws and regulations.

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 290 065 820 580

Passcode: SkiWCo

Dial-in by phone

+1 469-706-0532,,401593650# United States, Dallas

Find a local number

Phone conference ID: 401 593 650#

Join on a video conferencing device

Tenant key: winston@m.webex.com

Video ID: 112 434 501 3

More info

For organizers: Meeting options | Reset dial-in PIN

EXHIBIT E

From:	Schwerin, Andrew
To:	Dotson, David C.; Vinci, Brianna; Padmanabhan, Krishnan; Michalek, Brian R.; Logan, William; Ahearn, Terry W.; Gaudet, Matthew C.; Snedeker, Alice; Clark, Patrick
Cc:	Kuo, Joseph M.; Grabenstein, Casey
Subject:	RE: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement
Date:	Friday, May 3, 2024 3:10:05 PM
Attachments:	image004.png image005.png image006.png image007.png

Thank you all—I will get these on file.

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Dotson, David C. <DCDotson@duanemorris.com>
Sent: Friday, May 3, 2024 3:55 PM
To: Vinci, Brianna <BVinci@duanemorris.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Michalek, Brian R. <brian.michalek@saul.com>; Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Schwerin, Andrew <andrew.schwerin@saul.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Clark, Patrick <PClark@winston.com>
Cc: Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: RE: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

Likewise for Fortinet.

Thanks,
David

On May 3, 2024 3:49 PM, "Logan, William" <WLogan@winston.com> wrote:
Thanks Andrew. These changes are acceptable to Cisco and you have our permission to file.

William Logan
Associate Attorney
Winston & Strawn LLP
T: +1 713-651-2600
D: +1 713-651-2766
F: +1 713-651-2700
Email | winston.com
Pronouns: He, Him, His

WINSTON & STRAWN LLP

From: Schwerin, Andrew <andrew.schwerin@saul.com>
Sent: Friday, May 3, 2024 12:37 PM
To: Logan, William <WLogan@winston.com>; Dotson, David C. <DCDotson@duanemorris.com>; Michalek, Brian R. <brian.michalek@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Vinci, Brianna <BVinci@duanemorris.com>
Cc: Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: RE: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

Counsel:

Thank you for your edits. We have accepted all changes, and made additional edits in redline. Please let us know if we have your permission to file clean versions of these. Or, if you have further edits, please let us know them timely so we can get these on file today.

Regarding changes to the schedule, InfoExpress is generally amenable to the six-week extension you propose. Though, given the fact that InfoExpress has other filings due today, we think it makes sense to file those papers early next week. However, if you wanted to send us a draft amended scheduling order for our review, that would help.

Regards,

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Logan, William <WLogan@winston.com>
Sent: Thursday, May 2, 2024 9:12 PM
To: Dotson, David C. <DCDotson@duanemorris.com>; Schwerin, Andrew <andrew.schwerin@saul.com>; Michalek, Brian R. <brian.michalek@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Vinci, Brianna <BVinci@duanemorris.com>
Cc: Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: RE: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

Counsel:

While we await your response to the below, our current responsive edits to the JCCS are attached. Please note that we have moved three terms to Exhibit B as additional proposed terms pending leave so that we are compliant with the Court's order regarding identifying 10 terms at this stage. We have also added an impact statement for each term consistent with the Court's order. Please send us back your responsive edits for review.

Thanks,
William

William Logan
Associate Attorney
Winston & Strawn LLP
T: +1 713-651-2600
D: +1 713-651-2766
F: +1 713-651-2700
Email | winston.com
Pronouns: He, Him, His
WINSTON & STRAWN LLP

From: Dotson, David C. <DCDotson@duanemorris.com>
Sent: Thursday, May 2, 2024 5:09 PM
To: Schwerin, Andrew <andrew.schwerin@saul.com>; Logan, William <WLogan@winston.com>; Michalek, Brian R. <brian.michalek@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Vinci, Brianna <BVinci@duanemorris.com>
Cc: Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: RE: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

Andrew,

To your first point on the schedule, given that we are set to file the JCCS tomorrow, the Defendants believe we need to seek relief as necessary on the claim construction schedule by tomorrow as well.

We propose that the Parties agree to extend the current claim construction dates (starting with the exchange of expert declarations on May 17) by six weeks, coupled with asking the Court to reset the Markman hearing date at the Court's convenience.

We do not think we can propose a Markman hearing date certain, since the Court said it is inclined

to vacate the current date in view of a criminal trial. But, the six weeks may move our Markman enough that it will come after (or close to after) the Court's scheduled trial.

Please let us know whether InfoExpress agrees by tomorrow so that we can move as appropriate.

Thanks,
David

From: Schwerin, Andrew <andrew.schwerin@saul.com>
Sent: Thursday, May 2, 2024 4:17 PM
To: Logan, William <WLogan@winston.com>; Michalek, Brian R. <brian.michalek@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>; Dotson, David C. <DCDotson@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Vinci, Brianna <BVinci@duanemorris.com>
Cc: Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: RE: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

Counsel: Thank you for meeting yesterday. We write to follow up on items from that call.

As to altering the claim construction schedule, InfoExpress reiterated its position that the court's scheduling order, including the current dates for claim construction briefs and hearing, is still in effect. We also noted that we would consider a reasonable proposed change to the schedule, so long as it included ***date(s) certain***. What InfoExpress would not agree is wholly striking the case deadlines, without providing amended dates.

As to "audit data" and "audit/auditing," which terms are currently numbered 3 and 10, we declined to accept Cisco and Fortinet's compromise positions as to each of those terms. Cisco and Fortinet further noted that they may revert back to their originally proposed constructions.

As to "the protected network," (term no. 9; '460 Patent, claim 16), Fortinet asked InfoExpress to clarify its position. InfoExpress's position is that a POSITA would know with reasonable certainty what it means and it is therefore not indefinite. *See, e.g.*, *In re Downing*, 754 F. App'x 988, 996 (Fed. Cir. 2018); *Receivership Est. of AudienceScience Inc. v. Google LLC*, No. 5:22-CV-04756-EJD, 2023 WL 8720139 (N.D. Cal. Dec. 18, 2023); *Fortinet, Inc. v. Forescout Techs., Inc.*, No. 20-CV-03343-EMC, 2022 WL 17254313, at *11 (N.D. Cal. Nov. 28, 2022); *Pelican Int'l Inc. v. Hobie Cat Co.*, No. 20-CV-2390-BAS-MSB, 2022 WL 298959, at *13 (S.D. Cal. Feb. 1, 2022); *Dolby Lab'ys, Inc. v. Intertrust Techs. Corp.*, No. 19-CV-03371-EMC, 2021 WL 369542, at *16 (N.D. Cal. Feb. 3, 2021); *Hong Kong Ucloudlink Network Tech. Ltd. v. SIMO Holdings Inc.*, No. 18-CV-05031-EMC, 2020 WL 1305626, at *12 (N.D. Cal. Mar. 19, 2020).

As to term nos. 13 and 14, "a wireless access point configured to support an 802.1x standard" ('484 Patent: Claim 17) and "an access point configured to use an 802.1x protocol" ('444 Patent: Claim

22), Cisco and Fortinet agreed that such terms could be consolidated, and further that you would provide to us a revised Exhibit A table with these terms and defendants' supporting evidence combined.

As to "protected network" (term no. 8), InfoExpress does not agree with Fortinet that the preamble is limiting.

The last item as to claim construction was the mechanism for asking the court adjudicate claim terms in excess of Judge Rogers's 10-term maximum. On the call, we explained that this would be Defendants' motion to bring in light how of the District's Patent Local Rule 4-3(c) counts terms. Regardless, to help facilitate agreement, InfoExpress is amenable to addressing this 10-term maximum through a joint stipulation of the parties. Please send us a draft when you have it.

We sent you the draft 4-3 statement and table on Tuesday. If you have any further changes, please send us the next version for our review so that the parties can timely file tomorrow.

Last, apart from claim construction, are Cisco's and Fortinet's pending stay motions. As things stand now, there are two different hearing dates—June 4 at 2:00 pm for Cisco's (Dkt. 80), and May 28 at 2:00 pm for Fortinet's (Dkt. 57). Would Cisco and Fortinet agree to asking Judge Rogers to have the stay hearings on the same date? If you agree, InfoExpress can draft something for your consideration. InfoExpress would also be happy to meet and confer on this issue if you'd like.

Regards,

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Logan, William <WLogan@winston.com>
Sent: Wednesday, May 1, 2024 7:41 AM
To: Schwerin, Andrew <andrew.schwerin@saul.com>; Michalek, Brian R. <brian.michalek@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>; Dotson, David C. <DCDotson@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Vinci, Brianna <BVinci@duanemorris.com>
Cc: Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: Re: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

Thanks Andrew. Let's plan to talk at 4 ET today.

William Logan
Associate Attorney

Winston & Strawn LLP
D +1 (713) 651-2766

From: Schwerin, Andrew <andrew.schwerin@saul.com>
Sent: Tuesday, April 30, 2024 7:32:41 PM
To: Logan, William <WLogan@winston.com>; Michalek, Brian R. <brian.michalek@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>; Dotson, David C. <DCDotson@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Vinci, Brianna <BVinci@duanemorris.com>
Cc: Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: RE: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

Counsel:

Please see InfoExpress's further edits to the Joint Claim Construction Statement and Exhibit A chart. We have accepted your edits and made our further edits in redline. We look forward to discussing your proposed compromise for "audit/auditing" and "audit data" and the antecedent basis issue with you. Also, we believe that terms #13 and #14 can be combined.

We are available tomorrow 4 pm ET to 5 pm ET and Thursday from 12 pm ET to 2 pm ET. Please let us know if that works.

Regards,

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Logan, William <WLogan@winston.com>
Sent: Wednesday, April 24, 2024 6:49 PM
To: Michalek, Brian R. <brian.michalek@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Schwerin, Andrew <andrew.schwerin@saul.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>; Dotson, David C. <DCDotson@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Vinci, Brianna <BVinci@duanemorris.com>
Cc: Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: RE: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

Counsel:

Attached are Cisco's and Fortinet's edits to the draft JCCS and Exhibit A you circulated. In the interest of narrowing disputes, we have withdrawn some terms and agreed on others. We have proposed some potential compromise constructions below for two of the terms that we may be able to live with if InfoExpress agrees, and we can eliminate a dispute for the Court:

- Term 3, "audit data". Potential compromise position: "data used for determining compliance with a security policy"
- Term 19, "audit/auditing". Potential compromise position: "determin[e/ing] compliance of [a device / the access device] with a security policy"

Also, as we discussed on our last call, please let us know InfoExpress's position as to what is the antecedent basis for "the protected network" in claim 16 of the '460 Patent (term 17).

Further, several disputed terms are directed to a single dependent claim (in most cases), including "access control," "monitor," "and that contains antivirus software," "the protected network," "update module," "access to the restricted subset of the protected network . . .," "a wireless access point configured to support an 802.1x standard," and "an access point configured to use an 802.1x protocol." If you drop some or all of the claims associated with these terms, the number of disputed terms would be narrowed, which would streamline claim construction for the Court and the parties. Please let us know if you would be agreeable to this.

Thanks,
William

William Logan
Associate Attorney
Winston & Strawn LLP
T: +1 713-651-2600
D: +1 713-651-2766
F: +1 713-651-2700
Email | winston.com
Pronouns: He, Him, His
WINSTON & STRAWN LLP

From: Michalek, Brian R. <brian.michalek@saul.com>
Sent: Wednesday, April 17, 2024 6:17 PM
To: Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Schwerin, Andrew <andrew.schwerin@saul.com>; Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>; Dotson, David C. <DCDotson@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Vinci, Brianna <BVinci@duanemorris.com>
Cc: Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: RE: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

Cisco and Fortinet Counsel,

As discussed today, please see the joint stipulation. Please let me know if you have any edits or it is good to file.

Additionally, on April 9, 2024, InfoExpress circulated a draft LPR 4.3 statement and chart. Pursuant to rule LPR 4.2(c), Fortinet and Cisco agreed to review the draft statement and chart and supply their edits and comments. Please do so by April 24, 2024 so the parties can continue to make meaningful progress toward narrowing the issues.

Best,

Brian

Brian R. Michalek
Partner
SAUL EWING LLP | Chicago
Office: (312) 876-7836

From: Padmanabhan, Krishnan <KPadmanabhan@winston.com>
Sent: Friday, April 12, 2024 7:51 PM
To: Michalek, Brian R. <brian.michalek@saul.com>; Schwerin, Andrew <andrew.schwerin@saul.com>; Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>; Dotson, David C. <DCDotson@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Vinci, Brianna <BVinci@duanemorris.com>
Cc: Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: Re: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

****EXTERNAL EMAIL** - This message originates from outside our Firm. Please consider carefully before responding or clicking links/attachments.**

Brian,

Let's plan to meet and confer on Wed. at 4 EST (if InfoExpress is available).

Importantly, we think it makes sense to meet and confer pursuant to the Court's Order on Cisco's Rule 12 Motion, which provided additional guidance regarding scheduling issues (including that the Markman Hearing is likely to be taken off calendar), and asked the parties to confer on claim reduction in light of the Court's Order.

Thanks
KP

Krishnan Padmanabhan
(D) 212-294-3564
(M) 415-632-8214

From: Michalek, Brian R. <brian.michalek@saul.com>
Sent: Friday, April 12, 2024 3:38:49 PM
To: Schwerin, Andrew <andrew.schwerin@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>; Dotson, David C. <DCDotson@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Vinci, Brianna <BVinci@duanemorris.com>
Cc: Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: RE: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

Counsel,

Please let us know what times next week work to meet and confer pursuant to LPR 4-2(c) in advance of Friday's deadline to submit its Joint Claim Construction Chart.

In anticipation of that meet and confer, it would be helpful if Defendants could circulate any edits it had to the draft statement and chart provided by InfoExpress on Tuesday, April 9, 2024.

Further to the parties agreement to extend the service of claim construction expert reports to May 17, 2024 and the limited LPR 4-4 extension from May 17, 2024 to May 24, 2024, the parties agreed to follow up on the appropriate procedural mechanism to memorialize that agreement before the Court. InfoExpress believes a joint stipulation among the parties is the appropriate way to do so. Please let us know if you disagree or have other thoughts.

Thanks,

Brian

Brian R. Michalek
Partner
SAUL EWING LLP | Chicago
Office: (312) 876-7836

From: Schwerin, Andrew <andrew.schwerin@saul.com>

Sent: Tuesday, April 9, 2024 5:40 PM
To: Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Logan, William <WLogan@winston.com>; Clark, Patrick <PClark@winston.com>; Dotson, David C. <DCDotson@duanemorris.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Vinci, Brianna <BVinci@duanemorris.com>
Cc: Michalek, Brian R. <brian.michalek@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>
Subject: InfoExpress v. Cisco, Case No. 4:23-cv-02698-YGR; InfoExpress v. Fortinet, Case No. 4:23-cv-04389-YGR--Patent L.R. 4-3 Joint Claim Construction and Prehearing Statement

Counsel:

Attached is a draft of the Joint Claim Construction Prehearing Statement along with an Exhibit A with term constructions and evidence (as required by Patent Local Rule 4-3(b)).

Per Rule 4-2(c), we're required to meet and confer. Once you've had an opportunity to review, please let us when you are ready to meet for the purpose of narrowing the issues.

Regards,

Andrew Schwerin
Associate
(215) 972-7184
andrew.schwerin@saul.com
Read my bio >>

SAUL EWING LLP
Centre Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102-2186

"Saul Ewing LLP (saul.com)" has made the following annotations:
+~~~~~~~~~~~~~~~~~~~~~~~~+
This e-mail may contain privileged, confidential, copyrighted, or other legally protected information. If you are not the intended recipient (even if the e-mail address is yours), you may not use, copy, or retransmit it. If you have received this by mistake please notify us by return e-mail, then delete.
+~~~~~~~~~~~~~~~~~~~~~~~~+

The contents of this message may be privileged and confidential. If this message has been received in error, please delete it without reading it. Your receipt of this message is not intended to waive any applicable privilege. Please do not disseminate this message without the permission of the author. Any tax advice contained in this email was not intended to be used, and cannot be used, by you (or any other taxpayer) to avoid penalties under applicable tax laws and regulations.

For more information about Duane Morris, please visit http://www.DuaneMorris.com

Confidentiality Notice: This electronic mail transmission is privileged and confidential and is intended only for the review of the party to whom it is addressed. If you have received this transmission in error, please immediately return it to the sender. Unintended transmission shall not constitute waiver of the attorney-client or any other privilege.

EXHIBIT F

From:	Schwerin, Andrew
To:	Dotson, David C.; Logan, William; Ahearn, Terry W.; Clark, Patrick
Cc:	Vinci, Brianna; Kuo, Joseph M.; Padmanabhan, Krishnan; mflynnobrien@bdiplaw.com; Michalek, Brian R.; bentzminger@bdiplaw.com; Snedeker, Alice; Grabenstein, Casey; Tosti, Jacob A.
Subject:	RE: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation
Date:	Friday, July 26, 2024 2:20:04 PM
Attachments:	52703060-v1-2024-07-26 DRAFT Joint Stipulation to Amend Claim Construction Schedule.docx

All:

Attached is a stip that reflects the change in Dr. Striegel's deposition date, and the attendant changes to briefing. Please let us know if we have your approval to e-sign and file. Second, please let us know about the credentials for Dr. Striegel's remote deposition when you get a chance. Last, let us know your thoughts on a 12:00 pm start time.

Regards,

Andrew

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Dotson, David C. <DCDotson@duanemorris.com>
Sent: Wednesday, July 24, 2024 9:12 PM
To: Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Schwerin, Andrew <andrew.schwerin@saul.com>; Clark, Patrick <PClark@winston.com>
Cc: Vinci, Brianna <BVinci@duanemorris.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; mflynnobrien@bdiplaw.com; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com; Snedeker, Alice <AESnedeker@duanemorris.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>; Tosti, Jacob A. <jacob.tosti@saul.com>
Subject: Re: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

That works for fortinet as well.

David

On Jul 24, 2024 8:52 PM, "Logan, William" <WLogan@winston.com> wrote:
Thanks Andrew. That works for the Winston team.

From: Schwerin, Andrew <andrew.schwerin@saul.com>
Sent: Tuesday, July 23, 2024 8:23:35 PM
To: Dotson, David C. <DCDotson@duanemorris.com>; Clark, Patrick <PClark@winston.com>; Logan,

William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>
Cc: Vinci, Brianna <BVinci@duanemorris.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; mflynnobrien@bdiplaw.com <mflynnobrien@bdiplaw.com>; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com <bentzminger@bdiplaw.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>; Tosti, Jacob A. <jacob.tosti@saul.com>
Subject: RE: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

All: How does August 1 work for everyone?

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Dotson, David C. <DCDotson@duanemorris.com>
Sent: Monday, July 22, 2024 9:53 AM
To: Schwerin, Andrew <andrew.schwerin@saul.com>; Clark, Patrick <PClark@winston.com>; Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>
Cc: Vinci, Brianna <BVinci@duanemorris.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; mflynnobrien@bdiplaw.com; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com; Snedeker, Alice <AESnedeker@duanemorris.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>; Tosti, Jacob A. <jacob.tosti@saul.com>
Subject: RE: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

Hi Andrew,

For Fortinet, our team has a pre-trial conference July 31st in another matter, so that day won't work on our end. Can you provide additional dates Dr. Striegel is available?

Thanks,
David

From: Schwerin, Andrew <andrew.schwerin@saul.com>
Sent: Monday, July 22, 2024 9:48 AM
To: Clark, Patrick <PClark@winston.com>; Dotson, David C. <DCDotson@duanemorris.com>; Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>
Cc: Vinci, Brianna <BVinci@duanemorris.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; mflynnobrien@bdiplaw.com; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com; Snedeker, Alice <AESnedeker@duanemorris.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>; Tosti, Jacob A. <jacob.tosti@saul.com>

Subject: RE: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

Hi Patrick:

In view of the CrowdStrike outage and cancelling Dr. Striegel's deposition on Friday, we wanted to propose a plan going forward. In terms of Dr. Striegel's deposition, he does not have availability next week. He is next available for his deposition on July 31. Let us know if this date works for you.

As consistent with that deposition date we further propose August 12, August 26, and September 4 respectively for the parties' opening, responsive and reply claim construction briefs. We can draft a stipulation and circulate to you no later than early next week.

Regards,

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Clark, Patrick <PClark@winston.com>
Sent: Friday, July 19, 2024 2:41 PM
To: Schwerin, Andrew <andrew.schwerin@saul.com>; Dotson, David C. <DCDotson@duanemorris.com>; Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>
Cc: Vinci, Brianna <BVinci@duanemorris.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; mflynnobrien@bdiplaw.com; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com; Snedeker, Alice <AESnedeker@duanemorris.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>; Tosti, Jacob A. <jacob.tosti@saul.com>
Subject: Re: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

Andrew,

In light of today's technical issues, we're reaching out to reschedule Dr. Striegel's deposition. Does he have availability on Thursday, July 25, or Friday, July 26, next week?

Thank you,

Patrick Clark
Winston & Strawn LLP
D: +1 214-453-6492
M: +1 724-388-1732
winston.com

From: Schwerin, Andrew <andrew.schwerin@saul.com>
Sent: Monday, July 15, 2024 9:19 AM
To: Dotson, David C. <DCDotson@duanemorris.com>; Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>
Cc: Vinci, Brianna <BVinci@duanemorris.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; mflynnobrien@bdiplaw.com <mflynnobrien@bdiplaw.com>; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com <bentzminger@bdiplaw.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>; Tosti, Jacob A. <jacob.tosti@saul.com>
Subject: RE: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

Thanks all. We'll get this on file in both cases and send a copy to Judge Gonzalez Rogers.

- Andrew

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Dotson, David C. <DCDotson@duanemorris.com>
Sent: Friday, July 12, 2024 7:04 PM
To: Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Schwerin, Andrew <andrew.schwerin@saul.com>; Clark, Patrick <PClark@winston.com>
Cc: Vinci, Brianna <BVinci@duanemorris.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; mflynnobrien@bdiplaw.com; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com; Snedeker, Alice <AESnedeker@duanemorris.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>; Tosti, Jacob A. <jacob.tosti@saul.com>
Subject: Re: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

Good for Fortinet. You can use my signature.

David

On Jul 12, 2024 6:56 PM, "Clark, Patrick" <PClark@winston.com> wrote:

Andrew,

Cisco approves of that edit. Upon Fortinet's approval, is InfoExpress willing to file the stipulation in both cases? If that works, you have our permission to add KP's signature.

Thanks,

Patrick Clark
Winston & Strawn LLP
D: +1 214-453-6492
M: +1 724-388-1732
winston.com

From: Schwerin, Andrew <andrew.schwerin@saul.com>
Sent: Friday, July 12, 2024 4:01:20 PM
To: Clark, Patrick <PClark@winston.com>; Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>
Cc: Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com <bentzminger@bdiplaw.com>; mflynnobrien@bdiplaw.com <mflynnobrien@bdiplaw.com>; Tosti, Jacob A. <jacob.tosti@saul.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Dotson, David C. <DCDotson@duanemorris.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Vinci, Brianna <BVinci@duanemorris.com>
Subject: RE: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

Counsel: Thanks for preparing this. One small edit in redline (to Dr. Striegel's name). If you accept that edit, you have our permission to sign Brian Michalek's name and file it.

- Andrew

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Clark, Patrick <PClark@winston.com>
Sent: Friday, July 12, 2024 1:45 PM
To: Schwerin, Andrew <andrew.schwerin@saul.com>; Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>
Cc: Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com; mflynnobrien@bdiplaw.com; Tosti, Jacob A. <jacob.tosti@saul.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Dotson, David C. <DCDotson@duanemorris.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Vinci, Brianna <BVinci@duanemorris.com>
Subject: RE: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

Counsel:

We've attached a joint proposed stipulation to extend the claim construction schedule by one week

to provide additional time for Dr. Striegel's deposition. Please let us know whether you have any edits or comments.

Thank you,

Patrick Clark
Winston & Strawn LLP
D: +1 214-453-6492
M: +1 724-388-1732
winston.com

From: Schwerin, Andrew <andrew.schwerin@saul.com>
Sent: Thursday, July 11, 2024 8:27 AM
To: Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>
Cc: Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com; mflynnobrien@bdiplaw.com; Tosti, Jacob A. <jacob.tosti@saul.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Dotson, David C. <DCDotson@duanemorris.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Vinci, Brianna <BVinci@duanemorris.com>
Subject: RE: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

Hi William: InfoExpress has decided to forego taking Dr. Reddy's deposition. As for Dr. Striegel's deposition, he will be available on July 19 at 1:00 pm EDT. Please send the remote deposition credentials when you can.

Thanks,

Andrew

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Logan, William <WLogan@winston.com>
Sent: Tuesday, July 9, 2024 12:48 PM
To: Schwerin, Andrew <andrew.schwerin@saul.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>

Cc: Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com; mflynnobrien@bdiplaw.com; Tosti, Jacob A. <jacob.tosti@saul.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Dotson, David C. <DCDotson@duanemorris.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Vinci, Brianna <BVinci@duanemorris.com>
Subject: RE: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

Thanks Andrew. We confirm July 19 for Dr. Striegel. As to Dr. Reddy, he will be ready to begin on July 12 at 10:00 AM CT. Please provide connection and exhibit sharing details for Dr. Reddy at your earliest convenience.

William Logan
Associate Attorney
Winston & Strawn LLP
T: +1 713-651-2600
D: +1 713-651-2766
F: +1 713-651-2700
Email | winston.com
Pronouns: He, Him, His

From: Schwerin, Andrew <andrew.schwerin@saul.com>
Sent: Wednesday, July 3, 2024 12:49 PM
To: Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>
Cc: Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com; mflynnobrien@bdiplaw.com; Tosti, Jacob A. <jacob.tosti@saul.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Dotson, David C. <DCDotson@duanemorris.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Vinci, Brianna <BVinci@duanemorris.com>
Subject: RE: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

William:

In addition to the dates we previously provided, we can also offer Dr. Aaron Striegel on the following dates:

- Tuesday, July 16, and
- Friday, July 19.

Please let us know which of these might work for you, so that Dr. Striegel can make arrangements.

We are fine with 2.5 hours record time for each deposition.

Thanks,

Andrew

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Logan, William <WLogan@winston.com>
Sent: Monday, July 1, 2024 8:44 AM
To: Schwerin, Andrew <andrew.schwerin@saul.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>
Cc: Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com; mflynnobrien@bdiplaw.com; Tosti, Jacob A. <jacob.tosti@saul.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Dotson, David C. <DCDotson@duanemorris.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Vinci, Brianna <BVinci@duanemorris.com>
Subject: Re: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

Hi Andrew,

July 10 and 11 pose significant conflicts for us. Would you please provide some additional dates when Dr. Striegel is available for deposition? We may be agreeable to a reasonable extension of the expert discovery deadline of a week if that would help. Also, please confirm whether you agree 2.5 hours on the record is sufficient for these depositions.

Thanks,
William

From: Schwerin, Andrew <andrew.schwerin@saul.com>
Sent: Friday, June 28, 2024 2:53:08 PM
To: Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>
Cc: Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com <bentzminger@bdiplaw.com>; mflynnobrien@bdiplaw.com <mflynnobrien@bdiplaw.com>; Tosti, Jacob A. <jacob.tosti@saul.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Dotson, David

C. <DCDotson@duanemorris.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Vinci, Brianna <BVinci@duanemorris.com>
Subject: RE: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

Counsel: Dr. Striegel can be available for his deposition on July 10 and 11. On the 10th, we would need a hard stop at 5:00 pm EDT due to a prior scheduling commitment. Please let us know at your earliest convenience which of these dates you prefer.

Regards,

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Schwerin, Andrew
Sent: Friday, June 21, 2024 1:02 PM
To: Logan, William <WLogan@winston.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>
Cc: Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com; mflynnobrien@bdiplaw.com; Tosti, Jacob A. <jacob.tosti@saul.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Dotson, David C. <DCDotson@duanemorris.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Vinci, Brianna <BVinci@duanemorris.com>
Subject: RE: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

William:

Thank you for the update. InfoExpress agrees to July 12 for Dr. Reddy's deposition.

- Andrew

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Logan, William <WLogan@winston.com>
Sent: Friday, June 21, 2024 11:19 AM
To: Schwerin, Andrew <andrew.schwerin@saul.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>
Cc: Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>;

Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com; mflynnobrien@bdiplaw.com; Tosti, Jacob A. <jacob.tosti@saul.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Dotson, David C. <DCDotson@duanemorris.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Vinci, Brianna <BVinci@duanemorris.com>
Subject: RE: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

Counsel:

Dr. Reddy will be available for his deposition on Friday, July 12. Please confirm this date as soon as possible as we cannot hold it indefinitely. Also, Defendants intend to drop the following terms for claim construction: "3. access control," "6. and that concerns antivirus software," "11. monitor," "12. protected network," and "13. update module."

Thanks,
William

William Logan
Associate Attorney
Winston & Strawn LLP
T: +1 713-651-2600
D: +1 713-651-2766
F: +1 713-651-2700
Email | winston.com
Pronouns: He, Him, His
WINSTON & STRAWN LLP

From: Schwerin, Andrew <andrew.schwerin@saul.com>
Sent: Thursday, June 13, 2024 9:16 AM
To: Ahearn, Terry W. <TWAhearn@duanemorris.com>; Clark, Patrick <PClark@winston.com>
Cc: Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com; mflynnobrien@bdiplaw.com; Tosti, Jacob A. <jacob.tosti@saul.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Dotson, David C. <DCDotson@duanemorris.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Logan, William <WLogan@winston.com>; Vinci, Brianna <BVinci@duanemorris.com>
Subject: RE: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

Thanks—InfoExpress will go ahead and file this.

- Andrew

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Ahearn, Terry W. <TWAhearn@duanemorris.com>
Sent: Wednesday, June 12, 2024 11:55 PM
To: Clark, Patrick <PClark@winston.com>
Cc: Schwerin, Andrew <andrew.schwerin@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com; mflynnobrien@bdiplaw.com; Tosti, Jacob A. <jacob.tosti@saul.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Dotson, David C. <DCDotson@duanemorris.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Logan, William <WLogan@winston.com>; Vinci, Brianna <BVinci@duanemorris.com>
Subject: Re: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

June 28 works for Fortinet as well. Andrew, can IE file for both cases like last time? That small edit was fine.

On Jun 12, 2024, at 8:51 PM, Clark, Patrick <PClark@winston.com> wrote:

Counsel:

Cisco approves the draft stipulation for filing and June 28 as the deadline to exchange expert reports.

Best regards,

Patrick Clark
Winston & Strawn LLP
D: +1 214-453-6492
M: +1 724-388-1732
winston.com
<image001.jpg>

From: Ahearn, Terry W. <TWAhearn@duanemorris.com>
Sent: Wednesday, June 12, 2024 1:29 PM
To: Schwerin, Andrew <andrew.schwerin@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com; mflynnobrien@bdiplaw.com; Tosti, Jacob A. <jacob.tosti@saul.com>
Cc: Snedeker, Alice <AESnedeker@duanemorris.com>; Dotson, David C. <DCDotson@duanemorris.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Clark, Patrick <PClark@winston.com>; Logan, William <WLogan@winston.com>; Vinci, Brianna

<BVinci@duanemorris.com>
Subject: RE: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

Thank you Andrew. We will get back to you on the expert report exchange date.

<image007.jpg>

www.duanemorris.com
Terry W. Ahearn
Partner
Duane Morris LLP
260 Homer Ave., #202
Palo Alto, CA 94301-2777
P: +1 650 847 4144
F: +1 650 403 1902
E-MAIL | VCARD

From: Schwerin, Andrew <andrew.schwerin@saul.com>
Sent: Wednesday, June 12, 2024 6:14 AM
To: Ahearn, Terry W. <TWAhearn@duanemorris.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com; mflynnobrien@bdiplaw.com; Tosti, Jacob A. <jacob.tosti@saul.com>
Cc: Snedeker, Alice <AESnedeker@duanemorris.com>; Dotson, David C. <DCDotson@duanemorris.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Clark, Patrick <PClark@winston.com>; Logan, William <WLogan@winston.com>; Vinci, Brianna <BVinci@duanemorris.com>
Subject: RE: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

Terry, all:

Thanks for drafting. One small edit in redline. You have our permission to file.

Also, we didn't hear back on our request for a date for exchanging expert reports. How does June 28 work for everyone here?

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Ahearn, Terry W. <TWAhearn@duanemorris.com>
Sent: Tuesday, June 11, 2024 5:40 PM
To: Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; Michalek, Brian R. <brian.michalek@saul.com>; bentzminger@bdiplaw.com; mflynnobrien@bdiplaw.com; Tosti, Jacob A. <jacob.tosti@saul.com>; Schwerin, Andrew

<andrew.schwerin@saul.com>
Cc: Ahearn, Terry W. <TWAhearn@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Dotson, David C. <DCDotson@duanemorris.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Clark, Patrick <PClark@winston.com>; Logan, William <WLogan@winston.com>; Vinci, Brianna <BVinci@duanemorris.com>
Subject: InfoExpress v. Cisco/Fortinet - Claim Construction Discovery DRAFT Stipulation

****EXTERNAL EMAIL** - This message originates from outside our Firm. Please consider carefully before responding or clicking links/attachments.**

IE Team and Cisco Team,

Attached is a draft stipulation to extend claim construction deadlines. Please let us know if you have any edits or comments or whether we have your permission to file. Thank you.

Terry

Terry W. Ahearn
Partner

Duane Morris LLP
260 Homer Ave., #202
Palo Alto, CA 94301-2777
P: +1 650 847 4144
F: +1 650 403 1902

C: +1 408 623 2613

TWAhearn@duanemorris.com
www.duanemorris.com

<image008.jpg>

Check out our Duane Morris Law Blogs

<image009.png>

For more information about Duane Morris, please visit http://www.DuaneMorris.com

Confidentiality Notice: This electronic mail transmission is privileged and confidential and is intended only for the review of the party to whom it is addressed. If you have received this transmission in error, please immediately return it to the sender. Unintended transmission shall not constitute waiver of the attorney-client or any other privilege.

"Saul Ewing LLP (saul.com)" has made the following annotations:
+~~~~~~~~~~~~~~~~~~~~~~~~+
This e-mail may contain privileged, confidential, copyrighted, or other legally protected information. If you are not the intended recipient (even if the e-mail address is yours), you may not use, copy, or retransmit it. If you have received this by mistake please notify us by return e-mail, then delete.

+~~~~~~~~~~~~~~~~~~~~~~~~~+

The contents of this message may be privileged and confidential. If this message has been received in error, please delete it without reading it. Your receipt of this message is not intended to waive any applicable privilege. Please do not disseminate this message without the permission of the author. Any tax advice contained in this email was not intended to be used, and cannot be used, by you (or any other taxpayer) to avoid penalties under applicable tax laws and regulations.

<image003.png>

EXHIBIT G

From: Schwerin, Andrew
To: Logan, William; Dillner, Julie K.; Enzminger, David; David Lesht; Eamon Kelly; Padmanabhan, Krishnan; Clark, Patrick; Michalek, Brian R.; Streifthau-Livizos, Michelle C.
Subject: RE: InfoExpress v. Cisco [23-cv-02698] and Fortinet [23-cv-04389] | Service of Sealed Filings
Date: Thursday, May 9, 2024 2:29:25 PM
Attachments: image003.png
image004.png
image005.png
image006.png
image007.png
image008.png

Good by us—you have our consent to file.

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Logan, William <WLogan@winston.com>
Sent: Thursday, May 9, 2024 3:13 PM
To: Schwerin, Andrew <andrew.schwerin@saul.com>; Dillner, Julie K. <julie.dillner@saul.com>; Enzminger, David <DEnzminger@winston.com>; David Lesht <dlesht@sperling-law.com>; Eamon Kelly <ekelly@sperling-law.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Clark, Patrick <PClark@winston.com>; Michalek, Brian R. <brian.michalek@saul.com>; Streifthau-Livizos, Michelle C. <michelle.streifthau-livizos@saul.com>
Subject: RE: InfoExpress v. Cisco [23-cv-02698] and Fortinet [23-cv-04389] | Service of Sealed Filings

Thanks Andrew. Let us know if the minor edits in the attached for clarify are acceptable.

William Logan
Associate Attorney
Winston & Strawn LLP
T: +1 713-651-2600
D: +1 713-651-2766
F: +1 713-651-2700
Email | winston.com
Pronouns: He, Him, His
WINSTON & STRAWN LLP

From: Schwerin, Andrew <andrew.schwerin@saul.com>
Sent: Thursday, May 9, 2024 12:00 PM
To: Logan, William <WLogan@winston.com>; Dillner, Julie K. <julie.dillner@saul.com>; Enzminger, David <DEnzminger@winston.com>; David Lesht <dlesht@sperling-law.com>; Eamon Kelly <ekelly@sperling-law.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Clark, Patrick <PClark@winston.com>; Michalek, Brian R. <brian.michalek@saul.com>; Streifthau-Livizos,

Michelle C. <michelle.streifthau-livizos@saul.com>
Subject: RE: InfoExpress v. Cisco [23-cv-02698] and Fortinet [23-cv-04389] | Service of Sealed Filings

William: Please see our edits in redline. You have our permission to accept these changes and file this (along with the declaration and proposed order). If you make any more changes, please confer with us first before filing.

Regards,

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Logan, William <WLogan@winston.com>
Sent: Wednesday, May 8, 2024 8:15 PM
To: Schwerin, Andrew <andrew.schwerin@saul.com>; Dillner, Julie K. <julie.dillner@saul.com>; Enzminger, David <DEnzminger@winston.com>; David Lesht <dlesht@sperling-law.com>; Eamon Kelly <ekelly@sperling-law.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Clark, Patrick <PClark@winston.com>; Michalek, Brian R. <brian.michalek@saul.com>; Streifthau-Livizos, Michelle C. <michelle.streifthau-livizos@saul.com>
Subject: RE: InfoExpress v. Cisco [23-cv-02698] and Fortinet [23-cv-04389] | Service of Sealed Filings

Thanks Andrew. A draft stipulation and proposed order are attached. Let us know if you have any edits or if we have permission to file.

William Logan
Associate Attorney
Winston & Strawn LLP
T: +1 713-651-2600
D: +1 713-651-2766
F: +1 713-651-2700
Email | winston.com
Pronouns: He, Him, His
WINSTON & STRAWN LLP

From: Schwerin, Andrew <andrew.schwerin@saul.com>
Sent: Wednesday, May 8, 2024 10:02 AM
To: Logan, William <WLogan@winston.com>; Dillner, Julie K. <julie.dillner@saul.com>; Enzminger, David <DEnzminger@winston.com>; David Lesht <dlesht@sperling-law.com>; Eamon Kelly <ekelly@sperling-law.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Clark,

Patrick <PClark@winston.com>; Michalek, Brian R. <brian.michalek@saul.com>; Streifthau-Livizos, Michelle C. <michelle.streifthau-livizos@saul.com>
Subject: RE: InfoExpress v. Cisco [23-cv-02698] and Fortinet [23-cv-04389] | Service of Sealed Filings

Hi William: InfoExpress agrees to Cisco filing its reply on Monday, May 13. If you're planning on filing a stip with the court, can you send us a copy for our review?

Thanks,

Andrew

From: Logan, William <WLogan@winston.com>
Sent: Wednesday, May 8, 2024 8:24 AM
To: Dillner, Julie K. <julie.dillner@saul.com>; Enzminger, David <DEnzminger@winston.com>; dlesht@sperling-law.com; ekelly@sperling-law.com; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Clark, Patrick <PClark@winston.com>
Cc: Streifthau-Livizos, Michelle C. <michelle.streifthau-livizos@saul.com>; Michalek, Brian R. <brian.michalek@saul.com>
Subject: Re: InfoExpress v. Cisco [23-cv-02698] and Fortinet [23-cv-04389] | Service of Sealed Filings

****EXTERNAL EMAIL** - This message originates from outside our Firm. Please consider carefully before responding or clicking links/attachments.**

Counsel:

Given service of the sealed filings on Saturday, please confirm you will stipulate to Cisco filing its reply on Monday, May 13.

Thanks,
William

William Logan
Associate Attorney
Winston & Strawn LLP
D +1 (713) 651-2766

From: Dillner, Julie K. <julie.dillner@saul.com>
Sent: Saturday, May 4, 2024 7:38:03 AM
To: Enzminger, David <DEnzminger@winston.com>; dlesht@sperling-law.com <dlesht@sperling-law.com>; ekelly@sperling-law.com <ekelly@sperling-law.com>; Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Clark, Patrick <PClark@winston.com>; Logan, William <WLogan@winston.com>
Cc: Streifthau-Livizos, Michelle C. <michelle.streifthau-livizos@saul.com>; Michalek, Brian R.

<brian.michalek@saul.com>
Subject: InfoExpress v. Cisco [23-cv-02698] and Fortinet [23-cv-04389] | Service of Sealed Filings

Good morning:

Please note your access to the securemail sent last night have been removed. A revised transmission will be sent shortly. Please delete any documents you have downloaded from this transmission as it was sent in error.

Thanks,

Julie Dillner, CEDS
Paralegal
Pronouns: She/her/hers
(312) 876-6909
julie.dillner@saul.com

SAUL EWING LLP
161 North Clark
Suite 4200
Chicago, IL 60601

"Saul Ewing LLP (saul.com)" has made the following annotations:
+~~~~~~~~~~~~~~~~~~~~~~~~+
This e-mail may contain privileged, confidential, copyrighted, or other legally protected information. If you are not the intended recipient (even if the e-mail address is yours), you may not use, copy, or retransmit it. If you have received this by mistake please notify us by return e-mail, then delete.
+~~~~~~~~~~~~~~~~~~~~~~~~+

The contents of this message may be privileged and confidential. If this message has been received in error, please delete it without reading it. Your receipt of this message is not intended to waive any applicable privilege. Please do not disseminate this message without the permission of the author. Any tax advice contained in this email was not intended to be used, and cannot be used, by you (or any other taxpayer) to avoid penalties under applicable tax laws and regulations.

EXHIBIT H

From: Schwerin, Andrew
To: Dotson, David C.; Michalek, Brian R.; Grabenstein, Casey; Kuo, Joseph M.; mflynnobrien@bdiplaw.com
Cc: Padmanabhan, Krishnan; Logan, William; Clark, Patrick; Gaudet, Matthew C.; Snedeker, Alice; Ahearn, Terry W.
Subject: RE: InfoExpress v. Cisco, Fortinet - Follow-up From Court"s Video Conference
Date: Thursday, May 9, 2024 1:52:25 PM

That's no problem; we'll file in both case.

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Dotson, David C. <DCDotson@duanemorris.com>
Sent: Thursday, May 9, 2024 2:34 PM
To: Schwerin, Andrew <andrew.schwerin@saul.com>; Michalek, Brian R. <brian.michalek@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; mflynnobrien@bdiplaw.com
Cc: Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Logan, William <WLogan@winston.com>; Clark, Patrick <PClark@winston.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>
Subject: RE: InfoExpress v. Cisco, Fortinet - Follow-up From Court's Video Conference

Andrew—these changes are fine with Fortinet and Cisco. Since it will presumably need to be filed in both cases, it probably makes sense for IE to file. Does that work for you?

David

From: Schwerin, Andrew <andrew.schwerin@saul.com>
Sent: Thursday, May 9, 2024 1:38 PM
To: Dotson, David C. <DCDotson@duanemorris.com>; Michalek, Brian R. <brian.michalek@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; mflynnobrien@bdiplaw.com
Cc: Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Logan, William <WLogan@winston.com>; Clark, Patrick <PClark@winston.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>
Subject: RE: InfoExpress v. Cisco, Fortinet - Follow-up From Court's Video Conference

David, thank you for preparing this. InfoExpress's edits are in redline. We took the liberty of adding a proposed order for the judge to sign. You have our permission to accept changes and to file a clean version. If you have any other edits, please run them by us.

Best,

Andrew Schwerin
Associate
SAUL EWING LLP | Philadelphia
Office: (215) 972-7184

From: Dotson, David C. <DCDotson@duanemorris.com>
Sent: Thursday, May 9, 2024 9:08 AM
To: Michalek, Brian R. <brian.michalek@saul.com>; Schwerin, Andrew <andrew.schwerin@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; mflynnobrien@bdiplaw.com
Cc: Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Logan, William <WLogan@winston.com>; Clark, Patrick <PClark@winston.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>
Subject: RE: InfoExpress v. Cisco, Fortinet - Follow-up From Court's Video Conference

Brian,

I've attached a draft Joint Statement, which includes the issue you raised below regarding consolidating the Motion to Stay hearings, as well as addressing the Parties' previously-agreed six-week extension on claim construction deadlines.

David

From: Michalek, Brian R. <brian.michalek@saul.com>
Sent: Wednesday, May 8, 2024 4:33 PM
To: Dotson, David C. <DCDotson@duanemorris.com>; Schwerin, Andrew <andrew.schwerin@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; mflynnobrien@bdiplaw.com
Cc: Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Logan, William <WLogan@winston.com>; Clark, Patrick <PClark@winston.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>
Subject: RE: InfoExpress v. Cisco, Fortinet - Follow-up From Court's Video Conference

Hi David,

Thanks for the message. However, InfoExpress does not agree to the proposed stay including for the reasons set forth in its recent opposition papers. Given your message below, please send us a draft joint statement on the case update pursuant to the Court's order for filing tomorrow.

One issue we would like to address in the statement is whether Defendants will agree to have the motion to stay hearings on the same day rather than two separate dates as currently noticed. Please let us know.

Best,

Brian

Brian R. Michalek
Partner
SAUL EWING LLP | Chicago
Office: (312) 876-7836

From: Dotson, David C. <DCDotson@duanemorris.com>
Sent: Wednesday, May 8, 2024 10:11 AM
To: Michalek, Brian R. <brian.michalek@saul.com>; Schwerin, Andrew <andrew.schwerin@saul.com>; Grabenstein, Casey <Casey.Grabenstein@saul.com>; Kuo, Joseph M. <joseph.kuo@saul.com>; mflynnobrien@bdiplaw.com
Cc: Padmanabhan, Krishnan <KPadmanabhan@winston.com>; Logan, William <WLogan@winston.com>; Clark, Patrick <PClark@winston.com>; Gaudet, Matthew C. <MCGaudet@duanemorris.com>; Snedeker, Alice <AESnedeker@duanemorris.com>; Ahearn, Terry W. <TWAhearn@duanemorris.com>
Subject: InfoExpress v. Cisco, Fortinet - Follow-up From Court's Video Conference

****EXTERNAL EMAIL** - This message originates from outside our Firm. Please consider carefully before responding or clicking links/attachments.**

Brian,

I write on behalf of Fortinet and Cisco to follow up after the Court's video conference with the parties. Fortinet and Cisco do not agree to proceed to trial before a magistrate judge. In view of the Court's impending vacatur of the claim construction hearing, admonition against the parties filing motions, etc. during the pendency of her criminal trial, and our prior agreement to extend the claim construction exchanges for six weeks, please let us know whether InfoExpress would agree to stay the cases through October 2024. At that point, the Court's criminal trial will be over and the parties will know whether the IPRs are instituted.

Thanks,
David

David C. Dotson
Partner

Duane Morris LLP
1075 Peachtree Street NE, Suite 1700
Atlanta, GA 30309-3929
P: +1 404 253 6982
F: +1 404 581 5951

DCDotson@duanemorris.com
www.duanemorris.com

For more information about Duane Morris, please visit http://www.DuaneMorris.com

Confidentiality Notice: This electronic mail transmission is privileged and confidential and is intended only for the review of the party to whom it is addressed. If you have received this transmission in error, please immediately return it to the sender. Unintended transmission shall not constitute waiver of the attorney-client or any other privilege.

"Saul Ewing LLP (saul.com)" has made the following annotations:
+~~~~~~~~~~~~~~~~~~~~~~~~+
This e-mail may contain privileged, confidential, copyrighted, or other legally protected information. If you are not the intended recipient (even if the e-mail address is yours), you may not use, copy, or retransmit it. If you have received this by mistake please notify us by return e-mail, then delete.
+~~~~~~~~~~~~~~~~~~~~~~~~+

EXHIBIT I

From:	Kennedy, Vickie
To:	Tosti, Jacob A.; Michalek, Brian R.; Grabenstein, Casey; Schwerin, Andrew; Kuo, Joseph M.; mflynnobrien@bdiplaw.com; bentzminger@bdiplaw.com; eday@bdilaw.com
Cc:	WS-Cisco-InfoExpress
Subject:	InfoExpress Inc. v. Cisco Systems, Inc. (4:23-cv-02698-YGR) -- Cisco Notice of Deposition of Dr. Striegel
Date:	Tuesday, July 9, 2024 12:45:34 PM
Attachments:	2024.07.09 Notice of Dep of Striegel (Infoexpress).pdf

Counsel,
Attached please find Cisco's Notice of Deposition of Dr. Striegel.

Vickie Kennedy

Senior Paralegal

Winston & Strawn LLP
35 W. Wacker Drive
Chicago, IL 60601-9703

D: +1 312-558-5940

F: +1 312-558-5700

VCard | Email | winston.com

EXHIBIT J

Krishnan Padmanabhan (SBN 254220)
WINSTON & STRAWN LLP
200 Park Avenue
New York, NY 10166-4193
Telephone: (212) 294-6700
Facsimile: (212) 294-4700
KPadmanabhan@winston.com

David Enzminger (SBN: 137065)
WINSTON & STRAWN LLP
333 S. Grand Avenue
Los Angeles, CA 90071
Telephone: (213) 615-1700
Facsimile: (213) 615-1750
DEnzminger@winston.com

William Logan (*pro hac vice*)
WINSTON & STRAWN LLP
800 Capitol Street, Suite 2400
Houston, TX 77002-2925
Telephone: (713) 651-2600
Facsimile: (713) 651-2700
WLogan@winston.com

Patrick Clark (*pro hac vice*)
WINSTON & STRAWN LLP
2121 N. Pearl St., Suite 900
Dallas, TX 75201
Telephone: (214) 453-6492
Facsimile: (214) 453-6400
PClark@winston.com

Attorneys for Defendant
CISCO SYSTEMS, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INFOEXPRESS INC.,

Plaintiff,

v.

CISCO SYSTEMS, INC.,

Defendant.

Case No. 4:23-cv-02698-YGR

DEFENDANT CISCO SYSTEMS, INC.'S NOTICE OF DEPOSITION OF DR. AARON STRIEGEL

PLEASE TAKE NOTICE that, pursuant to Rule 30 of the Federal Rules of Civil Procedure, Defendant Cisco Systems, Inc., by and through their counsel, will take the deposition upon oral examination of Dr. Aaron Striegel on July 19, 2024 at 1:00 pm CT. The deposition will be conducted virtually via Zoom (or by other remote videoconferencing means). This deposition will be taken upon oral examination before an officer authorized to take depositions, who may also be remote for the purposes of reporting the proceeding and may or may not be present in the presence of the deponent. The deposition will be recorded by video and/or stenographic means.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 172 of 1144
INFOEXPRESS, INC. - EX2572

Dated: July 9, 2024

WINSTON & STRAWN LLP

By: */s/ Krishnan Padmanabhan*

Krishnan Padmanabhan (SBN 254220)
WINSTON & STRAWN LLP
200 Park Avenue
New York, NY 10166-4193
Telephone: 212-294-6700
Facsimile: 212-294-4700
KPadmanabhan@winston.com

David Enzminger (SBN: 137065)
WINSTON & STRAWN LLP
333 S. Grand Avenue
Los Angeles, CA 90071
Telephone: (213) 615-1700
Facsimile: (213) 615-1750
DEnzminger@winston.com

William Logan (*pro hac vice*)
WINSTON & STRAWN LLP
800 Capitol Street, Suite 2400
Houston, TX 77002-2925
Telephone: (713) 651-2600
Facsimile: (713) 651-2700
WLogan@winston.com

Patrick Clark (*pro hac vice*)
WINSTON & STRAWN LLP
2121 N. Pearl St., Suite 900
Dallas, TX 75201
Telephone: (214) 453-6492
Facsimile: (214) 453-6400
PClark@winston.com

Attorneys for Defendant
CISCO SYSTEMS, INC.

CERTIFICATE OF SERVICE

Case No. 4:23-CV-02698-YGR

I am employed in the County of Cook, State of Illinois. I am over the age of eighteen years and not a party to the within action; my business address is 35 W. Wacker Drive, Chicago, IL 60601.

On July 9, 2024, I served the following document(s) described as

DEFENDANT CISCO SYSTEMS, INC.'S NOTICE OF DEPOSITION TO DR. AARON STRIEGEL

☑	BY ELECTRONIC SERVICE: By electronically mailing a true and correct copy through Winston & Strawn LLP's electronic mail system from *vkennedy@winston.com* to the email addresses set forth below.

SERVICE LIST

Andrew F. Schwerin , I
Saul Ewing LLP
1500 Market St.,
3800 Centre Square West 19102
Philadelphia, PA 19102
215-972-7184
Email: andrew.schwerin@saul.com

Casey T. Grabenstein
Saul Ewing Arnstein & Lehr LLP
161 N. Clark Street
Ste 4200
Chicago, IL 60601
312-876-7810
Email: casey.grabenstein@saul.com

Michael E Flynn-O'Brien
Bunsow De Mory LLP
701 El Camino Real
Redwood City, CA 94063
512-365-4972
Email: mflynnobrien@bdiplaw.com

Attorneys for Plaintiff
InfoExpress, Inc.

Brenda Helen Entzminger
Bunsow De Mory LLP
701 El Camino Real
Redwood City, CA 94063
415-425-5230
Email: bentzminger@bdiplaw.com

Joseph M. Kuo
Saul Ewing Arnstein & Lehr LLP
161 N. Clark Street
Suite 4200
Chicago, IL 60601
312-876-7100
Fax: 312-876-0288
Email: joseph.kuo@saul.com

Brian Raymond Michalek
Saul Ewing Arnstein & Lehr LLP
161 North Clark Street, Suite 4200
Chicago, IL 60601
312-876-7836
Email: brian.michalek@saul.com

Executed on July 9, 2024.

/s/ Vickie Kennedy

Vickie Kennedy

EXHIBIT K

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INFOEXPRESS INC. Plaintiff, v. CISCO SYSTEMS, INC. Defendant.	Case No. 4:23-cv-02698-YGR **DECLARATION OF A.L. NARASIMHA REDDY, PH.D.**
INFOEXPRESS INC., Plaintiff, v. FORTINET, INC., Defendant.	Case No. 4:23-cv-04389-YGR **DECLARATION OF A.L. NARASIMHA REDDY, PH.D.**

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 176 of 1144
INFOEXPRESS, INC. - EX2572

DECLARATION OF A.L. NARASIMHA REDDY, PH.D.

I, Narasimha Reddy, Ph.D., hereby declare and state as follows:

I. INTRODUCTION

1. I have written this Declaration at the request of Cisco Systems, Inc. ("Cisco") and Fortinet Inc. ("Fortinet") in this case. I understand that InfoExpress Inc. ("InfoExpress") has accused Defendants of infringing U.S. Patent Nos. 7,523,484; 8,051,460; 8,677,450; 8,578,444; 8,347,350; and 8,117,645 (collectively, the "Asserted Patents"). My declaration sets forth my opinions in detail and provides the basis for my opinions regarding the meaning of certain claim terms. If called upon to testify or be deposed in this case, I may cite the content of this Declaration and the materials cited herein, as well as the additional documents considered, and any statements or references by InfoExpress's witnesses. I further reserve the right to create demonstrative exhibits and/or provide demonstrations in support of any testimony I may provide relating to the content of this Declaration. I reserve the right to supplement or amend my opinions, and bases for them, in response to any additional evidence, testimony, discovery, argument, and/or other additional information that may be provided to me after the date of this declaration.

II. BACKGROUND AND QUALIFICATIONS

2. I am currently the Truchard Foundation Chair Professor of Electrical and Computer Engineering at Texas A&M University in College Station, Texas. I have over 30 years of experience in a wide variety of technologies and industries relating to data communications, storage systems, and distributed systems, including packet-switched network communications.

3. My academic credentials include a Bachelor of Technology degree in Electronics and Electrical Communications Engineering from the Indian Institute of Technology, Kharagpur, India, in August 1985. I then received a Master of Science and a Ph.D. in Computer Engineering from the University of Illinois at Urbana-Champaign in May 1987 and August 1990, respectively.

4. I have worked for over 25 years in the field of Electrical Engineering. My primary focus and research interest has been on computer networks, storage systems, multimedia systems, and computer architecture. I have authored and co-authored over a hundred technical papers and several book chapters related to several of these interests, including on such topics as multipath routing, route control, high-speed networks, network congestion, packet management, quality of service regulation, network security, network modeling, differentiated services, storage system enhancements, caching strategies, and multimedia system enhancements to name a few examples. I am listed as an inventor on six U.S. patents in the field of multi-node communication networks and computer systems.

5. My employment history following my graduation from the University of Illinois at Urbana-Champaign began at the IBM Almaden Research Center in San Jose, California in 1990. At IBM, I worked on projects related to disk arrays, multiprocessor communication, hierarchical storage systems, and video servers. I spent the summer of 2022 at Google and sabbaticals at IBM Research Zurich during September 2022–July 2023 and at University of Carlos III in Madrid during September 2009–February 2010.

6. In 1995, I joined the faculty of the department of Electrical Engineering at Texas A&M University, initially as an Associate Professor and was later promoted to full, tenured Professor. At Texas A&M, from 2016 to 2021, I was the Associate Agency Director for Strategic Initiatives and Centers for the Texas A&M Engineering Experiment Station (TEES), which engages in engineering and technology-oriented research and educational collaborations. Further, I also served as Associate Dean for Research in the College of Engineering during that time.

7. At Texas A&M, I have taught dozens of courses related to computer networking and communications, as well as computer architecture, multimedia systems and networks, topics in networking security, multimedia storage and delivery, as well as networking for multimedia applications. I have done research on various topics of network security including anomaly detection, botnet detection, building mechanisms in routers and switches to improve security, spammer detection

in social networks, and improving security of cyberphysical systems. I have also served on various committees for the benefit of the scientific community and the Texas A&M University community.

8. I am a member of several professional societies, including the Institute of Electrical and Electronic Engineers (IEEE), where I have been elevated to an IEEE Fellow, and the Association for Computing Machinery (ACM). I have been responsible for chairing or co-chairing numerous conferences and programs, as well as presenting research at major IEEE and ACM conferences. For example, I served as program co-chair for the 2008 5th International Conference on Broadband Communications, Networks and Systems; panels co-chair for the 2008 3rd International Conference on Communication Systems Software & Middleware; and panel chair of the IEEE Conference of High Performance Computer Architecture.

9. My presentations include invited talks at New York University in April 2024 and May 2023, a speech on manufacturing security at ENSAM, France in 2023, a keynote speech at International Conference on Information Technology–New Generations in 2013, a keynote speech at IEEE International Symposium on Computers and Communications 2010, and several invited talks including at Georgia Tech (2013), COMSNETS Conference (2013), International Conference on Networking and Communications (2012), Samsung (2011), Korea University (2011), Aijou University (2011), Catedra Series at University of Carlos III, Madrid (2009), Thomson Research, Paris (2009), Telefonica Research, Barcelona (2009), and a Distinguished Seminar at IBM Austin Research Lab (2008).

10. I have received multiple awards in the field of networks and computer architecture. I received the NSF Career Award from 1996 to 2000. I received an outstanding professor award by the IEEE student branch at Texas A&M from 1997 to 1998, an outstanding faculty award by the department of Electrical and Computer Engineering from 2003 to 2004, a Distinguished Achievement award for teaching from the former students' association of Texas A&M University, and a citation "for one of the most influential papers" from the 1st ACM Multimedia conference.

11. My curriculum vitae, which includes a more detailed summary of my background and experience, is attached as Appendix .

III. MATERIALS CONSIDERED

12. My analyses and opinions—from the perspective of a person of ordinary skill in the art ("POSITA") as of the earliest possible priority date of the Asserted Patents[1]—are based on my education, research, knowledge, and vast experience in the fields of telecommunications and networking art that are pertinent to the Asserted Patents. In forming my opinions, I have reviewed the materials cited and referenced in this Declaration, including the Asserted Patents and their file histories, related patents and their file histories, the parties' claim construction disclosures, and the evidence cited in this Declaration.

IV. COMPENSATION ASSOCIATED WITH THIS ENGAGEMENT

I am being compensated for my work related to this matter at my standard rate of $650 per hour. My compensation is not contingent on the substance of my opinions or the outcome of any issue in this case.

V. LEGAL STANDARDS FOR CLAIM CONSTRUCTION

13. I am not an attorney. I have been informed by counsel for Defendants regarding the applicable legal standards for claim construction. I have relied on these principles in forming my opinions.

A. Claim Interpretation

14. I understand that during the claim construction process, a court must determine the proper meaning and scope of the claims.

[1] The Asserted Patents are U.S. Patent Nos. 7,523,484 (the "'484 Patent"); 8,051,460 (the "'460 Patent"); 8,677,450 (the "'450 Patent"); 8,578,444 (the "'444 Patent"); 8,347,350 (the "'350 Patent"); and 8,117,645 (the "'645 Patent") (collectively, the "Asserted Patents").

15. I understand that claim construction is a matter of law and will be decided by the Court. I understand that the relevant inquiry in claim construction is the question of how a POSITA would have understood the claim terms at the time of the invention, in the context of the particular claim in which it appears as well as in light of the patent specification, the prosecution history, and any other relevant intrinsic and extrinsic evidence.

16. I understand that intrinsic evidence includes the patent as well as its claims, specification, and prosecution history. I understand that in the intrinsic evidence, the inventors of a patent may expressly define certain terms. It has been explained to me that this is known as the inventors acting as "lexicographers." I understand that where the inventors acted as their own lexicographers, those definitions control the meaning of the defined terms in the claims.

17. I understand that the prosecution history provides evidence of how the patentee and the examiner viewed the patent, and that the public has a right to rely on the patent applicant's remarks made during prosecution in determining the scope of the claimed invention. For example, arguments and amendments made during prosecution may provide an explanation of the meaning of a claim term, or further narrow the claim term that is used more broadly in the specification. In some instances, when an applicant explicitly states that some breadth of a term is excluded from their invention, that applicant may disclaim claim scope through statements, or by making specific arguments distinguishing the claimed invention over cited prior art, during prosecution.

18. I understand that, absent lexicography or disavowal, claims are given their ordinary and customary meaning in light of the specification.

19. I understand that the ordinary and customary meaning is the meaning that the term would have to a POSITA at the time of the invention.

20. I have been informed that the Court may also consider additional evidence outside the patent and prosecution history. This type of evidence is known as "extrinsic" evidence. Extrinsic evidence can include expert opinion (including opinions about what a POSITA would have known or

understood), dictionaries, treatises, and testimony. As some examples, extrinsic evidence can be useful to provide background on the technology at issue, explain how an invention works, ensure that the Court's understanding of the technical aspects of the patent aligns with that of a POSITA, or establish that a particular term in the patent or the prior art has a particular meaning in the pertinent field. I understand that extrinsic evidence must be considered in the context of the intrinsic evidence and cannot be used to change the meaning of a claim term to contradict the intrinsic evidence.

B. Indefiniteness

21. I understand that there is a requirement in patent law that a claim must particularly point out and distinctly claim the subject matter that the patentee regards as the invention. I understand that a claim is invalid for indefiniteness if the claim, read in light of the intrinsic evidence, fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention. I understand that the claim must be clear enough for a POSITA to reasonably determine the metes and bounds of the claim (i.e., understand what falls within or outside the scope of the claim), and I understand that a claim is indefinite if a POSITA cannot ascertain the boundary of the claim with reasonable certainty.

22. For example, measurements or assessments, used in a claim without a clear indication of how those measurements or assessments may be made would leave a POSITA unable to objectively determine the boundary of the claim and render that claim indefinite. Similarly, subjective terms used in a claim, where the claim or specification provides no guidance on how to measure the scope of that term, would also leave a POSITA unable to determine the boundaries of the claim term and render the claim indefinite.

23. I also understand that a claim term that lacks an antecedent basis may be indefinite if it lacks a "reasonably ascertainable meaning" to a POSITA according to the claim construction standards I described above.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 182 of 1144
INFOEXPRESS, INC. - EX2572

VI. LEVEL OF SKILL IN THE ART

24. I understand that the level of ordinary skill may be reflected by the state of the art at the time of the invention, including the prior art of record. I also understand that a POSITA would have the capability of understanding the scientific and engineering principles applicable to the pertinent art and the claimed subject matter. I understand that a POSITA has ordinary creativity and is not an automaton.

25. I understand that there are multiple factors relevant to determining the ordinary level of skill in the art, including: (i) the levels of education and experience of persons working in the field; (ii) the types of problems encountered in the field; and (iii) the sophistication of the technology. I understand that a POSITA is not a specific real individual, but rather a hypothetical individual having the qualities reflected by the factors above.

26. Based on the materials and information I have reviewed, and on my experience in the technical areas relevant to the Asserted Patents, a POSITA with respect to the Asserted Patents as of the time of the invention, i.e., the earliest possible priority date of the Asserted Patents—September 24, 2003—would have had a working knowledge of the telecommunications and network art that is pertinent to the Asserted Patents. A POSITA would have had a bachelor's degree in computer science, computer engineering, or an equivalent, and two years of relevant experience in networking and network security, and related fields. Lack of professional experience can be remedied by additional education, and vice versa.

27. For purposes of this declaration, in general, and unless otherwise noted, my statements and opinions, such as those regarding my own experience and what a POSITA would have understood or known generally (and specifically related to the references I consulted herein), reflect the knowledge that existed in the relevant field as of the earliest effective priority date of the Asserted Patents: September 24, 2003.

28. As of September 24, 2003, I would have met or exceeded the level of skill required by the above definition, and I am in a position to opine on the understanding of a POSITA as of that date.

Unless otherwise noted, my statements and opinions below about the knowledge or understanding of a POSITA should be understood to refer to the knowledge or understanding of a POSITA as of September 24, 2003.

VII. OVERVIEW OF THE ASSERTED PATENTS

29. The Asserted Patents are related, stemming from an application (U.S. Patent Appl. No. 60/505,582) filed on September 24, 2003. The disclosures of the Asserted Patents are largely the same. In the following paragraphs, I will discuss the earliest filed of the Asserted Patents, the '484 Patent, which is representative.

30. The '484 Patent relates to a network security method that purportedly controls access to resources within part of a network using an amorphous network security entity referred to as a "gatekeeper." '484 Patent at Abstract. The systems and methods of the Asserted Patents are described as including "a protected network physically or logically divided into a restricted subset and one or more less-restricted subsets." '484 Patent at 2:48–50. They elaborate that "[r]equests from an access device for access to the less-restricted subset are first passed to the restricted subset." *Id*. at 2:50–52. Asserted independent claim 1 is exemplary of the concepts, which are claimed in the Asserted Patents. It relates to a "network gatekeeper comprising" the following: (1) a security policy including requirements that must be satisfied for an access device to be granted access to a "less-restricted subset" of a protected network; and (2) a policy auditor that audits the access device using a security policy, in response to a request to access the less-restricted subset of the protected network. The claim elaborates that this request is sent from the access device to the gatekeeper, the gatekeeper being on or part of the "restricted subset" of the protected network; and (3) an access control that reconfigures the communication device if the access device meets the requirements of the security policy.

31. The gatekeeper "sends commands to the access point in order to reconfigure the communication port through which the access request was received." '484 Patent at 5:42–45. The gatekeeper authenticates the user. '484 Patent at 10:34. In addition, the gatekeeper may also have

updating and storing functions. '484 Patent at 6:14–16 (". . . a single computing device [is] configured to function as both Update Module 255 and GateKeeper 225."); '484 Patent at 6:59–61 ("Security policies may be stored on GateKeeper 225, on Policy Manager 250, or elsewhere accessible to Restricted Subset 205."). While the term is characterized as a "gatekeeper," "future general network traffic between" the access device and the less-restricted subset may pass "without passing through" the gatekeeper if access has been granted. '484 Patent at 10:4–8.

32. The concept of a "gatekeeper" in the Asserted Patents appears to relate to a variety of different physical structures and/or logical techniques. In Fig. 2, the gatekeeper is shown as a box in a "restricted subset" of the network. '484 Patent at 5:51–58; Fig. 2. The '484 Patent describes that in one embodiment, the gatekeeper can be a server. '484 Patent at 6:11–14 (". . . Restricted Subset 205 includes a server configured to function as DHCP 260 and a server configured to function as GateKeeper 225."). In another embodiment, the gatekeeper can be a single computing device. '484 Patent at 6:14–16 (". . . a single computing device [is] configured to function as both Update Module 255 and GateKeeper 225."). In some embodiments, there is only "a single instance of" a gatekeeper within the protected network, whereas in some other embodiments, there are "a plurality of gatekeepers." '484 Patent at 6:61–7:6. Further, in some embodiments, "various aspects of GateKeeper 225 may be incorporated into Access Point 215 and/or Router 220." '484 Patent at 15:32–36. As shown in Fig. 2, the access points and the routers are neither part of the less-restricted subset nor part of the restricted subset. '484 Patent at Fig. 2. The '484 Patent thus claims a "gatekeeper" that can be one computing device, multiple computing devices, one server, or multiple servers and can be located anywhere in the network.

33. Such uncertainties plague the Asserted Patents, making various aspects of the claims indefinite. A POSITA would not be able to reasonably determine the metes and bounds of the claim (i.e., understand what falls within or outside the scope of the claim) primarily because of the uncertainty as to where the amorphous gatekeeper resides and what constitutes a gatekeeper.

VIII. THE CLAIM TERMS

A. "gatekeeper" ('484 Patent: Claims 1–5, 11–13, 15–20, 23–25, 27, 28, 41, 43, 56, 57, 68; '460 Patent: Claims 1, 5, 16, 20, 22; '444 Patent: Claim 22)

Defendants' Construction	Plaintiff's Construction
Indefinite	Plain and ordinary meaning; no construction necessary

34. As an initial matter, "gatekeeper" is not a term of art. Although the '484 Patent recites the term "gatekeeper" nearly 100 times in the specification, a POSITA could not come to any other conclusion than that it is simply some abstract and amorphous concept of network security. The specification reveals that it relates to a variable scope of functions and structures. The specification explains that the gatekeeper is "configured to administer a security policy governing access to those parts of the protected computing network that are not part of the restricted subset." '484 Patent at 5:34–36.

35. However, what the gatekeeper **is**, and where it is **located**, are both black boxes. Starting first with the location of the gatekeeper, the specification and claims offer a variety of contradictory disclosures. First, in the background section, the gatekeeper may reside between the access device and the secure network. *See* '484 Patent at 1:53–56. In this way, the gatekeeper acts like a firewall. This setup was well known at the time, for instance, as depicted below.

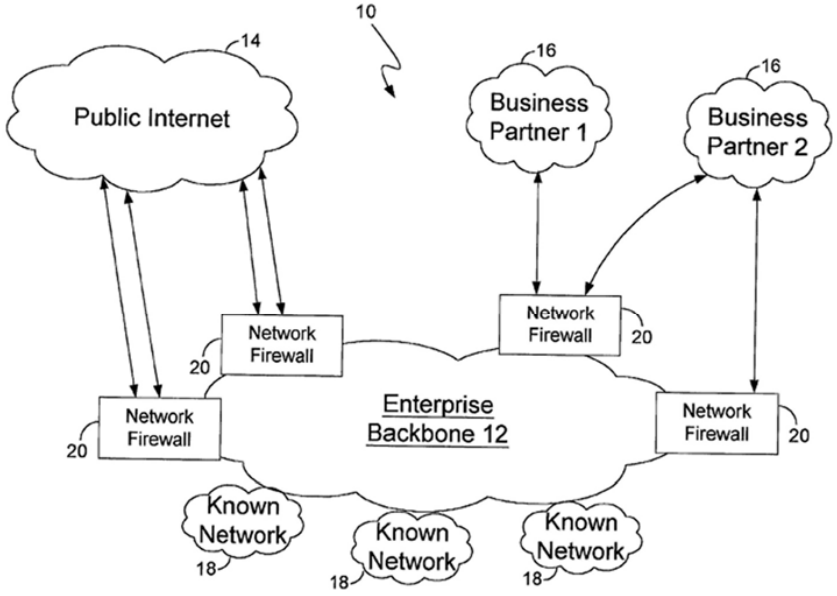


FIG. 1

See, e.g., U.S. Patent Application Publication No. 2001/0037384 A1 (attached hereto as Ex. 1) at Fig. 1; *see also id.* at [0008] (explaining that "**the network firewall 20** is made up of devices that provide the interconnections between these network categories. The **network firewall is located between the internal network and the external network**, e.g., the public Internet 14, and at any direct links to other companies. End-user hosts, internal Servers and known networks 18 are part of the internal network . . . "). This is a simple concept to understand—the "gatekeeper," in this instance, is like a "wall" protecting the network.

36. The '484 Patent does not provide this level of clarity, however. It explains that "Access Point 215" (not the GateKeeper 225) may be "a remote access virtual private network (VPN), secure socket layer VPN, **firewall**, or the like." '484 Patent at 7:51–61; *see also id.* at Fig. 3A below (with emphasis added highlighting the Access Point 215 and GateKeeper 225):

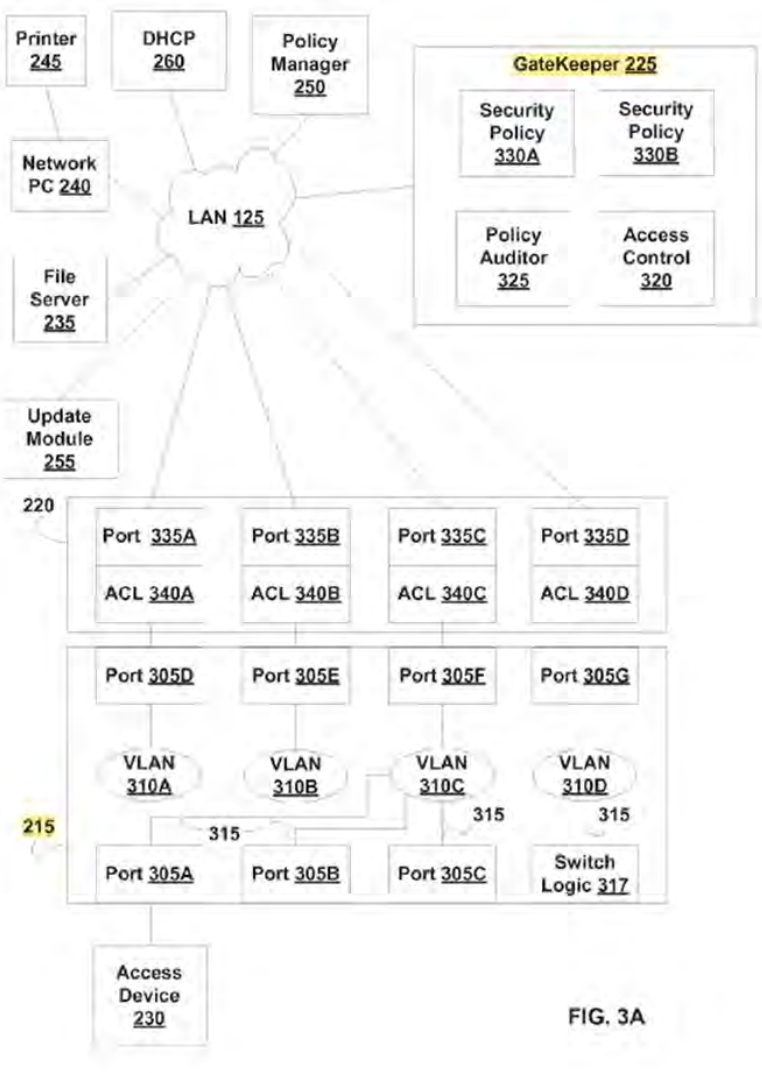


FIG. 3A

37. Indeed, the gatekeeper is discussed as residing within a "restricted subset of the protected network." *See, e.g.*, '484 Patent at 4:10–24. When an access device seeks access to a less-restricted portion of the network, such "[r]equests . . . are first passed to the restricted subset." *Id*. at 2:50–52. The gatekeeper "of the restricted subset" can apply security policies at that point. *Id*. at 2:52–56.

38. The "gatekeeper" appears to be acting like a firewall as discussed *supra* (*see also* '484 Patent at 1:53–63), but the concept of a "gatekeeper," as described in the specification, is so amorphous that it could be any number of other things such as a switch, software-defined network router, and/or a generic authentication device. *See, e.g.*, '484 Patent at 1:31–40 ("[A] network switch is programmed to

grant access to a secure network only after proper authentication is achieved."); *id*. at 2:62–3:4 ("[T]he less-restricted subset of the protected network and the restricted subset of the protected network are characterized by [VLANs] defined within the access point and optionally by access control lists (ACL) of a router, firewall, or switch situated between the VLAN and the protected network."); *id*. at 2:14–19 ("GateKeeper 110 is configured to control access to Secure Network 100. In addition to authenticating users who wish to access Secure Network 100 using an Access Device 160, GateKeeper 110 is configured to ensure that Access Device 160 conforms to a predetermined security policy, before granting access to Secure Network 100."). And the gatekeeper can even control VLAN traffic. *See, e.g.*, *id*. at 3:16–20 ("For example, the restricted VLAN allows traffic to pass to a gatekeeper configured to receive requests for access to the less-restricted VLAN, and to determine if, and to what extent, access may be allowed."). Indeed, the specification even notes that "[i]n some embodiments, various aspects of GateKeeper 225 may be **incorporated into Access Point 215** and/or Router 220" even though the functionality is intended to reside on the restricted portion of the network and the gatekeeper is supposed to "send[] commands to the access point" that resides at a different location. *Id*. at 15:32–34 (emphasis added); 5:42–45; *see also id.* at Figs. 2 and 5 (emphasis added).

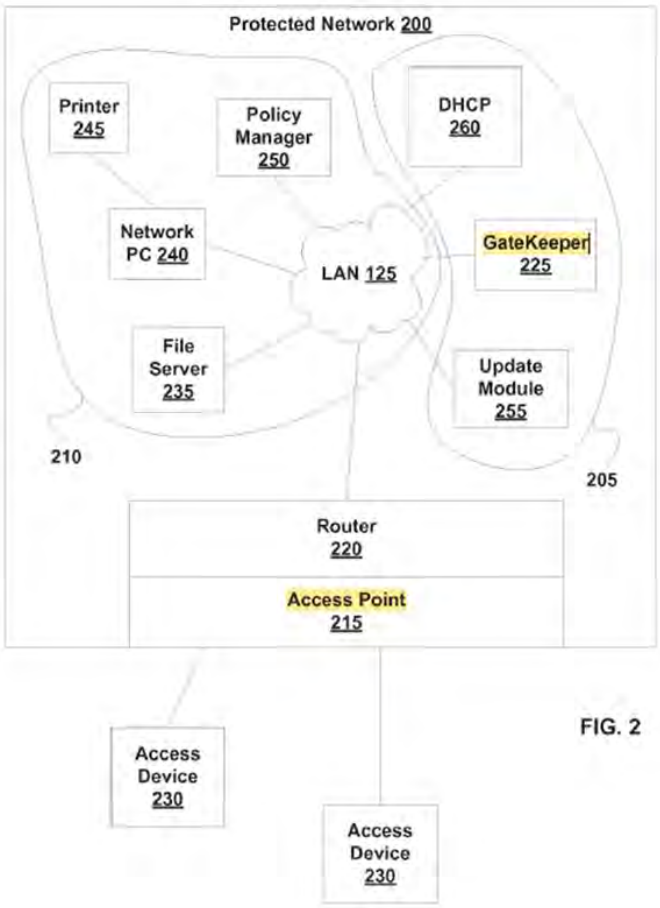


FIG. 2

Id. at Fig. 2 (emphasis added).

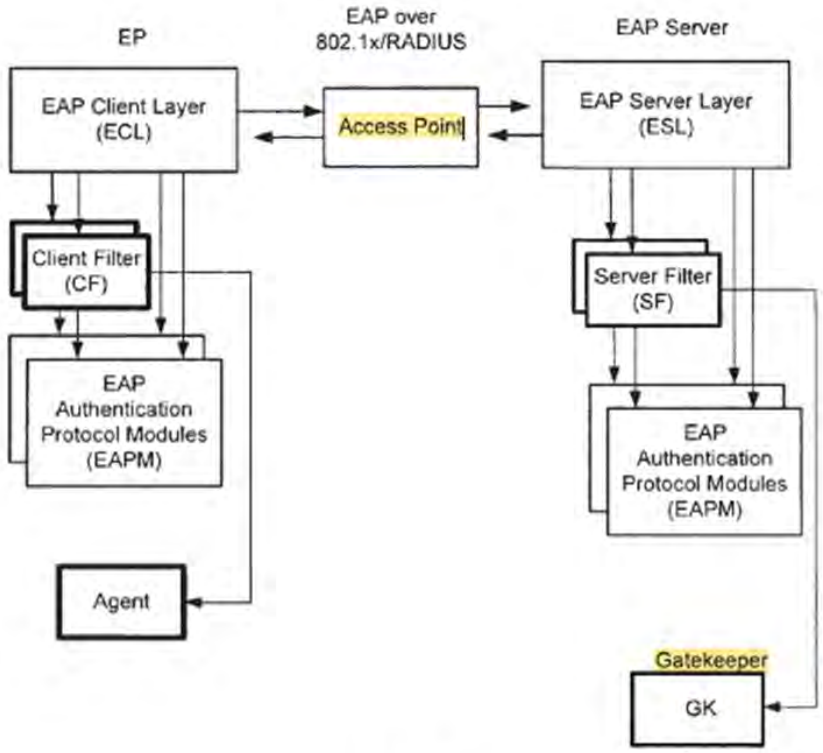
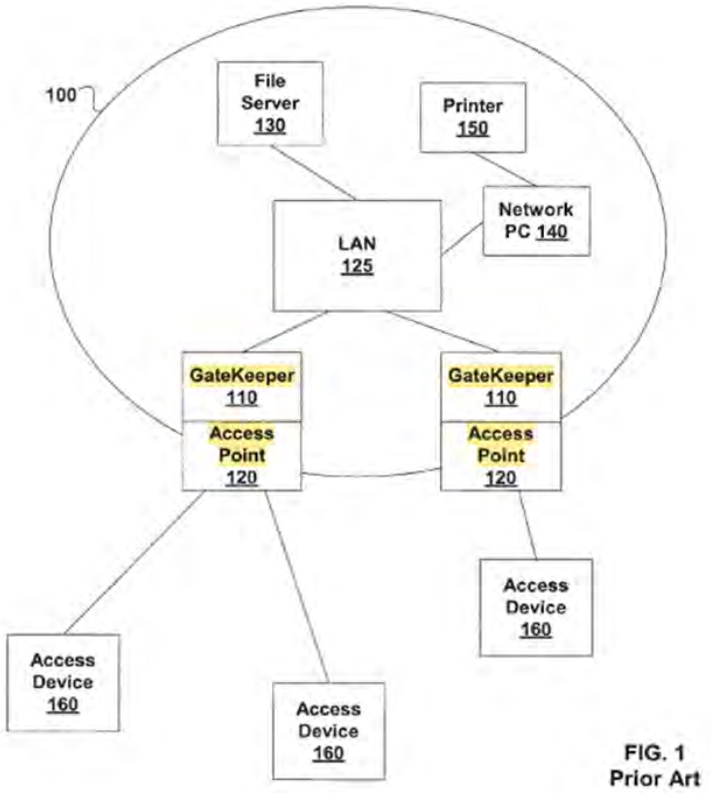


FIG. 5

Id. at Fig. 5 (emphasis added).

39. This also appears to contradict the basic concepts of the purported invention, according to InfoExpress, which argues that the "prior art . . . talks about having a gatekeeper associated **with every access point**, and any access device that wanted to go through that access point would be determined by the gatekeeper." Nov. 28, 2023 Hearing Tr. (Ex. 2) at 32:8–16 (emphasis added); *see also* '484 Patent at Fig. 1 Prior Art below (with emphasis added):



'484 Patent at Fig. 1 (emphasis added).

40. InfoExpress articulated that the difference between the gatekeeper in the Asserted Patents and the prior art is that the "gatekeeper . . . **is managing all of** . . . the various access points and the [traffic] coming in." Nov. 28, 2023 Hearing Tr. (Ex. 2) at 32:25–33:8 (emphasis added). InfoExpress noted that such a concept was not "contemplated or [one] that would even work. It kind of breaks down the system." *Id.* The goal of the gatekeeper appears to be related to enforcing some undefined security policies. But the method by which it performs that goal, which would help explain what the device is, leaves a POSITA without guidance on what is, and is not, a gatekeeper. The claims are further confusing regarding what a gatekeeper is, as the claims recite other networking components explicitly, such as "switch" and "router," distinctly from gatekeeper. '484 Patent at cls. 18, 33, 48, 61, 76 ("a network switch"); *id.* at cl. 19 ("The network gatekeeper of claim 1, wherein the communication device

includes a router."). Similarly, the claims and specification are unclear as to whether a gatekeeper can be a firewall, since the specification discusses an access point as a firewall, and "access point" is an explicitly claimed term distinct from "gatekeeper." *Id.* at 7:53–56 ("Access Point 215 is, for example, a network switch, a wireless access point, a remote access virtual private network (VPN), secure socket layer VPN, **firewall**, or the like.") (emphasis added); *see, e.g.*, *id.* at cls. 27–28, 33–35, 40–41, 48–50, 56, 73–78, 82. This creates confusion as to whether the gatekeeper can be a switch, router, or firewall. Hence, a POSITA would not understand if a device is a gatekeeper in light of the intrinsic evidence, which fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.

B. "a wireless access point configured to support an 802.1x standard" ('484 Patent: Claim 17) / "an access point configured to use an 802.1x protocol" ('444 Patent: Claim 22)

Defendants' Construction	**Plaintiff's Construction**
"802.1x protocol as it existed on or before September 24, 2003"; Otherwise, indefinite	Plain and ordinary meaning; no construction necessary

41. The phrases "a wireless access point configured to support an 802.1x standard," ('484 Patent at cl. 1) and "an access point configured to use an 802.1x protocol" ('444 Patent at cl. 22) fail to delineate and inform a POSITA of the boundaries of terms "802.1x standard" and "802.1x protocol."

42. Claim 1 of the '484 Patent and claim 22 of the '444 Patent broadly refer to "**an** 802.1x standard." '484 Patent at cl. 1; '444 Patent at cl. 22. But the specification is to the contrary, as it contemplates "the existing 802.1x protocol implementation," which would have been at the time of the earliest claimed priority date: September 24, 2003. '484 Patent at 13:1–3; *see also* U.S. Provisional Application No. 60/513,080 (Ex. 3) at 4 ("Existing System 1c: 802.1x"); *id.* at 6 ("The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol.").

43. Alternatively, "a wireless access point configured to support an 802.1x standard" and "an access point configured to use an 802.1x protocol" are indefinite because these terms, as claimed,

encompass all future version of the 802.1x protocol or standard, and a POSITA has no way of knowing what will exist in future variations. As noted above, both phrases broadly claim "**an** 802.1x standard" and "**an** 802.1x protocol," and the claims fail to demarcate which specific version or implementation of the 802.1x standard or protocol is covered.

44. The background of the specification generically references "**a** [sic] IEEE 802.1x standard protocol." '484 Patent at 1:37–40. Indeed, other references to 802.1x lack specificity: "A client filter redirects calls for audit information to an agent on the EP and sends the responses to **the 802.1x compliant AP** which relays them to the EAP server" (*id.* at 14:9–11 (emphasis added);

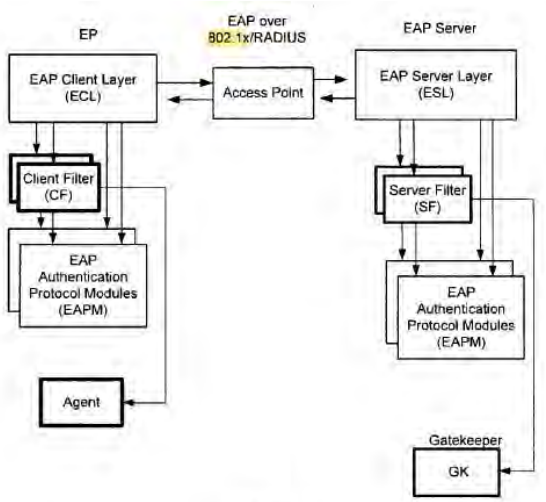


FIG. 5

(*id.* at Fig. 5 (emphasis added));

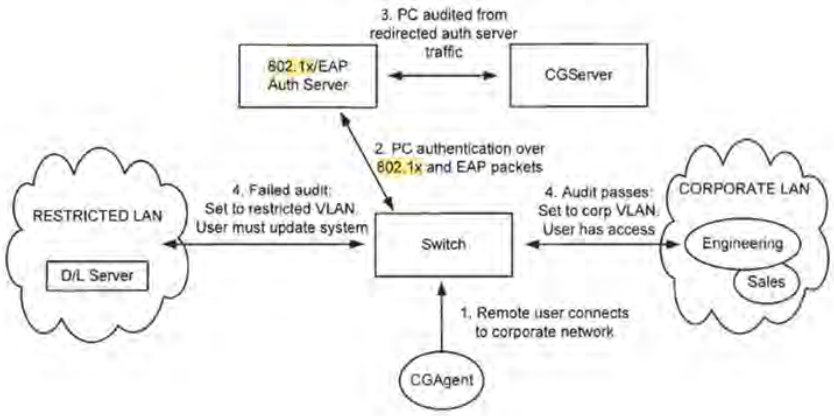


FIG. 9

(*id.* at Fig. 9 (emphasis added)).

45. While the specification refers to "the existing 802.1x protocol implementation," (*id.* at 14:1–3), to the extent that InfoExpress intends the breadth of these terms to encompass all future versions of the 802.1x standard, this would include many technical details contained in numerous additional specifications, developed by dozens of engineers, and which a POSITA at the time of the claimed invention would have no reasonable ability to predict. Future versions of 802.1x could include changes or enhancements that were unforeseeable at the time of the patent application, thus expanding the scope of these claims in unpredictable ways. For example, the provisional patent applications contemplates the use of 802.11a and 802.11b:

> AP – A switch or wireless access point (WAP) which is used to connect EPs to the corporate network. An EP connects to a switch with an Ethernet cable to one of the switch's ports. An EP typically connects to a WAP through a wireless network card, commonly through protocols like 802.11a or 802.11b.

U.S. Provisional Application No. 60/513,080 (Ex. 3) at 1; U.S. Provisional Application No. 60/505,582 (Ex. 4) at 1. 802.11b operated at 2.4 GHz and 802.11a supported 5 GHz with 20 MHz bandwidth. *See* https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/ (Ex. 5). But future standards included a variety of enhancements that would not have been known, let alone predicted, by a POSITA at the time of the priority date. 802.11g, which was released in 2003, offered

"faster data rates of up to 54 Mbit/s in the same 24 GHz frequency band as IEEE 802.11b." *Id.* Later, in 2009, 802.11n provided even faster data rates of up to 600 Mbit/s in both the 2.4 GHz and 5GHz frequency bands. *Id.* Later versions have provided additional enhancements, including 802.11ac (released in 2013), supporting up to 3.5 Gbit/s, and 802.11ax (released in 2021), theoretically supporting 9.6 Gbit/s. *Id.* These exemplary enhancements, including other operational improvements that were added after the release of 802.11b and 802.11a standards and the claimed priority date, would not have been known by a POSITA.

46. Thus, the specification does not teach a POSITA the scope of the claimed 802.1x protocol or standard beyond "the existing 802.1x protocol implementation" at the time of the invention, but the claims do not include any such qualification, and I understand that InfoExpress has not agreed to any such qualification.

47. Therefore, it is my opinion that a POSITA, at the time of the invention of the '484 and '444 Patents, would not understand the boundaries of the terms "an 802.1x standard" and "an 802.1x protocol" from the context of the claims or from the intrinsic record, unless those terms are construed to mean the 802.1x standard or protocol that existed as of the filing date (i.e., September 24, 2003).

C. "policy auditor" ('484 Patent: Claims 1, 6, 12, 15)

Defendants' Construction	**Plaintiff's Construction**
Indefinite	Plain and ordinary meaning; no construction necessary

48. "Policy auditor" is not a term of art in the context of the '484 Patent. Based on my education and experience, a POSITA would have understood that there are virtually unlimited possibilities to audit security policies based on the security needs of a network. With this vast array of possibilities, there are likewise virtually unlimited varieties of computer components or software structures that might be characterized as a "policy auditor," such that a POSITA would not understand

with reasonable certainty which of them would, or would not, fall within the scope of "policy auditor" as used in the claims.

49. For example, an enterprise running a secured network may want to restrict or deny access to resources if an access request originates from an unknown outside IP address. In this scenario, the configuration of access control lists to restrict or deny such access can be considered a security policy, and a firewall that audits the access device and thus enforces the configuration of the access control lists could be considered a "policy auditor." Similarly, the idea of regulating access to corporate resources to one corporate department but not another can be called a security policy and a VLAN switch that segments the network into different parts for employees with different levels of authorization could be a "policy auditor." In addition, the requirement for login credentials can be considered a security policy and any computer component that checks login credentials could be considered a "policy auditor." The checking of such login credentials can take place anywhere in the network, including a local check by an agent at the access device, an intermediate check by a firewall or network switch, or a central check by the server located in the protected network. As a final example, the requirement for the installation of antivirus software can be a "security policy," and the antivirus software itself could be a "policy auditor" because the software will check to determine if it is up-to-date and perform updates as necessary. Thus, for any possible security policy defined, there will correspondingly be a set of design choices of hardware components and software that could enforce the security policy and fall into the purview of the claimed "policy auditor." In the examples above, a "policy auditor" might be a firewall, a VLAN switch, an agent running on an access device, a server, and/or an antivirus software, or similar hardware and software, depending on the specific security policy it is "auditing."

50. The specification does not provide any guidance that would help a POSITA delineate the bounds of what is, and is not, a "policy auditor." The specification portrays a "policy auditor" using only functional language—it "receives a request for access," "provides a notice to access control," "authenticates the identity of access device," and "collects further data to perform a security audit."

'484 Patent at 9:31–33, 9:42–45, 11:31–33, 11:39–42. Other than this functional language, the specification does not limit the claimed "policy auditor" to any specific algorithm or structure, nor does it provide any meaningful guidance at all as to its metes and bounds. "Policy auditor" therefore apparently includes all possible hardware components or software that might carry out those functions, directly or indirectly. Given this context, it is my opinion that a POSITA would not understand with reasonable certainty the scope of that term.

D. "access to the restricted subset of the protected network [is / being] responsive to a VLAN configured to communicate with the protected network subject to the access control list" ('484 Patent: Claim 56;'460 Patent: Claim 30)

Defendants' Construction	**Plaintiff's Construction**
Indefinite	Plain and ordinary meaning; no construction necessary

51. A POSITA would not understand with reasonable certainty what it means for "access" to be "responsive to" a VLAN or how access could be "responsive to" a VLAN. A VLAN is a logical overlay network that, for instance, groups together a subset of devices. Under no typical nomenclature in the art would "access" be "responsive to" a VLAN, and the specification provides no guidance for what the VLAN would "do" such that access would be responsive to it.

52. For example, in other contexts, the specification uses the term "responsive" consistent with its plain and ordinary meaning. The specification recites "a gatekeeper, applying a security policy to the access device, responsive to **the request** [for access to a less-restricted subset of the protected network from an access device.]" '484 Patent at 4:10–19 (emphasis added). In this example, "responsive to" means the gatekeeper takes the action of "applying a security policy" in response to the access request sent from the access device. As another example, the specification recites that "configuration of the communication port including association of the communication port alternatively with the first VLAN or the second VLAN, configuration of the communication port being responsive to **the commands** issued by the gatekeeper" and "means for allowing communication to the less-restricted

subset, responsive to the enforcement of the security policy." '484 Patent at 3:55–59, 4:50–51 (emphasis added). There, "responsive to" means that the communication port is configured in response to the commands given by the gatekeeper.

53. In other words, consistent with the above excerpts, as a POSITA would expect, "responsive to" connects with a request or a command. Yet the claim does not identify any request or command coming from, or going to, the VLAN, to which the requisite access would be responsive. The specification does not provide any clarity on this point, as it simply recites the same language without any further explanation: "access to the less-restricted subset being responsive to a first VLAN" and "access to the restricted subset of the computing network being responsive to a second VLAN." '484 Patent at 3:45–46, 3:50–51. Accordingly, it is my opinion, based on my education and experience, that a POSITA would not understand with reasonable certainty what this limitation means.

Dated: June 28, 2024

Respectfully Submitted,

Narasimha Reddy

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 200 of 1144
INFOEXPRESS, INC. - EX2572

EXHIBIT L

Krishnan Padmanabhan (SBN: 254220)
kpadmanabhan@winston.com
WINSTON & STRAWN LLP
200 Park Ave.
New York City, NY 10166
Tel: (212) 294-6700

David Enzminger (SBN: 137065)
denzminger@winston.com
WINSTON & STRAWN LLP
333 S. Grand Avenue
Los Angeles, CA 90071
Telephone: (213) 615-1700

William Logan (*pro hac vice*)
wlogan@winston.com
WINSTON & STRAWN LLP
800 Capitol Street
Suite 2400
Houston, TX 77002-2925
Tel: (713) 651-2600

Patrick Clark (*pro hac vice*)
pclark@winston.com
WINSTON & STRAWN LLP
2121 N. Pearl Street
Dallas, TX 75201
Tel: (214) 453-6500

Attorneys for Defendant
Cisco Systems, Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INFOEXPRESS INC.,

Plaintiff,

v.

CISCO SYSTEMS, INC.,

Defendant.

Case No. 4:23-cv-02698-YGR

DEFENDANT'S AMENDED INVALIDITY CONTENTIONS

I. INTRODUCTION

Pursuant to the Federal Rules of Civil Procedure and this Court's Patent L.R. 3-3 and 3-4, Defendant Cisco Systems, Inc. ("Cisco" or "Defendant") serves the following Preliminary Invalidity Contentions and accompanying claim charts on Plaintiff InfoExpress Inc. ("InfoExpress" or "Plaintiff"). Plaintiff asserts the following patents against Cisco: United States Patent Nos. 7,523,484 (the "'484 Patent"); 8,051,460 (the "'460 Patent"); 8,677,450 (the "'450 Patent"); 8,578,444 (the "'444 Patent"); 8,347,350 (the "'350 Patent"); and 8,117,645 (the "'645 Patent") (collectively, the "Asserted Patents"). Plaintiff alleges infringement of the Asserted Patents in its Amended Complaint, dated September 28, 2023. Plaintiff identified the following claims as asserted in this matter (collectively, "Asserted Clams") against Cisco:

Asserted Patent	Asserted Claims
'484 Patent	1–5, 11–13, 15–20, 23–25, 27–28, 33–35, 38–39, 41–43, 48–50, 53, 57–59, 61–63, 65–66, 68, 71, and 82
'460 Patent	1–6, 10–12, 16–22, and 27
'450 Patent	1–4, 7–9, 11, 14, 16, 22–23, and 25–28
'444 Patent	1–7, 10–14, 17, and 22
'350 Patent	1–2, 4–10, 13, and 18–19
'645 Patent	1–2 and 5–6

Cisco's Preliminary Invalidity Contentions demonstrate that the Asserted Claims are invalid under 35 U.S.C. §§ 101, 102, 103, and/or 112 for at least the reasons disclosed herein. Cisco's accompanying charts include Exhibits A1–A37, B1–B37, C1–C37, D1–D37, E1–E37, F1–F37, and OO. Cisco further identifies herein the limitations of the Asserted Claims that it contends are indefinite for lack of written description or enablement under 35 U.S.C. § 112 or are directed to ineligible subject matter under 35 U.S.C. § 101.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 203 of 1144
INFOEXPRESS, INC. - EX2572

II. PRELIMINARY STATEMENT

Cisco's Preliminary Invalidity Contentions are based on its current knowledge, understanding, and belief of the Asserted Patents and prior art, of Plaintiff's infringement theories (inasmuch as they can be inferred from its Preliminary Infringement Contentions), and of the facts and other information available as of the date of these invalidity contentions. Cisco's investigation, discovery, and analysis of information related to this action are ongoing. Additional discovery, clarification of Plaintiff's impermissibly vague and overly broad infringement contentions, and/or orders of the Court may require Cisco to amend or supplement these invalidity and eligibility contentions, and Cisco expressly reserves the right to do so as the case proceeds. Accordingly, the present contentions represent Cisco's good-faith effort to provide a comprehensive identification of prior art relevant to this case in addition to Cisco's remaining invalidity and ineligibility positions. Cisco reserves the right to modify or supplement its prior art list and invalidity and eligibility contentions at a later time with, or based upon, pertinent information that may be subsequently discovered.

III. GENERAL OBJECTIONS AND RESERVATION OF RIGHTS

Cisco provides its Preliminary Invalidity Contentions subject to the reservations of rights below. For instance, Cisco reserves the right to further amend and/or supplement its Preliminary Invalidity Contentions in accordance with the Court's Standing Orders, the Federal Rules of Civil Procedure, and as discovery begins in this matter.

A. No Waiver of Invalidity or Ineligibility Arguments

Nothing in these contentions is intended, nor should be construed, as a waiver of any argument under 35 U.S.C. §§ 101, 102, 103, or 112. Cisco's statements herein (including the accompanying claim charts) reflect Cisco's present understanding of the purported scope of the claims as alleged by Plaintiff in its Preliminary Infringement Contentions (as best those contentions can be understood given any present deficiencies). The accompanying charts attached hereto are representative claim charts that identify where the elements of the Asserted Claims of the Asserted Patents may be found in the prior art and further identify why those Asserted Claims are not novel or non-obvious. Except where explicitly indicated, Cisco's identification of where the preambles of the Asserted Claims of the Asserted Patents may be found in the prior art is not intended to indicate that any such preamble is limiting. Thus, all

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 204 of 1144
INFOEXPRESS, INC. - EX2572

disclosures made with respect to the preambles of the Asserted Claims are made only to the extent the preamble is determined to be limiting.

The references and systems cited in the attached claim charts may disclose and/or anticipate the limitations of the Asserted Claims expressly and/or inherently. The suggested obviousness combinations may be presented in conjunction with or in alternative to Cisco's contentions regarding anticipation. The obviousness combinations should not be construed to suggest that any reference included in any combination is not anticipatory. Further, to the extent that Plaintiff contends that any of the references identified does not constitute prior art under 35 U.S.C. § 102, Cisco reserves the right to rely upon other prior art references in the same patent family with substantially identical disclosures as evidence of invalidity based on the same theories as those disclosed below.

B. No Admission Regarding Infringement

Nothing in these contentions is intended, nor should be construed, as a waiver of any noninfringement position. Further, nothing disclosed herein is an admission or acknowledgement that any product accused of infringement by Plaintiff in its Preliminary Infringement Contentions (the "Accused Products"), or any of Cisco's other products or services, infringes any of the Asserted Claims. To the extent that any of the prior art references or systems disclose the same functionality or feature of any of the Accused Products, Cisco reserves the right to argue that said feature or functionality does not practice any element of any of the Asserted Claims, and to argue, in the alternative, that if said feature or functionality is found to practice any element of any of the Asserted Claims, then the prior art reference or system demonstrates that the element is not novel, is obvious, and/or is otherwise not patentable.

C. Plaintiff's Preliminary Infringement Contentions

Plaintiff's Amended Complaint and Preliminary Infringement Contentions are deficient in multiple respects and do not provide Cisco with sufficient information to understand the specific accused features and components and the alleged factual and evidentiary bases for Plaintiff's infringement allegations. Plaintiff's Infringement Contentions are in most places too general, vague, inconsistent, and conclusory to discern Plaintiff's infringement theories and how exactly Plaintiff contends each Accused Product meets or practices each element of the Asserted Claims.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 205 of 1144
INFOEXPRESS, INC. - EX2572

Further, Plaintiff appears to rely upon overly broad interpretations of the Asserted Claims. Plaintiff's Infringement Contentions and their evidentiary bases also contradict the teachings of the Asserted Patents and the Asserted Claims, and the plain and ordinary meaning of the claim terms as would be understood by a person of ordinary skill in the art. Plaintiff's Infringement Contentions therefore fail to put Cisco on notice of Plaintiff's interpretation of the Asserted Claims, thereby prejudicing Cisco's ability to identify relevant prior art.

As a result, Cisco has been prejudiced in its ability to prepare its Invalidity Contentions. Cisco nonetheless provides these disclosures consistent with the current Scheduling Order. (ECF No. 34.) Cisco's Invalidity Contentions are therefore based in part on Cisco's present understanding of Plaintiff's Complaint and Infringement Contentions (including its overly broad interpretations of the Asserted Claims). To the extent that Plaintiff's Preliminary Invalidity Contentions cure the deficiencies of its current contentions or Plaintiff is later permitted by the Court to amend its contentions to cure the deficiencies of its infringement contentions, Cisco reserves the right to supplement or amend its invalidity contentions to account for such amendments.

D. Claim Construction

Cisco provides these Invalidity Contentions based in part on its knowledge and present understanding of the potential scope of the Asserted Claims at this time, and, in part, upon Plaintiff's apparent constructions and interpretations of the Asserted Claims as advanced in its Preliminary Infringement Contentions. Cisco however takes no position on any matter of claim construction in these Contentions. These contentions do not represent Cisco's agreement or view as to the proper interpretation of any claim term contained therein as Cisco may disagree with Plaintiff's interpretation of the meaning of many terms and phrases in the Asserted Claims. For example, to the extent that Cisco asserts that prior art is anticipatory or renders obvious claims based on any apparent construction of the Asserted Claims by Plaintiff, Cisco's Contentions are not—and should not be interpreted as—adoptions of or admissions as to the accuracy of that scope or construction. Any similarity between any apparent claim interpretation in any of Cisco's invalidity charts and Plaintiff's infringement contentions is not an adoption, admission, or agreement with Plaintiff regarding the meaning of any claim term, but rather a

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 206 of 1144
INFOEXPRESS, INC. - EX2572

reflection of the fact that the subject matter Plaintiff believes is claimed is present in the prior art, or that the claims are otherwise invalid.

Cisco's Invalidity Contentions are not, and should not, be seen as adoptions or admissions as to any particular claim scope or construction, any priority date, any admission that any claims have been properly asserted in this case, or as any admission that any aspect of any accused products or systems meets any particular claim element in any particular way. These Invalidity Contentions are made under a variety of alternatives and do not represent Cisco's agreement or view as to the meaning, definiteness, written description support for, or enablement of any claim contained therein. These Invalidity Contentions also should not be interpreted to rely upon, or in any way affect, the non-infringement arguments Cisco may assert in this case.

Cisco objects to any attempt to imply claim construction from the attached charts. Cisco reserves the right to amend and/or supplement its Invalidity Contentions in response to any claim construction or interpretation positions that Plaintiff may take in this case, including any infringement and/or additional claim construction positions that Plaintiff may take. Cisco also reserves the right to amend and/or supplement these Invalidity Contentions in response to any allegedly supporting evidence offered by Plaintiff, or any report from any expert witness for Plaintiff regarding claim construction, infringement, or validity issues.

Cisco further reserves the right to amend and/or supplement its Invalidity Contentions in accordance with the Court's Patent Local Rules or following any clarification of the Court's claim construction ruling. Cisco also reserves the right to assert that certain claim terms, phrases, and elements are indefinite, not enabled, not novel, not patentable, fail to meet the written description requirement of 35 U.S.C. § 112, or are otherwise invalid under 35 U.S.C. §§ 101 et seq., based on any claim construction or interpretation position Plaintiff may take in this case or based on any claim construction the Court may further adopt in this case.

E. Discovery and Disclosures

Discovery in this case is ongoing, including regarding Cisco's search for prior art and corroborating evidence. Cisco therefore reserves all rights to supplement these Invalidity Contentions once Plaintiff has fulfilled its discovery obligations or based on any other materials received through the

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 207 of 1144
INFOEXPRESS, INC. - EX2572

EXHIBIT M

Krishnan Padmanabhan (SBN 254220)
WINSTON & STRAWN LLP
200 Park Avenue
New York, NY 10166-4193
Telephone: (212) 294-6700
Facsimile: (212) 294-4700
KPadmanabhan@winston.com

David Enzminger (SBN: 137065)
WINSTON & STRAWN LLP
333 S. Grand Avenue
Los Angeles, CA 90071
Telephone: (213) 615-1700
Facsimile: (213) 615-1750
DEnzminger@winston.com

William Logan (*pro hac vice*)
WINSTON & STRAWN LLP
800 Capitol Street, Suite 2400
Houston, TX 77002-2925
Telephone: (713) 651-2600
Facsimile: (713) 651-2700
WLogan@winston.com

Patrick Clark (*pro hac vice*)
WINSTON & STRAWN LLP
2121 N. Pearl St., Suite 900
Dallas, TX 75201
Telephone: (214) 453-6492
Facsimile: (214) 453-6400
PClark@winston.com

Attorneys for Defendant
CISCO SYSTEMS, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INFOEXPRESS INC.,

Plaintiff,

v.

CISCO SYSTEMS, INC.,

Defendant.

Case No. 4:23-cv-02698-YGR

DEFENDANT CISCO SYSTEMS, INC.'S IDENTIFICATION OF PROPOSED CLAIM TERMS FOR CONSTRUCTION

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 209 of 1144
INFOEXPRESS, INC. - EX2572

I. INTRODUCTION

Pursuant to Patent L.R. 4-1, Defendant Cisco Systems, Inc. ("Cisco" or "Defendant") hereby provides its proposed terms for construction.

II. ASSERTED PATENTS AND CLAIMS

Plaintiff InfoExpress Inc. ("InfoExpress" or "Plaintiff") has asserted the following patents, claims, and priority dates:

Asserted Patents	Asserted Claims	Asserted Priority Dates
U.S. Patent No. 7,523,484 (the "'484 patent")	1-5, 11-13, 15-20, 23-25, 27-28, 33-35, 38-39, 41-43, 48-50, 53, 57-59, 61-63, 65-66, 68, 71, and 82	September 24, 2003 / October 21, 2003
U.S. Patent Nos. 8,347,350 (the "'350 patent")	1-2, 4-10, 13, and 18-19	September 24, 2003 / October 21, 2003
U.S. Patent No. 8,051,460 (the "'460 patent")	1-6, 10-12, 16-22, and 27	September 24, 2003 / October 21, 2003
U.S. Patent No. 8,677,450 (the "'450 patent")	1-6, 10-12, 16-22, and 27	September 24, 2003 / October 21, 2003
U.S. Patent No. 8,578,444 (the "'444 patent")	1-7, 10-14, 17, and 22	September 24, 2003 / October 21, 2003
U.S. Patent No. 8,117,645 (the "'645 patent")	1-2, and 5-6	September 24, 2003 / October 21, 2003

III. PRELIMINARY STATEMENT AND RESERVATION OF RIGHTS

Cisco proposes construing the following terms based on the Asserted Claims in InfoExpress's October 2, 2023, Disclosure of Asserted Claims and Infringement Contentions. Cisco identifies these terms pursuant to Patent L.R. 4-1(a).

Cisco may revise this preliminary list of proposed claim terms for construction. Cisco reserves the right to modify, add to, or delete from its list based on, without limitation, the claim terms identified by InfoExpress. Cisco reserves the right to supplement or otherwise amend its list of terms should

InfoExpress amend its Infringement Contentions or assert additional claims against Cisco. Cisco further reserves the right to supplement or amend this list pursuant to the meet-and-confer process contemplated in Patent L.R. 4-1(b).

The identification of any term in the following list is not an admission or indication that such term has a special or uncommon meaning, nor is it an admission or indication that such term is capable of construction and not indefinite or lacking enablement or adequate written description under 35 U.S.C. § 112.

Cisco reserves the right to refine this list to construe any portion of any identified term or element, additional language surrounding any identified term or element, or any term or element similar to an identified term or element found in any additional claim limitations within any of the Asserted Claims. If the claim terms or elements set forth herein include particular terms or elements appropriate for separate constructions, such terms or elements are deemed part of this disclosed list. Similarly, to the extent additional claim language provides appropriate context to construe terms or elements listed herein, such additional language is deemed part of this disclosure.

Cisco has grouped certain terms below for ease of reference when conferring. Cisco may adjust or eliminate the groupings over the course of the meet and confer process.

IV. IDENTIFICATION OF CLAIM TERMS

Subject to the foregoing, Cisco identifies the following claim terms, which it contends may require construction for the Asserted Patents:

No.	Claim Term, Clause or Phrase	Claim(s)
1.	access control	’484 patent claim 1C ’350 patent claim 1PRE ’645 patent claims 1PRE, 2, 5, 6
2.	access control list	’484 patent claims 2, 59 ’450 patent claim 3

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 211 of 1144
INFOEXPRESS, INC. - EX2572

No.	Claim Term, Clause or Phrase	Claim(s)
		’444 patent claim 3
3.	access point	’484 patent claims 16, 17, 27A, 27D & E, 28A, 33, 34, 35, 41A, 48, 49, 50, 62, 82A, 82D ’350 patent claims 1C, 1D, 4, 18 ’460 patent claims 1A, 10, 11, 12, 16A ’450 patent claims 1A, 1D, 3, 4, 16A, 22A, 22D ’444 patent claims 1A, 2, 3, 4, 5, 7, 22A, 22D ’645 patent claim 1[C-ii]
4.	access device	’484 patent claims 1A, 1B, 1C, 3, 4, 5, 11, 13, 15, 23, 24, 27A, 27B, 27C, 28A, 28B, 28C, 28D, 38, 39, 41A, 41B, 41C, 41D, 42, 43, 53, 57A, 57D, 65, 66, 68, 71, 82A, 82B, 82C ’460 patent claims 1A, 1B, 1C, 1D, 2, 3, 5, 6, 16A, 16B, 16C, 17, 18, 20, 21, 22, 27, ’450 patent claims 16A, 16B, 16C, 16D, 16E, 22A, 22B, 22C, 22D, 23, 25, 27
5.	authentication	’450 patent claims 1A, 1C, 7, 8, 16E ’444 patent claims 1A, 1D, 22A, 22D ’645 patent claims 1A, 1C, 1[C-i], 6
6.	communication port	’484 patent claims 27A, 27C, 27D&E, 28A, 28C, 28D, 41A, 41C, 57A, 57B, 57C, 57D, 58, 59, 61, 62, 63, 71, 82A, 82C, 82D ’460 patent claims 1A, 1D, 16A, 16C, 22
7.	configuration/reconfiguration of the communication port	’484 patent claims 27A, 27C, 27D&E, 28A, 28C, 28D, 41A, 41C, 57A, 57B, 57C, 57D, 58, 71, 82A, 82C, 82D ’460 patent claims 1A, 1D, 16A, 16C, 22
8.	reconfiguring	’484 patent claims 27C, 28C, 28D, 41C, 71, 82C ’460 patent claims 1D, 16C, 22 ’350 patent claims 1C, 1D, 18

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 212 of 1144
INFOEXPRESS, INC. - EX2572

No.	Claim Term, Clause or Phrase	Claim(s)
9.	communication device	'484 patent claims 1B, 1C, 16, 17, 18, 19, 20, 25
10.	virtual local area networks / VLAN	'484 patent claim 58 '450 patent claim 4 '444 patent claim 4
11.	gatekeeper	'484 patent claims 1PRE, 1B, 1C, 2, 3, 4, 5, 11, 12, 13, 15, 16, 17, 18, 19, 20, 23, 24, 25, 27A, 27C, 28A, 28C, 41A, 41C, 43, 57A, 57B, 68, 71, 82A, 82C '460 patent claims 1A, 1C, 1D, 5, 16A, 16C, 20, 22 '450 patent claims 1C, 2 '444 patent claims 1C, 1D, 7, 17, 22C, 22D '645 patent claims 1[B-i], 1[C-ii], 2
12.	protected network	'484 patent claims 1A, 1B, 1C, 12, 20, 27PRE, 27A, 27C, 28PRE, 28A, 28C, 41PRE, 41A, 41C, 57PRE, 57A, 57B, 57C, 57D, 59, 82A, 82C '460 patent claims 1PRE, 1D, 16A, 16C
13.	restricted subset	'484 patent claims 1C, 2, 20, 27A, 28A, 41A, 57A, 57C, 59, 82A '460 patent claims 1A, 16A
14.	less-restricted subset	'484 patent claims 1A, 1B, 1C, 5, 12, 20, 27A, 27C, 28A 28C, 28D, 41A, 41C, 57A, 57B, 57C, 57D, 71, 82A, 82C '350 patent claims 1A, 1C, 19 '460 patent claims 1A, 1D, 16A, 16C, 27 '450 patent claims 16A, 16D, 22A, 22D '444 patent claims 6, 22E
15.	policy auditor	'484 patent claims 1B, 12, 15
16.	audit	'484 patent claims 1B, 1C, 13, 39, 42 '350 patent claims 1A 1B 1C 1D 1E 6 8 9 10 13 18 19

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 213 of 1144
INFOEXPRESS, INC. - EX2572

No.	Claim Term, Clause or Phrase	Claim(s)
		’460 patent claim 1E ’450 patent claims 16B, 16C, 22B, 22C, 23, 25 ’444 patent claims 1B, 1C, 1D, 5, 6, 7, 10, 11, 12, 13, 14, 22B, 22C, 22D, 22E, 22F ’645 patent claims 1[B-i], 1[B-ii], 1[B-iii]
17.	security policy	’484 patent claims 1A, 1B, 1C, 5, 11, 12, 24, 27B, 27C, 28B, 28C, 38, 39, 41B, 41C, 41D, 42, 43, 57A, 66, 68, 82B, 82C ’350 patent claims 1B, 1C, 1E, 2, 4, 5, 7, 8, 9, 10, 13, ’460 patent claims 1B, 1C, 1D, 1E, 3, 5, 16B, 16C, 18, 20, 27 ’450 patent claims 1PRE, 1C, 1D, 2, 16B, 16C, 16D, 22B, 22C, 22D ’444 patent claims 1D, 2, 17, 22D, 22F
18.	agent	’484 patent claims 15, 28D, 43, 68, 71 ’350 patent claims 6, 8, 9, 10, 13, 18, 19, ’460 patent claims 5, 20, 22 ’450 patent claims 14, 23 ’444 patent claims 1B, 1C, 5, 6, 7, 22B, 22C, 22E
19.	update the access device / using an update module	’484 patent claims 3, 24 ’460 patent claim 27 ’450 patent claims 2, 16D, 22D, 27, 28
20.	system data	’484 patent claims 4, 5 43, 66, 67 ’460 patent claims 3, 4, 5, 6, 18, 19, 20, 21
21.	server filter / SF	’645 patent claims 2, 5
22.	audit data	’350 patent claims 1A, 1B, 1D, 1E, 6, 8, 9, 10, 13, 18, 19 ’460 patent claim 1E

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 214 of 1144
INFOEXPRESS, INC. - EX2572

No.	Claim Term, Clause or Phrase	Claim(s)
		’444 patent claims 1B, 1C, 1D, 5, 6, 7, 10, 11, 12, 13, 14, 22B, 22C, 22D, 22F
23.	identity of the access device	’484 patent claim 11
24.	monitor security status / monitor continued compliance	’484 patent claims 28D, 71 ’350 patent claims 1E, 2, 4 ’460 patent claims 1E, 22
25.	code segment	’484 patent claims 82A, 82B, 82C, 82D, 82E
26.	apply a security policy	’484 patent claims 27B, 28B, 41B, 43, 66, 68, 82B ’460 patent claims 1B, 3, 5, 16B, 18, 20 ’450 patent claims 1PRE, 1C, 1D, 2, 16B, 22B ‘444 patent claims 1D, 2, 17, 22D
27.	evaluate device information	’645 patent claim 1[B-iii]
28.	scan the device	’450 patent claims 1B, 14
29.	element	’484 patent claim 20
30.	EAP Protocol	’444 patent claims 1A, 8 ’450 patent claim 7 ’645 patent claims 1C, 1[C-i], 2, 6
31.	without passing the data through the gatekeeper	’484 patent claims 27C, 28C, 41C, 82C ’460 patent claims 1D, 16C
32.	improve compliance	’450 patent claims 16C, 22C

Dated: November 30, 2023

WINSTON & STRAWN LLP

By: */s/ Krishnan Padmanabhan*

Krishnan Padmanabhan (SBN 254220)
WINSTON & STRAWN LLP
200 Park Avenue
New York, NY 10166-4193
Telephone: 212-294-6700
Facsimile: 212-294-4700
KPadmanabhan@winston.com

David Enzminger (SBN: 137065)
WINSTON & STRAWN LLP
333 S. Grand Avenue
Los Angeles, CA 90071
Telephone: (213) 615-1700
Facsimile: (213) 615-1750
DEnzminger@winston.com

William Logan (*pro hac vice*)
WINSTON & STRAWN LLP
800 Capitol Street, Suite 2400
Houston, TX 77002-2925
Telephone: (713) 651-2600
Facsimile: (713) 651-2700
WLogan@winston.com

Patrick Clark (*pro hac vice*)
WINSTON & STRAWN LLP
2121 N. Pearl St., Suite 900
Dallas, TX 75201
Telephone: (214) 453-6492
Facsimile: (214) 453-6400
PClark@winston.com

Attorneys for Defendant
CISCO SYSTEMS, INC.

CERTIFICATE OF SERVICE

I am employed in the City and County of San Francisco, State of California. I am over the age of 18 and not a party to the within action; my business address is 101 California Street, Suite 3500, San Francisco, CA 94111.

On November 30, 2023, I served the following document described as:

DEFENDANT CISCO SYSTEMS, INC.'S IDENTIFICATION OF PROPOSED CLAIM TERMS FOR CONSTRUCTION

on the interested parties in this action listed on the service list below.

☒ by electronically transmitting a true and correct copy thereof via e-mail to the following, in accordance with their agreement to be served electronically pursuant to Federal Rule of Civil Procedure 5(b)(2)(E). No error messages were received after said transmission.

SERVICE LIST:

Andrew F. Schwerin , I
Saul Ewing LLP
1500 Market St.,
3800 Centre Square West 19102
Philadelphia, PA 19102
Email: andrew.schwerin@saul.com

Brenda Helen Entzminger
Bunsow De Mory LLP
701 El Camino Real
Redwood City, CA 94063
Email: bentzminger@bdiplaw.com

Casey T. Grabenstein
Saul Ewing Arnstein & Lehr LLP
161 N. Clark Street, Ste 4200
Chicago, IL 60601
Email: casey.grabenstein@saul.com

Joseph M. Kuo
Saul Ewing Arnstein & Lehr LLP
161 N. Clark Street, Suite 4200
Chicago, IL 60601
Email: joseph.kuo@saul.com

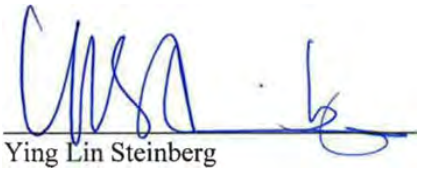
Michael E Flynn-O'Brien
Bunsow De Mory LLP
701 El Camino Real
Redwood City, CA 94063
Email: mflynnobrien@bdiplaw.com

Brian Raymond Michalek
Saul Ewing Arnstein & Lehr LLP
161 North Clark Street, Suite 4200
Chicago, IL 60601
Email: brian.michalek@saul.com

Attorneys for Plaintiff InfoExpress, Inc.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on November 30, 2023 at San Francisco, California.



Ying Lin Steinberg

EXHIBIT N

Brian R. Michalek (SBN 302007)
Casey T. Grabenstein (*pro hac vice*)
Joseph M. Kuo (*pro hac vice*)
SAUL EWING LLP
161 N. Clark St., Suite 4200
Chicago, IL 60601
Telephone: (312) 876-7100
Facsimile: (312) 876-0288
brian.michalek@saul.com
casey.grabenstein@saul.com
joseph.kuo@saul.com

Andrew Schwerin (*pro hac vice*)
SAUL EWING LLP
Centre Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102 2186
Telephone: (215) 972-7184
Facsimile: (215) 972-7184
andrew.schwerin@saul.com

Michael E. Flynn-O'Brien (SBN 291301)
BUNSOW DE MORY LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: (650) 351-7245
Facsimile: (415) 426-4744
mflynnobrien@bdiplaw.com

Attorneys for Plaintiff InfoExpress Inc.

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

INFOEXPRESS INC. Plaintiff, v. **CISCO SYSTEMS, INC.** Defendant.	**Case No. 4:23-cv-02698-YGR** **PLAINTIFF INFOEXPRESS, INC.'S PROPOSED PATENT CLAIM TERMS FOR CONSTRUCTION, PER PATENT L.R. 4-1(a)**

Pursuant to Patent Local Rule 4-1, Plaintiff InfoExpress Inc. ("InfoExpress") hereby provides its initial list of claim terms, phrases, or clauses of the Asserted Patents, U.S. Patent Nos. 7,523,484 (the '484 Patent); 8,051,460 (the '460 Patent); 8,677,450 (the '450 Patent); 8,578,444 (the '444 Patent); 8,347,350 (the '350 Patent); and 8,117,645 (the '645 Patent), which InfoExpress contends should be construed by the Court.

The below list of terms for construction reflects InfoExpress's presently selected claim terms, and InfoExpress reserves the right to add, eliminate, amend, supplement, or modify the proposed terms, and their constructions, for any reason, including after consideration of Cisco's proposed terms and constructions and following any meet-and-confer discussions regarding the parties' terms and constructions.

Proposed Claim Terms, Phrases, Clauses For Construction	Asserted Patent Claims
"configured to reconfigure the communication device"	'484 patent, claim 1
"reconfiguring a port on the communication device"	'484 patent, claim 20
"reconfiguring the communication port"	'484 patent, claims 27, 28, 28, 41, 71; '460 patent, claims 1, 16, 22
"configured to reconfigure the communication port"	'484 patent, claim 57
"configured for reconfiguring the communication port"	'484 patent, claim 82
"reconfiguring [an/the] access point"	'350 patent, claims 1, 1, 18
"wherein the access point is reconfigured"	'350 patent, claim 4
"configuring [an/the] access point"	'450 patent, claims 1, 3, 4, 22; '444 patent, claims 2, 3, 4, 5, 7, 22; '645 patent, claim 1
"a router configured to limit access to only the restricted subset using an access control list"	'484 patent, claim 2
"wherein the communication port is limited to communicating with the restricted subset of the protected network by an access control list"	'484 patent, claim 59
"setting an access control list on the access point"	'450 patent, claim 3
"assigning an access control list"	'444 patent, claim 3
"associating the communication port with a VLAN"	'484 patent, claim 58
"wherein configuring the access point includes assigning a VLAN"	'450 patent, claim 4; '444 patent, claim 4

Proposed Claim Terms, Phrases, Clauses For Construction	Asserted Patent Claims
"restricted subset"	'484 patent, claims 1, 2, 20, 27, 28, 41, 57, 59, 82; '460 patent, claims 1, 16
"a different subset of the network"	'350 patent, claim 4
"less-restricted subset"	'484 patent, claims 1, 5, 12, 20, 27, 28, 41, 57, 71, 82; '350 patent, claims 1, 19; '460 patent, claims 1, 16, 22; '450 patent, claims 16, 22; '444 patent, claims 6, 22
"to issue commands [], the commands being configured to grant access to the less-restricted subset"	'484 patent, claim 5
"receiving a command from the gatekeeper, the command being responsive to the received first communication and being configured to reconfigure the communication port"	'484 patent, claim 57
"the received command"	'484 patent, claim 57
"the applying of the security policy taking place under control of the gatekeeper"	'444 patent, claim 1, 22
"a gatekeeper stored in memory and executable to: . . . evaluate device information received from the device in response to the audit request"	'645 patent, claim 1
"applying a security policy"	'484 patent, claims 27, 28, 41, 43, 66, 68, 82; '460 patent, claims 1, 3, 5, 16, 18, 20; '450 patent, claims 1, 2, 16, 22; '444 patent, claims 1, 2, 22
"application of the security policy"	'450 patent, claims 1, 16, 22

Proposed Claim Terms, Phrases, Clauses For Construction	Asserted Patent Claims
"wherein the network gatekeeper is further configured to obtain system data from the access device."	'484 patent, claim 4
"to obtain system data from the access device"	'484 patent, claims 43, 68; '460 patent, claims 5, 18, 20
"obtaining system data from the access device"	'484 patent, claim 66; '460 patent, claim 3
"…having been obtained by the agent"	'444 patent, claims 1, 22
"system data"	'484 patent, claims 4, 5, 43, 66, 68; '460 patent, claims 3, 4, 5, 6, 18, 19, 20, 21
"information regarding the device"	'450 patent, claim 1
"information regarding the access device"	'450 patent, claim 23
"device information received from the device in response to the audit request"	'645 patent, claim 1
"audit data pertaining to [a/the] device"	'350 patent, claims 1, 18, 19; '444 patent, claims 1, 5, 6, 7, 10, 22
"audit data"	'350 patent, claims 1, 6, 8, 9, 10, 13, 18, 19; '444 patent, claims 1, 5, 6, 7, 10, 11, 12, 13, 14, 22

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 224 of 1144
INFOEXPRESS, INC. - EX2572

Proposed Claim Terms, Phrases, Clauses For Construction	Asserted Patent Claims
"receiving [] audit data pertaining to a device" "wherein [] audit data pertaining to the device continues to be received from the agent" "receiving the audit data at a gatekeeper configured to control access to a network, from the agent" "receiving, from the agent, [] audit data pertaining to the device" "the received audit data" "device information received from the device in response to the audit request,"	'350 patent, claims 1, 1 '350 patent, claims 18, 19 '444 patent, claims 1, 22 '444 patent, claims 5, 6, 22 '444 patent, claims 11, 12, 13, 14 '645 patent, claim 1
"collect[][the] audit data" "audit data collected by the agent" "collect information regarding the [access] device"	'350 patent, claim 6 '350 patent, claims 8, 9, 10, 13 '450 patent, claims 1, 23
"an agent executing on the access device to monitor security status of the access device" "an agent running on the device"	'484 patent, claims 28, 71; '460 patent, claim 22 '350 patent, claim 6
"scanning the device to collect information regarding the device" "wherein the scanning is performed"	'450 patent, claim 1 '450 patent, claim 14
"requirements of the security policy are satisfied" "that the access device satisfies the requirements of the security policy" "based on satisfaction of the security policy"	'460 patent, claims 1, 16; '484 patent, claims 27, 28, 41, and 82 '460 patent, claims 3, 5, 18, 20 '450 patent, claims 16, 22

Proposed Claim Terms, Phrases, Clauses For Construction	Asserted Patent Claims
"wherein the at least one security policy is responsive to an identity of the access device"	'484 patent, claim 11
"wherein selecting the security policy is responsive to an identity of the access device . . ."	'484 patent, claim 47; '460 patent, claims 9, 25
"wherein the authentication identifies the device"	'450 patent, claim 6
"other devices coupled to the device"	'350 patent, claim 10; '450 patent, claim 11; '444 patent, claim 14
"devices connected to the access device"	'460 patent, claims 6, 21
"application[s]	'350 patent, claim 13; '444 patent, claim 10; '444 patent, claim 11
"a status of an application on the device"	'450 patent, claim 9
"operating system"	'350 patent, claim 8; '450 patent, claim 25; '444 patent, claim 16
"antivirus software executing on the device"	'484 patent, claim 13
"that concerns antivirus software on the device"	'350 patent, claim 9; '444 patent, claim 13
"wherein the system data includes antivirus software status"	'460 patent, claim 4
"update[e/ing] the access device"	'484 patent, claims 3, 24, 38, 41; 460 patent, claim 27
"updating the device"	'350 patent, claim 7
"facilitating updates to software on the device"	'450 patent, claim 2
"the updated access device"	'450 patent, claims 16, 22
"software update"	'450 patent, claims 27, 28

Proposed Claim Terms, Phrases, Clauses For Construction	Asserted Patent Claims
"wherein the authentication includes using a RADIUS protocol"	'450 patent, claim 8
"wherein the authentication includes using an EAP protocol"	'450 patent, claim 7
"performing an authentication using an EAP protocol"	'444 patent, claims 1, 22
"EAP protocol"	'450 patent, claim 7; '444 patent, claims 1, 22
"EAP encryption protocol"	'645 patent, claim 1
"receive the authentication information from the device using an EAP encryption protocol"	'645 patent, claim 1
EAPM [EAP module]	'645 patent, claims 2, 6
"EAP server layer (SL)", "ESL"	'645 patent, claims 1, 2, 5
"SF"	'645 patent, claims 2, 5
"wherein the SF is part of the ESL"	'645 patent, claim 5
"a wireless access point configured to support an 802.1x standard"	'484 patent, claim 17
"an access point configured to use an 802.1x protocol"	'444 patent, claims 1, 22
"storing the read administrator specified configuration"	'484 patent, claims 27, 82

Dated: November 30, 2023

Respectfully submitted,

s/Brian R. Michalek
Brian R. Michalek (SBN 302007)

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing document has been served via e-mail on **November 30, 2023,** to all counsel of record who are deemed to have consented to electronic service via the Court's CM/ECF system.

s/Andrew Schwerin
Andrew Schwerin (*pro hac vice*)

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 228 of 1144
INFOEXPRESS, INC. - EX2572

EXHIBIT O

Brian R. Michalek (SBN 302007)
Casey T. Grabenstein (*pro hac vice*)
Joseph M. Kuo (*pro hac vice*)
SAUL EWING LLP
161 N. Clark St., Suite 4200
Chicago, IL 60601
Telephone: (312) 876-7100
Facsimile: (312) 876-0288
brian.michalek@saul.com
casey.grabenstein@saul.com
joseph.kuo@saul.com

Andrew Schwerin (*pro hac vice*)
SAUL EWING LLP
Centre Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102 2186
Telephone: (215) 972-7184
Facsimile: (215) 972-7184
andrew.schwerin@saul.com

Michael E. Flynn-O'Brien (SBN 291301)
Brenda Entzminger (SBN 226760)
BUNSOW DE MORY LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: (650) 351-7245
Facsimile: (415) 426-4744
mflynnobrien@bdiplaw.com

Attorneys for Plaintiff InfoExpress Inc.

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

INFOEXPRESS INC. Plaintiff, v. **CISCO SYSTEMS, INC.** Defendant.	**Case No. 4:23-cv-02698-YGR** **PLAINTIFF INFOEXPRESS PROPOSED PATENT CLAIM TERMS FOR CONSTRUCTION, PER PATENT L.R. 4-1(a)**

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 230 of 1144
INFOEXPRESS, INC. - EX2572

INFOEXPRESS INC., Plaintiff, v. **FORTINET, INC.**, Defendant.	**Case No.: 4:23-cv-04389-YGR** **PLAINTIFF INFOEXPRESS PROPOSED PATENT CLAIM TERMS FOR CONSTRUCTION, PER PATENT L.R. 4-1(a)**

Pursuant to Patent Local Rule 4-1, Plaintiff InfoExpress Inc. ("InfoExpress") hereby provides its initial list of claim terms, phrases, or clauses of the Asserted Patents, U.S. Patent Nos. 7,523,484 (the '484 Patent); 8,051,460 (the '460 Patent); 8,677,450 (the '450 Patent); 8,578,444 (the '444 Patent); 8,347,350 (the '350 Patent); and 8,117,645 (the '645 Patent), which InfoExpress contends should be construed by the Court.

The below list of terms for construction reflects InfoExpress's presently selected claim terms, and InfoExpress reserves the right to add, eliminate, amend, supplement, or modify the proposed terms, and their constructions, for any reason, including after consideration of Cisco's and Fortinet's proposed terms and constructions and following any meet-and-confer discussions regarding the parties' terms and constructions.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 231 of 1144
INFOEXPRESS, INC. - EX2572

Proposed Claim Terms, Phrases, Clauses For Construction	Asserted Patent Claims
"configured to reconfigure the communication device"	'484 patent, claim 1
"reconfiguring [an/the] access point"	'350 patent, claims 1, 1, 18
"wherein the access point is reconfigured"	'350 patent, claim 4
"configuring [an/the] access point"	'450 patent, claims 1, 3, 4, 22; '444 patent, claims 2, 3, 4, 5, 7, 22; '645 patent, claim 1
"reconfiguring a port on the communication device"	'484 patent, claim 20
"reconfiguring the communication port"	'484 patent, claims 27, 28, 41, 71; '460 patent, claims 1, 16, 22
"configuring the communication port"	'484 patent, claims 57, 58
"configured to reconfigure the communication port"	'484 patent, claim 57
"configured for reconfiguring the communication port"	'484 patent, claim 82
"a router configured to limit access to only the restricted subset using an access control list"	'484 patent, claim 2
"wherein the communication port is limited to communicating with the restricted subset of the protected network by an access control list"	'484 patent, claim 59
"setting an access control list on the access point"	'450 patent, claim 3
"assigning an access control list"	'444 patent, claim 3

Proposed Claim Terms, Phrases, Clauses For Construction	Asserted Patent Claims
"access point"	'484 patent, claims 16, 17, 27, 28, 33, 34, 35, 41, 48, 49, 50, 62, 82; '460 patent, claims 1, 10, 11, 12, 16; '450 patent, claims 1, 3, 4, 16, 22; '444 patent, claims 1–5, 7, 22; '350 patent, claim 1, 4, 18; '645 patent, claim 1
"associating the communication port with a VLAN" "wherein configuring the access point includes assigning a VLAN"	'484 patent, claim 58 '450 patent, claim 4; '444 patent, claim 4
"restricted subset" "a different subset of the network"	'484 patent, claims 1, 2, 20, 27, 28, 41, 57, 59, 82; '460 patent, claims 1, 16 '350 patent, claim 4
"less-restricted subset"	'484 patent, claims 1, 5, 12, 20, 27, 28, 41, 57, 71, 82; '350 patent, claims 1, 19; '460 patent, claims 1, 16, 22; '450 patent, claims 16, 22; '444 patent, claims 6, 22
"to issue commands [], the commands being configured to grant access to the less-restricted subset" "receiving a command from the gatekeeper, the command being responsive to the received first communication and being configured to reconfigure the communication port" "the received command"	'484 patent, claim 5 '484 patent, claim 57 '484 patent, claim 57

Proposed Claim Terms, Phrases, Clauses For Construction	Asserted Patent Claims
"the applying of the security policy taking place under control of the gatekeeper"	'444 patent, claim 1, 22
"a gatekeeper stored in memory and executable to: . . . evaluate device information received from the device in response to the audit request"	'645 patent, claim 1
"applying a security policy"	'484 patent, claims 27, 28, 41, 43, 66, 68, 82; '460 patent, claims 1, 3, 5, 16, 18, 20; '450 patent, claims 1, 2, 16, 22; '444 patent, claims 1, 2, 22
"application of the security policy"	'450 patent, claims 1, 16, 22
"wherein the network gatekeeper is further configured to obtain system data from the access device."	'484 patent, claim 4
"to obtain system data from the access device"	'484 patent, claims 43, 68; '460 patent, claims 5, 18, 20
"obtaining system data from the access device"	'484 patent, claim 66; '460 patent, claim 3
"…having been obtained by the agent"	'444 patent, claims 1, 22
"system data"	'484 patent, claims 4, 5, 43, 66, 68; '460 patent, claims 3, 4, 5, 6, 18, 19, 20, 21
"information regarding the device"	'450 patent, claim 1
"information regarding the access device"	'450 patent, claim 23
"device information received from the device in response to the audit request"	'645 patent, claim 1

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 234 of 1144
INFOEXPRESS, INC. - EX2572

Proposed Claim Terms, Phrases, Clauses For Construction	Asserted Patent Claims
"audit data pertaining to [a/the] device"	'350 patent, claims 1, 18, 19; '444 patent, claims 1, 5, 6, 7, 10, 22
"audit data"	'350 patent, claims 1, 6, 8, 9, 10, 13, 18, 19; '444 patent, claims 1, 5, 6, 7, 10, 11, 12, 13, 14, 22
"receiving [] audit data pertaining to a device"	'350 patent, claims 1, 1
"wherein [] audit data pertaining to the device continues to be received from the agent"	'350 patent, claims 18, 19
"receiving the audit data at a gatekeeper configured to control access to a network, from the agent"	'444 patent, claims 1, 22
"receiving, from the agent, [] audit data pertaining to the device"	'444 patent, claims 5, 6, 22
"the received audit data"	'444 patent, claims 11, 12, 13, 14
"device information received from the device in response to the audit request,"	'645 patent, claim 1
"collect[][the] audit data"	'350 patent, claim 6
"audit data collected by the agent"	'350 patent, claims 8, 9, 10, 13
"collect information regarding the [access] device"	'450 patent, claims 1, 23
"an agent executing on the access device to monitor security status of the access device"	'484 patent, claims 28, 71; '460 patent, claim 22
"an agent running on the device"	'350 patent, claim 6

Proposed Claim Terms, Phrases, Clauses For Construction	Asserted Patent Claims
"scanning the device to collect information regarding the device" "wherein the scanning is performed"	'450 patent, claim 1 '450 patent, claim 14
"requirements of the security policy are satisfied" "that the access device satisfies the requirements of the security policy" "based on satisfaction of the security policy"	'460 patent, claims 1, 16; '484 patent, claims 27, 28, 41, and 82 '460 patent, claims 3, 5, 18, 20 '450 patent, claims 16, 22
"other devices coupled to the device"	'350 patent, claim 10; '450 patent, claim 11; '444 patent, claim 14
"devices connected to the access device"	'460 patent, claims 6, 21
"update[e/ing] the access device" "updating the device" "facilitating updates to software on the device" "the updated access device" "software update"	'484 patent, claims 3, 24, 38, 41; 460 patent, claim 27 '350 patent, claim 7 '450 patent, claim 2 '450 patent, claims 16, 22 '450 patent, claims 27, 28
"wherein the authentication includes using a RADIUS protocol"	'450 patent, claim 8
"wherein the authentication includes using an EAP protocol" "performing an authentication using an EAP protocol" "EAP protocol"	'450 patent, claim 7 '444 patent, claims 1, 22 '450 patent, claim 7; '444 patent, claims 1, 22

Proposed Claim Terms, Phrases, Clauses For Construction	Asserted Patent Claims
"EAP encryption protocol" "receive the authentication information from the device using an EAP encryption protocol"	'645 patent, claim 1 '645 patent, claim 1
EAPM [EAP module]	'645 patent, claims 2, 6
"EAP server layer (SL)", "ESL"	'645 patent, claims 1, 2, 5
"SF" "wherein the SF is part of the ESL"	'645 patent, claims 2, 5 '645 patent, claim 5
"a wireless access point configured to support an 802.1x standard" "an access point configured to use an 802.1x protocol"	'484 patent, claim 17 '444 patent, claims 1, 22

Dated: March 4, 2024

Respectfully submitted,

s/Brian R. Michalek
Brian R. Michalek (SBN 302007)

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing document has been served via e-mail on **March 4, 2024,** to all counsel of record who are deemed to have consented to electronic service via the Court's CM/ECF system.

s/Andrew Schwerin
Andrew Schwerin (*pro hac vice*)

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 238 of 1144
INFOEXPRESS, INC. - EX2572

EXHIBIT P

Brian R. Michalek (SBN 302007)
Casey T. Grabenstein (*pro hac vice*)
Joseph M. Kuo (*pro hac vice*)
SAUL EWING LLP
161 N. Clark St., Suite 4200
Chicago, IL 60601
Telephone: (312) 876-7100
Facsimile: (312) 876-0288
brian.michalek@saul.com
casey.grabenstein@saul.com
joseph.kuo@saul.com

Andrew Schwerin (*pro hac vice*)
SAUL EWING LLP
Centre Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102 2186
Telephone: (215) 972-7184
Facsimile: (215) 972-7184
andrew.schwerin@saul.com

Michael E. Flynn-O'Brien (SBN 291301)
Brenda Entzminger (SBN 226760)
BUNSOW DE MORY LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: (650) 351-7245
Facsimile: (415) 426-4744
mflynnobrien@bdiplaw.com

Attorneys for Plaintiff InfoExpress Inc.

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

INFOEXPRESS INC. Plaintiff, v. **CISCO SYSTEMS, INC.** Defendant.	**Case No. 4:23-cv-02698-YGR** **PLAINTIFF INFOEXPRESS'S AMENDED PROPOSED PATENT CLAIM TERMS FOR CONSTRUCTION, PER PATENT L.R. 4-1(a)**

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 240 of 1144
INFOEXPRESS, INC. - EX2572

INFOEXPRESS INC., Plaintiff, v. **FORTINET, INC.,** Defendant.	**Case No.: 4:23-cv-04389-YGR** **PLAINTIFF INFOEXPRESS'S AMENDED PROPOSED PATENT CLAIM TERMS FOR CONSTRUCTION, PER PATENT L.R. 4-1(a)**

Pursuant to Patent Local Rule 4-1, Plaintiff InfoExpress Inc. ("InfoExpress") hereby provides its amended list of claim terms, phrases, or clauses of the Asserted Patents, U.S. Patent Nos. 7,523,484 (the '484 Patent); 8,051,460 (the '460 Patent); 8,677,450 (the '450 Patent); 8,578,444 (the '444 Patent); 8,347,350 (the '350 Patent); and 8,117,645 (the '645 Patent), which InfoExpress contends should be construed by the Court.

The below list of terms for construction reflects InfoExpress's presently selected claim terms, and InfoExpress reserves the right to add, eliminate, amend, supplement, or modify the proposed terms, and their constructions, for any reason, including after consideration of Cisco's and Fortinet's proposed terms and constructions and following any meet-and-confer discussions regarding the parties' terms and constructions.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 241 of 1144
INFOEXPRESS, INC. - EX2572

Proposed Claim Terms, Phrases, Clauses For Construction	Asserted Patent Claims
"configured to reconfigure the communication device"	'484 patent, claim 1
"reconfiguring [an/the] access point"	'350 patent, claims 1, 1, 18
"wherein the access point is reconfigured"	'350 patent, claim 4
"configuring [an/the] access point"	'450 patent, claims 1, 3, 4, 22; '444 patent, claims 2, 3, 4, 5, 7, 22; '645 patent, claim 1
"reconfiguring a port on the communication device"	'484 patent, claim 20
"reconfiguring the communication port"	'484 patent, claims 27, 28, 41, 71; '460 patent, claims 1, 16, 22
"configuring the communication port"	'484 patent, claims 57, 58
"configured to reconfigure the communication port"	'484 patent, claim 57
"configured for reconfiguring the communication port"	'484 patent, claim 82
"access point"	'484 patent, claims 16, 17, 27, 28, 33, 34, 35, 41, 48, 49, 50, 62, 82; '460 patent, claims 1, 10, 11, 12, 16; '450 patent, claims 1, 3, 4, 16, 22; '444 patent, claims 1–5, 7, 22; '350 patent, claim 1, 4, 18; '645 patent, claim 1
"associating the communication port with a VLAN"	'484 patent, claim 58
"wherein configuring the access point includes assigning a VLAN"	'450 patent, claim 4; '444 patent, claim 4

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 242 of 1144
INFOEXPRESS, INC. - EX2572

Proposed Claim Terms, Phrases, Clauses For Construction	Asserted Patent Claims
"the applying of the security policy taking place under control of the gatekeeper" "a gatekeeper stored in memory and executable to: . . . evaluate device information received from the device in response to the audit request" "applying a security policy" "application of the security policy"	'444 patent, claim 1, 22 '645 patent, claim 1 '484 patent, claims 27, 28, 41, 43, 66, 68, 82; '460 patent, claims 1, 3, 5, 16, 18, 20; '450 patent, claims 1, 2, 16, 22; '444 patent, claims 1, 2, 22 '450 patent, claims 1, 16, 22
"system data"	'484 patent, claims 4, 5, 43, 66, 68; '460 patent, claims 3, 4, 5, 6, 18, 19, 20, 21
"information regarding the device" "information regarding the access device" "device information received from the device in response to the audit request"	'450 patent, claim 1 '450 patent, claim 23 '645 patent, claim 1
"audit data pertaining to [a/the] device" "audit data"	'350 patent, claims 1, 18, 19; '444 patent, claims 1, 5, 6, 7, 10, 22 '350 patent, claims 1, 6, 8, 9, 10, 13, 18, 19; '444 patent, claims 1, 5, 6, 7, 10, 11, 12, 13, 14, 22
"requirements of the security policy are satisfied" "that the access device satisfies the requirements of the security policy" "based on satisfaction of the security policy"	'460 patent, claims 1, 16; '484 patent, claims 27, 28, 41, and 82 '460 patent, claims 3, 5, 18, 20 '450 patent, claims 16, 22

Proposed Claim Terms, Phrases, Clauses For Construction	Asserted Patent Claims
"update[e/ing] the access device"	'484 patent, claims 3, 24, 38, 41; 460 patent, claim 27
"updating the device"	'350 patent, claim 7
"facilitating updates to software on the device"	'450 patent, claim 2
"the updated access device"	'450 patent, claims 16, 22
"software update"	'450 patent, claims 27, 28
"EAP encryption protocol"	'645 patent, claim 1
"receive the authentication information from the device using an EAP encryption protocol"	'645 patent, claim 1
"EAP server layer (SL)", "ESL"	'645 patent, claims 1, 2, 5
"SF"	'645 patent, claims 2, 5
"wherein the SF is part of the ESL"	'645 patent, claim 5
"a wireless access point configured to support an 802.1x standard"	'484 patent, claim 17
"an access point configured to use an 802.1x protocol"	'444 patent, claims 1, 22

Dated: March 15, 2024

Respectfully submitted,

s/Brian R. Michalek
Brian R. Michalek (SBN 302007)

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing document has been served via e-mail on **March 15, 2024,** to all counsel of record who are deemed to have consented to electronic service via the Court's CM/ECF system.

s/Andrew Schwerin
Andrew Schwerin (*pro hac vice*)

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 245 of 1144
INFOEXPRESS, INC. - EX2572

EXHIBIT Q

Brian R. Michalek (SBN 302007)
Casey T. Grabenstein (*pro hac vice*)
Joseph M. Kuo (*pro hac vice*)
SAUL EWING LLP
161 N. Clark St., Suite 4200
Chicago, IL 60601
Telephone: (312) 876-7100
Facsimile: (312) 876-0288
brian.michalek@saul.com
casey.grabenstein@saul.com
joseph.kuo@saul.com

Andrew Schwerin (*pro hac vice*)
SAUL EWING LLP
Centre Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102 2186
Telephone: (215) 972-7184
Facsimile: (215) 972-7184
andrew.schwerin@saul.com

Michael E. Flynn-O'Brien (SBN 291301)
Brenda Entzminger (SBN 226760)
BUNSOW DE MORY LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: (650) 351-7245
Facsimile: (415) 426-4744
mflynnobrien@bdiplaw.com

Attorneys for Plaintiff InfoExpress Inc.

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

INFOEXPRESS INC. Plaintiff, v. **CISCO SYSTEMS, INC.** Defendant.	**Case No. 4:23-cv-02698-YGR** **PLAINTIFF INFOEXPRESS'S SECOND AMENDED PROPOSED PATENT CLAIM TERMS FOR CONSTRUCTION, PER PATENT L.R. 4-1(a)**

INFOEXPRESS INC., Plaintiff, v. **FORTINET, INC.**, Defendant.	**Case No.: 4:23-cv-04389-YGR** **PLAINTIFF INFOEXPRESS'S AMENDED PROPOSED PATENT CLAIM TERMS FOR CONSTRUCTION, PER PATENT L.R. 4-1(a)**

Pursuant to Patent Local Rule 4-1, Plaintiff InfoExpress Inc. ("InfoExpress") hereby provides its Second Amended list of claim terms, phrases, or clauses of the Asserted Patents, U.S. Patent Nos. 7,523,484 (the '484 Patent); 8,051,460 (the '460 Patent); 8,677,450 (the '450 Patent); 8,578,444 (the '444 Patent); 8,347,350 (the '350 Patent); and 8,117,645 (the '645 Patent), which InfoExpress contends should be construed by the Court.

The below list of terms for construction reflects InfoExpress's presently selected claim terms, and InfoExpress reserves the right to add, eliminate, amend, supplement, or modify the proposed terms, and their constructions, for any reason, including after consideration of Cisco's and Fortinet's proposed terms and constructions and following any meet-and-confer discussions regarding the parties' terms and constructions.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 248 of 1144
INFOEXPRESS, INC. - EX2572

Proposed Claim Terms, Phrases, Clauses For Construction	Asserted Patent Claims
"reconfigure the communication device" "configuring/reconfiguring . . . access point" "wherein the access point is reconfigured"	'484 patent, claim 1 '350 patent, claims 1, 1, 18; '450 patent, claims 1, 3, 4, 22; '444 patent, claims 2, 3, 4, 5, 7, 22; '645 patent, claim 1 '350 patent, claim 4
"configuring . . . communication port" "configuring/reconfiguring/reconfigure . . . communication port" "reconfiguring a port on the communication device"	'484 patent, claims 57, 58 '484 patent, claims 27, 28, 41, 57, 71; '460 patent, claims 1, 16, 22 '484 patent, claim 20
"the applying of the security policy taking place under control of the gatekeeper" "a gatekeeper stored in memory and executable to: . . . evaluate device information received from the device in response to the audit request" "applying a security policy" "application of the security policy"	'444 patent, claim 1, 22 '645 patent, claim 1 '484 patent, claims 27, 28, 41, 43, 66, 68, 82; '460 patent, claims 1, 3, 5, 16, 18, 20; '450 patent, claims 1, 2, 16, 22; '444 patent, claims 1, 2, 22 '450 patent, claims 1, 16, 22
"system data"	'484 patent, claims 4, 5, 43, 66, 68; '460 patent, claims 3, 4, 5, 6, 18, 19, 20, 21
"audit data"	'350 patent, claims 1, 6, 8, 9, 10, 13, 18, 19; '444 patent, claims 1, 5, 6, 7, 10, 11, 12, 13, 14, 22
"SF"	'645 patent, claims 2, 5

Dated: March 22, 2024

Respectfully submitted,

s/Brian R. Michalek
Brian R. Michalek (SBN 302007)

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing document has been served via e-mail on **March 22, 2024,** to all counsel of record who are deemed to have consented to electronic service via the Court's CM/ECF system.

s/Andrew Schwerin
Andrew Schwerin (*pro hac vice*)

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 250 of 1144
INFOEXPRESS, INC. - EX2572

EXHIBIT R

Brian R. Michalek (SBN 302007)
Casey T. Grabenstein (*pro hac vice*)
Joseph M. Kuo (*pro hac vice*)
SAUL EWING LLP
161 N. Clark St., Suite 4200
Chicago, IL 60601
Telephone: (312) 876-7100
Facsimile: (312) 876-0288
brian.michalek@saul.com
casey.grabenstein@saul.com
joseph.kuo@saul.com

Andrew Schwerin (*pro hac vice*)
SAUL EWING LLP
Centre Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102 2186
Telephone: (215) 972-7184
Facsimile: (215) 972-7184
andrew.schwerin@saul.com

Michael E. Flynn-O'Brien (SBN 291301)
Brenda Entzminger (SBN 226760)
BUNSOW DE MORY LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: (650) 351-7245
Facsimile: (415) 426-4744
mflynnobrien@bdiplaw.com

Attorneys for Plaintiff InfoExpress Inc.

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

INFOEXPRESS INC. Plaintiff, v. **CISCO SYSTEMS, INC.** Defendant.	**Case No. 4:23-cv-02698-YGR** **PLAINTIFF INFOEXPRESS'S PRELIMINARY CLAIM CONSTRUCTIONS AND EXTRINSIC EVIDENCE, PER PATENT L.R. 4-2**

INFOEXPRESS INC., Plaintiff, v. **FORTINET, INC.**, Defendant.	**Case No.: 4:23-cv-04389-YGR** **PLAINTIFF INFOEXPRESS'S PRELIMINARY CLAIM CONSTRUCTIONS AND EXTRINSIC EVIDENCE, PER PATENT L.R. 4-2**

I. Introduction

Pursuant to Patent Local Rule 4-2, Plaintiff InfoExpress Inc. hereby provides its preliminary claim constructions and extrinsic evidence with respect to that identified for the Asserted Patents, U.S. Patent Nos. 7,523,484 (the '484 Patent); 8,051,460 (the '460 Patent); 8,677,450 (the '450 Patent); 8,578,444 (the '444 Patent); 8,347,350 (the '350 Patent); and 8,117,645 (the '645 Patent). InfoExpress further identifies the intrinsic and extrinsic evidence in support of such constructions.

InfoExpress reserves the right to add, eliminate, amend, supplement, or modify the proposed terms, their constructions, and the evidence in support thereof for any reason, including after consideration of Defendants' proposed terms and constructions and following any meet-and-confer discussions regarding the parties' terms and constructions.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 253 of 1144
INFOEXPRESS, INC. - EX2572

II. Constructions and Evidence

a. InfoExpress's Terms

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
1.	"reconfigure the communication device" "configuring/reconfiguring . . . access point" "wherein the access point is reconfigured"	'484 patent, claim 1 '350 patent, claims 1, 1, 18; '450 patent, claims 1, 3, 4, 22; '444 patent, claims 2, 3, 4, 5, 7, 22; '645 patent, claim 1 '350 patent, claim 4	**Construction**: Plain and ordinary meaning; no construction necessary. **Intrinsic Evidence**: '484 Patent, [1] FIGS. 2, 3A, 3B, 4, 5, 6, 7, 8, 9, Abstract, 3:20-25, 3:26-29, 3:39-42, 4:1-22, 4:30-43, 5:41-48; 8:18-23, 9:20-29, 9:38-40, 9:57-67, 10:3-8, 10:37-44, 10:45-54, 11:25-30, 12:17-35, 12:44-52, 13:10-37, 13:46-51; U.S. Prov. Appl. No. 60/505,582, pp. 4, 5, 6, 7, 8, FIGS. 3-4, Appendix; U.S. Prov. Appl. No. 60/513,080, pp. 4, 5, 6, 7, 8, 9, 10, 11, 12, FIGS. 3, 4, 5a, 5b, 6. 7a, 7b, Appendix; any evidence relied upon by Defendants. **Extrinsic Evidence**: Expert testimony directed to the meaning of claim term within the context of the intrinsic and extrinsic evidence and any opinion responsive to Defendants' proposed constructions; IEEE 802.1x (versions 2001, 2004, 2010, and 2020); any evidence relied upon by Defendants.

[1] All references to the patent specification are to the '484 patent, unless otherwise noted.

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
2.	"configuring . . . communication port" "configuring/reconfiguring/reconfigure . . . communication port"	'484 patent, claims 57, 58 '484 patent, claims 27, 28, 41, 57, 71; '460 patent, claims 1, 16, 22	**Construction**: Adjusting settings or parameters associated with a communication port

	"reconfiguring a port on the communication device"	'484 patent, claim 20	**Intrinsic Evidence**: '484 Patent, FIGS. 2, 3A, 3B, 4, 5, 6, 7, 8, 9, Abstract, 3:20-25, 3:26-29, 3:39-42, 4:1-22, 4:30-43, 5:41-48; 8:18-23, 9:20-29, 9:38-40, 9:57-67, 10:3-8, 10:37-44, 10:45-54, 11:25-30, 12:17-35, 12:44-52, 13:10-37, 13:46-51; U.S. Prov. Appl. No. 60/505,582, pp. 4, 5, 6, 7, 8, FIGS. 3-4, Appendix; U.S. Prov. Appl. No. 60/513,080, pp. 4, 5, 6, 7, 8, 9, 10, 11, 12, FIGS. 3, 4, 5a, 5b, 6. 7a, 7b, Appendix; any evidence relied upon by Defendants. **Extrinsic Evidence**: Expert testimony directed to the meaning of the claim term within the context of the intrinsic and extrinsic evidence and any opinion responsive to Defendants' proposed constructions; IEEE 802.1x (versions 2001, 2004, 2010, and 2020); Request for Comments (RFC) 3580 ("IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines"), RFC 2865 ("Remote Authentication Dial In User Service (RADIUS)"); Cisco, *802.1x*,[2] at, e.g. 3 ("Configuration Overview"); Cisco, *802.1X Authentication Services Configuration Guide, Cisco IOS Release 15M*;.[3] any evidence relied upon by Defendants.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 256 of 1144
INFOEXPRESS, INC. - EX2572

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
3.	"the applying of the security policy taking place under control of the gatekeeper" "a gatekeeper stored in memory and executable to: . . . evaluate device	'444 patent, claim 1, 22 '645 patent, claim 1	**Construction**: Plain and ordinary meaning; no construction necessary.

[2] https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/5-x/security/cisco-apic-security-configuration-guide-50x/m_802_1x.pdf

[3] https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/15-mt/sec-user-8021x-15-mt-book.pdf#page20

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
	information received from the device in response to the audit request" "applying a security policy" "application of the security policy"	'484 patent, claims 27, 28, 41, 43, 66, 68, 82; '460 patent, claims 1, 3, 5, 16, 18, 20; '450 patent, claims 1, 2, 16, 22; '444 patent, claims 1, 2, 22 '450 patent, claims 1, 16, 22	**Intrinsic Evidence**: FIGS. 1, 2, 3A, 3B, 4; Abstract; 2:14-25, 2:52-56, 3:60-67, 4:18-19, 5:1-8, 5:40-42, 5:57-60, 6:34-61, 7:27-31, 10:33-38, 11:56-67, 12:1-20, 12:35-40, 13:39-45, 13:63-66, 15:37-41; U.S. Prov. Appl. No. 60/505,582, pp. 1, 6, 8, Appendix; U.S. Prov. Appl. No. 60/513,080, pp. 1, Appendix; '450 patent file wrapper at 120-33; any evidence relied upon by Defendants. **Extrinsic Evidence**: Expert testimony directed to the meaning of claim term within the context of the intrinsic and extrinsic evidence and any opinion responsive to Defendants' proposed constructions; any evidence relied upon by Defendants.
4.	"system data"	'484 patent, claims 4, 5, 43, 66, 68; '460 patent, claims 3, 4, 5, 6, 18, 19, 20, 21	**Construction**: Data for operating system status, antivirus Software status, information concerning devices connected to access devices, Windows registry information, MAC address, IP addresses, cookies, status of applications executing on access device.

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
			Intrinsic Evidence: 11:39-50; 14:57-60; U.S. Prov. Appl. No. 60/505,582, pp. 3-5, 11; U.S. Prov. Appl. No. 60/513,080, pp. 3-4, 9, 11; '484 patent file wrapper at 101-02; all papers and exhibits filed in *Cisco Systems, Inc. v. InfoExpress Inc.*, IPR2024-00539 (PTAB) ('460 patent); any evidence relied upon by Defendants. **Extrinsic Evidence**: Expert testimony directed to the meaning of claim term within the context of the intrinsic and extrinsic evidence and any opinion responsive to Defendants' proposed constructions; any evidence relied upon by Defendants.
5.	"audit data"	'350 patent, claims 1, 6, 8, 9, 10, 13, 18, 19; '444 patent,	**Construction**: Data relating to compliance for a security policy.

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
		claims 1, 5, 6, 7, 10, 11, 12, 13, 14, 22	**Intrinsic Evidence**: FIG 4; 10:33-37, 11:39-55, 12:39, 13:8-9, 14:9, 15:15; U.S. Prov. Appl. No. 60/505,582, pp. 2, 4-5, 6, 8, Appendix; any evidence relied upon by Defendants. **Extrinsic Evidence**: Expert testimony directed to the meaning of claim term within the context of the intrinsic and extrinsic evidence and any opinion responsive to Defendants' proposed constructions; any evidence relied upon by Defendants.
6.	"SF" "wherein the SF is part of the ESL"	'645 patent, claims 2, 5	**Construction**: Plain and ordinary meaning; alternatively, a server filter (SF).

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
			Intrinsic Evidence: '484 Patent, 8:38-45, 8:60-67, 9:58-67, 14:1-17, 14:18-26, 14:27-34, 14:35-41, 14:42-56, 14:57-67; 15:1-4, 15:5-13, 5:14-19, FIGS. 5, 6A, 6B, 7, 8A, 8B, 9; U.S. Prov. Appl. No. 60/505,582, pp. 2, 3; U.S. Prov. Appl. No. 60/513,080, pp. 2, 3, 6, 7, 8, 9, 10, 11, 12, FIGS. 3, 4, 5a, 5b, 6, 7a, 7b, Appendix. **Extrinsic Evidence:** Expert testimony directed to the meaning of claim term within the context of the intrinsic and extrinsic evidence and any opinion responsive to Defendants' proposed constructions.

b. Cisco's Terms

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
7.	access control	'484 patent claim 1C '350 patent claim 1PRE '645 patent claims 1PRE, 2, 5, 6	**Construction**: Plain and ordinary meaning; no construction necessary. **Intrinsic Evidence:** '484 Patent, FIGS. 2, 3A, 3B, 4, 5, 6, 7, 8, 9, Abstract, 1:26-32, 1:53-55, 3:20-25, 3:26-29, 3:39-42, 4:1-22, 4:30-43, 5:41-48; 8:18-23, 9:20-29, 9:38-45, 9:57-67, 10:3-8, 10:37-44, 10:45-54, 10:55-63, 11:25-30, 12:17-37, 12:44-52, 12:53-56, 13:3-9, 13:10-37, 13:46-51, 15:20-54, 15:55-67; U.S. Prov. Appl. No. 60/505,582, pp. 4, 5, 6, 7, 8, FIGS. 3-4, Appendix; U.S. Prov. Appl. No. 60/513,080, pp. 4, 5, 6, 7, 8, 9, 10, 11, 12, FIGS. 3, 4, 5a, 5b, 6. 7a, 7b, Appendix; '350 patent file wrapper at 26, 30 (and U.S. Patent No. 7,752,320 to Kappes, cited therein), 34 (and U.S. Patent Pub. No. 2003/0229808 A1 to Heintz, cited therein), 38 (and U.S. Patent Pub. No. 2006/0147043 to Mann, cited therein), 136, 138, 171-72, 173-74, 189, 205, 290; '444 patent file wrapper at 72, 83 (and Mann, cited therein), 96, 99, 101, 143, 146 (and PCT Publication 2000/56027 A1 to Bacic, cited therein), 148, 157, 164, 170, 195; '450 patent file wrapper at 71, 82, 92, 95, 103, 124 (and Mann, cited therein), 163-66, 178, 181, 183, 192,

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 262 of 1144
INFOEXPRESS, INC. - EX2572

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
			199, 205, 230, 236, 291; '460 patent file wrapper at 14, 105 (and InfoExpress's patent applications cited therein), 123-25, 135 (and InfoExpress's patent applications cited therein), 141, 228-31; '484 patent file wrapper at 68 (and "Network Access Control from Mirage Networks," cited therein), 72 (and InfoExpress's patent applications cited therein), 78 (and PCT Publication 2006/029217 A1 to Foss, cited therein), 103, 117, 121, 224, 227, 229, 292, 295-96; '645 patent file wrapper at 19-20, 21-22 (and Kappes, cited therein), 23-26 (and Mann, cited therein), 29-32 (and specification references cited therein), 183; any evidence relied upon by Defendants. **Extrinsic Evidence:** Expert testimony; 802.1x (all versions); U.S. Patent Pub. No. 2005/0055570 ("Kwan 570 "), at, e.g., [0012]; U.S. Patent No. 7,185,360 (Anton) at, e.g., Title; U.S. Patent No. 7,334,254 (Boydstun) at, e.g., 1:41; U.S. Patent No. 7,334,254 6,230,271 (Wadlow) at, e.g., Title; 4:25-37; U.S. Patent Pub. No. 2006/0190984 (Heard) at, e.g., [0029], [0034]]; U.S. Patent No. 6,317,838 (Baize); Perfigo SecureSmart (CISCO-INFOEXPRESS_00005138) at, e.g., 3; Cisco Buys Perfigo (CISCO-INFOEXPRESS_00003873) at, e.g., 1; U.S. Patent Publication No. 2002/0069366 ("Schoettger 366") at,

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
			e.g., [0004]; U.S. Patent Pub. No. 2002/0138726 ("Sames 726") at, e.g., [0007]-[0009]; Maryville at, e.g., 1, 2 (cited in Fortinet's Invalidity Contentions, Chart A-27); Kerberos Network Authentication Protocol at, e.g., 2 (cited in Fortinet's Invalidity Contentions, Chart A-28); Sentinel Model III Computer Security System Security Target at, e.g., 2 (cited in Fortinet's Invalidity Contentions, Chart A-30); Computer Access Control Systems ("Benantar") at, e.g., 95 (cited in Fortinet's Invalidity Contentions, Chart A-31); Micro-Firewalls for Dynamic Network Security ("Micro-Firewalls") at, e.g., 69 (cited in Fortinet's Invalidity Contentions, Chart A-33); U.S. Patent No. 7,325,246 (Halasz) at, e.g., 1:44; U.S. Patent No. 7,506,054 (Fuh) at, e.g., Abstract; U.S. Patent Pub. No. 2005/0055573 (Smith) at, e.g., Abstract; U.S. Patent No. 6,219,706 B1 (Fan) at, e.g. Abstract; any evidence relied upon by Defendants.
8.	access control list	'484 patent claims 2, 59 '450 patent claim 3 '444 patent claim 3	**Construction**: Plain and ordinary meaning; no construction necessary. **Intrinsic Evidence**: '484 Patent, 2:62-67; 6:25-27, 7:1; 8:45-67; 9:45-67; 10:18-20, 10:57-62; 11:2-6, 12:27-32, 12:44-66, 13:1-9, 13:29-45, FIGS. 3A, 3B;

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 264 of 1144
INFOEXPRESS, INC. - EX2572

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
			U.S. Prov. Appl. No. 60/505,582, pp. 1, 6, 8; U.S. Prov. Appl. No. 60/513,080, pp. 1, 12; '350 patent file wrapper at 173-74; '444 patent file wrapper at 129, 195 (and PCT Publication 2000/56027 A1 to Bacic, cited therein); '450 patent file wrapper at 82 (and U.S. Patent Pub. No. 2006/0147043 to Mann, cited therein), 124, 163, 230; '460 patent file wrapper at 123, 229; '484 patent file wrapper at, e.g., 101 (and Mann, cited therein); any evidence relied upon by Defendants. **Extrinsic Evidence**: Expert testimony; Internet Security Glossary, Version 2 (RFC 4949; any evidence relied upon by Defendants.
9.	gatekeeper	'484 patent claims 1PRE, 1B, 1C, 2, 3, 4, 5, 11, 12, 13, 15, 16, 17, 18, 19, 20, 23, 24, 25, 27A, 27C, 28A, 28C, 41A, 41C, 43, 57A, 57B, 68, 71, 82A, 82C '460 patent claims 1A, 1C, 1D, 5, 16A, 16C, 20, 22 '450 patent claims 1C, 2	**Construction**: Plain and ordinary meaning; no construction necessary. **Intrinsic Evidence:** '484 Patent, Abstract; FIGS. 1, 2, 3A, 3B, 5; 1:53-63, 1:64-67, 2:1-4, 2:14-25, 2:26-42, 2:52, 3:20, 3:26-42, 3:48, 3:59, 3:61, 4:18, 4:32, 5:2, 5:5, 5:29-50, 5:58, 6:6, 6:14-16, 6:34-48, 6:49-61, 6:62-67, 7:1-6, 7:19-26, 7:29, 7:50, 7:52, 8:25-30, 8:47, 9:20-21, 9:30-31, 9:54, 10:6-14, 10:20, 10:34, 10:39, 10:53, 10:61-62, 11:10-30, 12:24, 13:29-45, 13:46-54, 13:64, 15:32-36, 15:37-54; U.S. Prov. Appl. No. 60/505,582, pp. 1, 2, 3, 4, 5, 6, 7, 8, 11, FIGS. 1, 2, 3; U.S. Prov. Appl. No. 60/513,080, pp.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 265 of 1144
INFOEXPRESS, INC. - EX2572

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
		'444 patent claims 1C, 1D, 7, 17, 22C, 22D '645 patent claims 1[B-i], 1[C-ii], 2	1, 2, 3, 6, 7, 9, 10, 11, 12, 15; FIGS. 1, 2, 4, 6, 7a, 7b, Appendix; '350 patent file wrapper at 132; '444 patent file wrapper at 82 (and U.S. Patent Pub. No. 2006/0147043 to Mann, cited therein), 84, 138 (and Mann and further U.S. Patent No. 7,373,508 to Meier, cited therein), 81-82, 121-22, 126, 132-33; '484 patent file wrapper at 100-03 (and Mann, cited therein); '645 patent file wrapper at 19-20 (and U.S. Patent No. 5,842,002 to Schnurer, cited therein), 21-22 (and U.S. Patent No. 7,752,320 to Kappes, cited therein), 23-24 (and U.S. Patent Pub. No. 2003/0229808 to Heintz, cited therein), 27, 29-30; any evidence relied upon by Defendants. **Extrinsic Evidence**: Expert testimony including that responsive to Defendants' proposed constructions; U.S. Patent No. 6,609,198 (Wood) at, e.g., 4:9-14, 5:44; U.S. Patent No. 7,334,254 ("Boydstun") at, e.g., Abstract; U.S. Patent Publication No. 2006/0190984 A1, Heard et al. ("Heard ") (titled "Gatekeeper architecture/features to support security policy maintenance and distribution"); U.S. Patent No. US 7,359,962 B2 Willebeek-LeMair et al. ("LeMair") at 6:25; InfoExpress's own CyberGatekeeper LAN and CyberGatekeeper Remote literature (cited in Cisco's Invalidity Contentions Chart A-17); U.S.

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
			Patent No. 7,359,967 ("Synnestvedt 967") at 2:35-37; any evidence relied upon by Defendants.
10.	policy auditor	'484 patent claims 1A, 6	**Construction**: Plain and ordinary meaning; no construction necessary. **Intrinsic Evidence**: '484 patent, 9:31-38; *see also* 11:31-34; FIGS 3A, 3B, 4; any evidence relied upon by Defendants. **Extrinsic Evidence**: Expert testimony including that responsive to Defendants' proposed construction; any evidence relied upon by Defendants.
11.	[EAP] authentication module	'645 patent claims 1[B-i], 1[C-ii], 2	**Construction**: The term "EAP authentication module(s)" is entitled to its plain and ordinary meaning; no construction necessary. **Intrinsic Evidence**: '484 patent, FIGS. 5, 6A, 6B, 7; 1:31-40, 1:41-52, 2:14-19,10:34, 11:31-38, 12:38, 13:8, 13:62-67, 14:1-1, 14:18-26, 14:27-34, 14:41, 14:42-49, 14:50-67; '645 patent file wrapper at 19-20 (and U.S. Patent No. 5,842,002 to Schnurer, cited therein), 21-22 (and U.S. Patent No. 7,752,320 to Kappes, cited therein), 23-24 (and U.S. Patent Pub. No. 2003/0229808 to Heintz, cited therein), 24-25 (and U.S. Patent Pub. No. 2006/0147043 to Mann, cited therein), 27, 29-30; any evidence relied upon by Defendants.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 267 of 1144
INFOEXPRESS, INC. - EX2572

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
			U.S. Prov. Appl. No. 60/505,582, pp. 3; U.S. Prov. Appl. No. 60/513,080, pp. 5, 6, 7, 8, 9, 10, 11, 12; Xin Zhao et al, SVGrid: *A Secure Virtual Environment For Untrusted Grid Applications*, MGC '05: Proceedings of the 3rd International Workshop on Middleware for Grid Computing (cited in '484 file wrapper at 294);[4] PCT Publication 2000/56027 A1 (cited in '484 file wrapper at 175, and 179-248); '444 file wrapper at 126-128. **Extrinsic Evidence**: 802.1x (all versions); expert testimony including that responsive to Defendants' proposed constructions; any evidence relied upon by Defendants.
12.	server filter/SF	'645 patent claims 2, 5	**Construction**: Addressed above at term no. 6. **Evidence**: Addressed above at term no. 6.
13.	code segment	'484 patent claims 82A, 82B, 82C, 82D, 82E	**Construction**: Not needed; claim not at issue. **Evidence**: Not needed; claim not at issue.

[4] https://web.eecs.umich.edu/~aprakash/papers/svgrid-grid-computing-workshop.pdf

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
14.	element	'484 patent claim 20	**Construction**: Not needed; claim not at issue. **Evidence**: Not needed; claim not at issue.
15.	EAP [encryption] protocol	'444 patent claims 1A, 8 '450 patent claim 7 '645 patent claims 1C, 1[C-i], 2, 6	**Construction**: Plain and ordinary meaning; no construction necessary. **Intrinsic Evidence:** '484 Patent, 5:13-14, 8:24-30, 12:33-40, 14: 14:1-17, 14:18-26, 14:27-34, 14:35-41, 14:42-56, 14:57-67; FIGS. 5, 6A, 6B, 7, 8A, 8B, 9; U.S. Prov. Appl. No. 60/505,582, pp. 3; U.S. Prov. Appl. No. 60/513,080, pp. 4, 5, 6, 7, 8, 9, 10, 11, FIGS. 3, 4, 5a, 5b, 6, 7a, 7b, Appendix; '444 patent file history at 121-134; '645 patent file wrapper at 19-20 (and U.S. Patent No. 5,842,002 to Schnurer, cited therein), 21-22 (and U.S. Patent No. 7,752,320 to Kappes, cited therein), 23-24 (and U.S. Patent Pub. No. 2003/0229808 to Heintz, cited therein), 24-25 (and U.S. Patent Pub. No. 2006/0147043 to Mann, cited therein), 27, 29-30; any evidence relied upon by Defendants. **Extrinsic Evidence:** Expert testimony including that responsive to Defendants' proposed constructions; RFC 5247, RFC 2284, RFC 3748 and any related versions;.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 269 of 1144
INFOEXPRESS, INC. - EX2572

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
			802.1x (all versions), any evidence relied upon by Defendants.
16.	monitor	'460 patent claim 22	**Construction**: Plain and ordinary meaning; no construction necessary.
			Intrinsic Evidence: '484 patent, 7:19-26, 11:51-55; any evidence relied upon by Defendants. **Extrinsic Evidence**: Expert testimony including that responsive to Defendants' proposed constructions; any evidence relied upon by Defendants.
17.	update the access device	'460 patent claim 27	**Construction**: Plain and ordinary meaning; no construction necessary.
			Intrinsic Evidence: '484 Patent, 6:6-16, 6:34-48, 7:27-29, 7:39-50, 11:44-50, 12:10-16, FIGS. 2, 3A, 3B; U.S. Prov. Appl. No. 60/513,080, pp. 11; any evidence relied upon by Defendants. **Extrinsic Evidence:** Expert testimony including that responsive to Defendants' proposed constructions;. any evidence relied upon by Defendants.
18.	and that contains antivirus software	'350 patent claim 9	**Construction**: Plain and ordinary meaning; no construction necessary.
			Intrinsic Evidence: 6:48, 7:43-44, 11:46, 12:14-16.

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
			'350 patent file wrapper at 28 (and U.S. Patent No. 5,842,002 to Schnurer, cited therein); 32 (and U.S. Patent No. 7,752,320 to Kappes, cited therein), 36 (and U.S. Patent Pub. No. 2003/0229808 to Heintz, cited therein), 40 (and U.S. Patent Pub. No. 2006/0147043 to Mann, cited therein), 43, 48; '444 patent file wrapper at 83 (and Mann); '484 patent file wrapper at 102 (and Mann, cited therein). **Extrinsic Evidence:** Expert testimony.
19.	different subset	'350 patent claim 4	**Construction**: Plain and ordinary meaning; no construction necessary.
			Intrinsic Evidence: '350 patent, 15:56-60; 16:15-16; any evidence relied upon by Defendants. **Extrinsic Evidence:** Expert testimony including that responsive to Defendants' proposed claim constructions.

c. Fortinet's Terms

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
20.	protected network	'484 Patent, claims 28, 41, 56, 57, 59 '460 Patent, claims 1, 16	**Construction**: Plain and ordinary meaning; no construction necessary. **Intrinsic Evidence**: FIGS. 2, 3B, 4; 2:48-67; 3:1-16, 3:60-67, 4:1-43, 4:66-67, 5:5-7, 5:9-11, 5:36-39, 5:49-55, 6:1-6, 6:21-27, 6:34-36, 6:62-67, 7:2-5,7:35-37, 7:48, 8:38-45, 8:53-55, 9:50, 10:8-14, 10:15-17, 11:4-6, 12:29-30, 12:53-56, 13:1-5, 13:20-26, 13:36-37, 13:48-49 any evidence relied upon by Defendants '484 patent file wrapper at 103. **Extrinsic Evidence**: Expert testimony including that responsive to Defendants' proposed claim constructions; any evidence relied upon by Defendants.
21.	access control 35 U.S.C. § 112(6)	'484 Patent, claim 1	**Construction**: Addressed above at term no. 7. **Evidence**: Addressed above at term no. 7.
22.	the protected network	'460 Patent, claim 16	**Construction**: Addressed above at term no. 20. **Evidence**: Addressed above at term no. 20.
23.	policy auditor 35 U.S.C. § 112(6)	'484 Patent, claim 1, 12, 15	**Construction**: Addressed above at term no. 10.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 272 of 1144
INFOEXPRESS, INC. - EX2572

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
			Evidence: Addressed above at term no. 10.
24.	audit/auditing	'484 Patent, claim 1, 13, 39, 42 '350 Patent, claim 1, 6, 8, 9, 10, 13, 18, 19 '450 Patent claim 16, 22, 23, 25 '444 Patent claim 22	**Construction**: To evaluate the compliance of a security policy. **Intrinsic Evidence**: FIGS. 7, 8A, 8B; Abstract; 3:64-65, 4:5-9, 9:35, 11:40, 11:56-65, 12:15-16, 12:20, 13:42-45; 13:63, 14:14-17, 14:20, 14:50-67, 15:1-19; *see also* term no. 5 above. U.S. Prov. Appl. No. 60/505,582, pp. 1, 2, 4, 5, 6, 7, 8, 11, 12, 14; U.S. Prov. Appl. No. 60/513,080, pp. 1, 2, 3, 9, 10, 11, 12, 15, 16, Appendix. **Extrinsic Evidence**: Expert testimony including that responsive to Defendants' proposed constructions; any evidence relied upon by Defendants.
25.	audit data	'350 Patent claims 1, 6, 8, 9, 10, 13, 18, 19 '460 Patent claim 1 '444 Patent claims 1, 5, 6, 10, 12, 22	**Construction**: Addressed above at term no. 5. **Evidence**: Addressed above at term no. 5.
26.	update module 35 U.S.C. §112(6)	'484 Patent, claim 3	**Construction**: Addressed above at term no. 17. **Evidence**: Addressed above at term no. 17.

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
27.	access to the restricted subset of the protected network [is / being] responsive to a VLAN configured to communicate with the protected network subject to the access control list	'484 Patent, claim 56 '460 Patent, claim 30	**Construction**: Plain and ordinary meaning; no construction necessary.
			Intrinsic Evidence: 12:44-52; *see also* FIGS. 3A, 3B; 2:5-13, 2:63-65, 3:1-25, 3:28, 3:46, 3:51, 3:55-59, 5:49, 5:62, 7:64-67, 8:1-12, 8:13-23, 8:58-67, 9:17, 9:25-26, 9:58-62, 10:4, 10:15, 10:21, 10:58, 11:1-9, 12:28, 12:42, 12:52, 12:58-67, 15:2-3; 15:11, 15:18-19, 15:28-31, 15:50-53; any evidence relied upon by Defendants. **Extrinsic Evidence:** Expert testimony including that responsive to Defendants' proposed constructions; 802.1x (all versions); any evidence relied upon by Defendants.
28.	the application of the security policy taking place in response to a gatekeeper	'450 Patent, claim 1	**Construction**: Plain and ordinary meaning; no construction necessary.
			Intrinsic Evidence: FIGS. 1, 2, 3A, 3B, 4; Abstract; 2:14-25, 2:52-56, 3:60-67, 4:18-19, 5:1-8, 5:40-42, 5:57-60, 6:34-61, 7:27-31, 10:33-38, 11:56-67, 12:1-20, 12:35-40, 13:39-45, 13:63-66, 15:37-41; U.S. Prov. Appl. No. 60/505,582, pp. 1, 6, 8, Appendix; U.S. Prov. Appl. No. 60/513,080, pp. 1, Appendix; '450 patent file wrapper at 120-33; any evidence relied upon by Defendants.

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
			Extrinsic Evidence: Expert testimony including that responsive to Defendants' proposed constructions; any evidence relied upon by Defendants.
29.	EAP protocol / extensible authentication protocol	'444 Patent, claim 1 '450 Patent, claim 7 '645 Patent, claim 1	**Construction**: Addressed above at term no. 15. **Evidence**: Addressed above at term no. 15.
30.	[EAP] authentication module 35 U.S.C. § 112(6)	'645 Patent, claim 1, 6	**Construction**: Addressed above at term no. 11. **Evidence**: Addressed above at term no. 11.
31.	gatekeeper	'484 Patent, claim 1-5, 11-13, 15-19, 23-25, 28, 41, 43, 56, 57, 68 '645 Patent, claim 1, 2 '450 Patent, claim 1, 2 '444 Patent, claim 1, 17, 22 '460 Patent, claim 1, 5, 16, 22,	**Construction**: Addressed above at term no. 9. **Evidence**: Addressed above at term no. 9.
32.	extensible authentication protocol (EAP) server layer (SL)	'645 Patent, claim 1	**Construction**: Plain and ordinary meaning; no construction necessary. **Intrinsic Evidence:** '484 Patent, 5:13-14, 8:24-30, 12:33-40, 14: 14:1-17, 14:18-26, 14:27-34, 14:35-41, 14:42-56, 14:57-67; FIGS. 5, 6A, 6B, 7, 8A, 8B, 9;

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 275 of 1144
INFOEXPRESS, INC. - EX2572

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
			U.S. Prov. Appl. No. 60/505,582, pp. 3; U.S. Prov. Appl. No. 60/513,080, pp. 4, 5, 6, 7, 8, 9, 10, 11, FIGS. 3, 4, 5a, 5b, 6, 7a, 7b, Appendix '645 patent file wrapper at 19-20 (and U.S. Patent No. 5,842,002 to Schnurer, cited therein), 21-22 (and U.S. Patent No. 7,752,320 to Kappes, cited therein), 23-24 (and U.S. Patent Pub. No. 2003/0229808 to Heintz, cited therein), 24-25 (and U.S. Patent Pub. No. 2006/0147043 to Mann, cited therein), 27, 29-30 ; any evidence relied upon by Defendants. **Extrinsic Evidence**: Expert testimony including that responsive to Defendants' proposed claim construction.
33.	EAP encryption protocol	'645 Patent, claim 1	**Construction**: Addressed above at term no. 15; any evidence relied upon by Defendants.
			Evidence: Addressed above at term no. 15; any evidence relied upon by Defendants.
34.	ESL	'645 Patent, claim 2, 5	**Construction**: Addressed above at term no. 32.
			Evidence: Addressed above at term no. 32.
35.	SF / server filter	'645 Patent, claim 2, 5	**Construction**: Addressed above at term no. 12.

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
			Evidence: Addressed above at term no. 12.
36.	EAPM	'645 Patent, claim 1, 6	**Construction**: Addressed above at term no. 30.
			Evidence: Addressed above at term no. 30.
37.	monitor	'460 Patent, claim 22	**Construction**: Addressed above at term no. 16.
			Evidence: Addressed above at term no. 16.
38.	a wireless access point configured to support an 802.1x standard	'484 Patent, claim 17	**Construction**: No construction necessary, that is, plain and ordinary meaning.
			Intrinsic Evidence: '484 Patent, Abstract, 1:35-40, 1:46-52, 5:12-13, 5:24-25, 14:1-3, 14:9-11, FIGS. 5, 6A, 6B, 7, 8A, 8B, 9; U.S. Prov. Appl. No. 60/505,582, pp. 1, 3, 4, Appendix; U.S. Prov. Appl. No. 60/513,080, pp. 1, 4, 5, 6, 7, 8, 9, 10, 11, FIGS. 3, 4, 5a, 5b, 6, 7a, 7b, Appendix. '460 patent file wrapper at 230 (and N. Blefari-Melazzi, et al, *Autonomic Control and Personalizaton of a Wireless Access Network*, 51(10) Computer Networks 2645-76 (2007)[5] cited therein); '444 patent file

[5] http://wpage.unina.it/pescape/cit/PG-5.pdf

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 277 of 1144
INFOEXPRESS, INC. - EX2572

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
			wrapper at 98 (and Y.M. Tseng, USIM-based *EAP-TLS Authentication Protocol for Wireless Local Area Networks* 31 (1) Computer Standards and Interfaces 128-36 (2009),[6] cited therein); 99 (and Munegowda Keshava, *Design and Implementation of WLAN Authentication and Security: Building Secure Wireless LAN by EAP-MD5, EAP-TLS and EAP-TTLS protocols* (2010), 100 (and Jyh-cheng Chen, *Extensible authentication protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience*, 43 IEEE Communications (2005),[7] cited therein), 101 (Weili Huang, *WLAN Authentication System Based on the Improved EAP-TLS Protocol* (2009),[8] I.G. Kim, *Formal verification of PAP and EAP-MD5 protocols in wireless networks*: *FDR model checking*[9] ; '450 patent file wrapper at 290; '645 patent file wrapper at 121 (and references cited therein); any evidence relied upon by Defendants. **Extrinsic Evidence:** Expert testimony including any responsive to Defendants' proposed

[6] https://www.sciencedirect.com/science/article/abs/pii/S0920548907001213

[7] https://ieeexplore.ieee.org/abstract/document/1561920

[8] https://ieeexplore.ieee.org/document/5232480

[9] https://ieeexplore.ieee.org/document/1283800

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 278 of 1144
INFOEXPRESS, INC. - EX2572

	Proposed Claim Terms, Phrases, Clauses For Construction	Claims	InfoExpress's Construction and Supporting Evidence
			construction; , RFC 3580; IEEE 802.1x (all versions); any evidence relied upon by Defendants.
39.	an access point configured to use an 802.1x protocol	'444 Patent, claims 1, 22	**Construction**: Addressed above at term no. 38.
			Evidence: Addressed above at term no. 38.

Dated: March 25, 2024

Respectfully submitted,

s/Brian R. Michalek
Brian R. Michalek (SBN 302007)

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing document has been served via e-mail on **March 25, 2024,** to all counsel of record who are deemed to have consented to electronic service via the Court's CM/ECF system.

s/Andrew Schwerin
Andrew Schwerin (*pro hac vice*)

EXHIBIT S

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INFOEXPRESS, INC.,

Plaintiff,

v.

CISCO SYSTEMS, INC.,

Defendants.

Case No. 4:23-cv-002698-YGR

INFOEXPRESS, INC.,

Plaintiff,

v.

FORTINET, INC.,

Defendants.

Case No. 4:23-cv-004389-YGR

HIGHLY CONFIDENTIAL - ATTORNEYS' EYES ONLY

REMOTE VIDEOTAPED DEPOSITION of

AARON D. STRIEGEL, Ph.D.

Chicago, Illinois

Reporter: Michael D. O'Connor, RMR, CRR, CRC

Thursday, August 1, 2024

11:53 a.m. CDT

HIGHLY CONFIDENTIAL - ATTORNEYS' EYES ONLY

REMOTE VIDEOTAPED DEPOSITION of AARON D. STRIEGEL, Ph.D., held via Zoom videoconference in Chicago, Illinois, pursuant to notice, before Michael D. O'Connor, Registered Merit Reporter, Certified Realtime Reporter, Certified Realtime Captioner.

A P P E A R A N C E S:

ATTORNEYS FOR INFOEXPRESS, INC.:
(Attending Remotely)
SAUL EWING LLP
161 North Clark Street, Suite 4200
Chicago, Illinois 60601
(312) 876-7100
JOSEPH M. KUO, ESQ.
joseph.kuo@saul.com
- and -
(Attending Remotely)
SAUL EWING LLP
Centre Square West
1500 Market Street, 38th Floor
Philadelphia, Pennsylvania 19102-2186
(215) 972-7184
BY: ANDREW SCHWERIN, ESQ.
andrew.schwerin@saul.com

A P P E A R A N C E S (Cont'd):

ATTORNEYS FOR CISCO SYSTEMS, INC.:
(Attending Remotely)
WINSTON & STRAWN LLP
800 Capitol Street, Suite 2400
Houston, Texas 77002-2925
(713) 651-2600
BY: WILLIAM LOGAN, ESQ.
WLogan@winston.com
- and -
(Attending Remotely)
WINSTON & STRAWN LLP
2121 North Pearl Street, Suite 900
Dallas, Texas 75201
(214) 453-6492
BY: PATRICK CLARK, ESQ.
PClark@winston.com

A P P E A R A N C E S (Cont'd):

ATTORNEYS FOR FORTINET, INC.
(Attending Remotely)
DUANE MORRIS
1075 Peachtree Street, NE, Suite 1700
Atlanta, Georgia 30309
(404) 253-6982
BY: DAVID DOTSON, ESQ.
dcdotson@duanemorris.com

Also Present: Joseph Townsend,
Videographer

I N D E X

Deposition of:		Page
AARON D. STRIEGEL, Ph.D.		
By Mr. Logan		8

E X H I B I T S

No.		Page
Exhibit 1	Expert Declaration of Dr. Aaron Striegel, Ph.D. in Support of InfoExpress's Proposed Claim Constructions	11
Exhibit 2	U.S. Patent No. 7,523,484	12

P R O C E E D I N G S

THE VIDEOGRAPHER: Here begins the videotaped deposition of Aaron Striegel, taken in the matter of InfoExpress, Inc. v. Cisco Systems, Inc. and InfoExpress, Inc. v. Fortinet, Inc. in the United States District Court, for the Northern District of California, Oakland Division, first case No. 4:23-CV-002698-YGR. Second case caption case No. 4:23-CV-004389-YGR. 08:13:32 08:13:32 11:52:17 11:52:18 11:52:26 11:52:31 11:52:36 11:52:37 11:52:38 11:52:42 11:52:52

Today's date is August 1, 2024. The time is 11:53 a.m. central daylight time. This deposition is being held remotely via Zoom. The court reporter is Michael O'Connor. My name is Joe Townsend. I'm the video operator. We are both here on behalf of Henderson Legal Services. 11:53:05 11:53:08 11:53:13 11:53:16 11:53:19 11:53:23 11:53:25 11:53:28

Will counsel please introduce themselves and state whom they represent. 11:53:29 11:53:30 11:53:32

MR. LOGAN: William Logan from Winston & Strawn on behalf of Cisco 11:53:35 11:53:38

Systems, and with me today is Patrick Clark, also from Winston & Strawn. 11:53:41 11:53:43

MR. DOTSON: David Dotson from the law firm of Duane Morris on behalf of Fortinet, Inc. 11:53:46 11:53:48 11:53:51

MR. SCHWERIN: Andrew Schwerin with the law firm of Saul Ewing, representing Plaintiff, InfoExpress, Inc. 11:53:53 11:53:55 11:53:58 11:53:59

THE VIDEOGRAPHER: Will the court reporter please administer the oath. 11:54:01 11:54:03

AARON D. STRIEGEL, Ph.D.

having been duly sworn by the Notary Public, was examined and testified as follows:

EXAMINATION

BY MR. LOGAN: 11:54:27

Q. Good morning. Would you please state your name again for the record. 11:54:27 11:54:28

A. Sure. My name is Aaron Striegel, S-t-r-i-e-g-e-l. 11:54:30 11:54:35

Q. And it's Dr. Striegel; is that correct? 11:54:35 11:54:38

A. That is correct. 11:54:38

Q. Dr. Striegel, where are you joining from today? I know you're joining remotely? 11:54:38 11:54:40 11:54:43

A. Sure. I'm joining from Chicago at the offices of Saul Ewing. 11:54:44 11:54:49

Q. And who is in the room with you? 11:54:51

A. Currently in the room with me is Andrew Schwerin and Joseph Kuo. 11:54:52 11:54:54

Q. And those are both attorneys for InfoExpress; is that correct? 11:54:59 11:55:05

A. Yes. 11:55:07

Q. Dr. Striegel, have you given depositions before? 11:55:07 11:55:12

A. I have. 11:55:17

Q. I know you're probably familiar with all the kind of, you know, underlying rules and procedures, but one thing I do want to highlight for you is that, you know, today I'm going to ask questions, and I'm probably going to ask some of them poorly. So if at any point you don't understand my question and need clarification, I would greatly appreciate it if you would let me know. 11:55:18 11:55:19 11:55:21 11:55:23 11:55:26 11:55:29 11:55:31 11:55:34 11:55:36

Is that fair? 11:55:40

A. That is fair. I'll do my best, but I do reserve the right upon further reflection if I maybe at the time didn't understand it to appropriately denote that later. 11:55:40 11:55:43 11:55:45 11:55:48 11:55:50

Q. And if you do realize later in the day as we're talking that you misunderstood something earlier, would you please call that out to my attention so we can address it while we're here? 11:55:50 11:55:52 11:55:54 11:55:56 11:55:59

A. Sure. 11:55:59

Q. Dr. Striegel, you have produced an expert report in this case on claim construction; is that correct? 11:56:00 11:56:05 11:56:07

A. I believe that would be correct, although I think it's a declaration; at least that was the title. 11:56:08 11:56:12 11:56:16

Q. Fair enough. I'm happy to call it that. You've produced in this case an expert declaration in support of InfoExpress' proposed claim construction; is that fair? 11:56:17 11:56:20 11:56:22 11:56:28

A. I believe that would be the title of the report. 11:56:30 11:56:32

Q. All right. I've loaded in the share file Exhibit 1. Would you open that for 11:56:32 11:56:33

me? 11:56:36

(Document marked as Exhibit 1 11:56:36

for identification) 11:56:54

A. Okay. I have the file. Yes, I'm able to open it. 11:56:54

Q. Do you recognize this file? 11:56:56

A. I don't know about the exact file name, but at least the front matter, yes. 11:56:58

Q. Does this appear to be the expert declaration that you've issued in this case about claim construction? 11:57:06

A. Yes, that does appear to be the case. And, Counsel, I do have a printed copy with me as well that is unmarked as provided by my counsel. And just to clarify, it would be okay if I refer to that as well? 11:57:08

Q. Very well. That's perfectly fine. 11:57:11

A. Thank you, sir. 11:57:14

Q. Dr. Striegel, if we go to Paragraph 1, it lists there six patents that you've offered opinions on. 11:57:15

Do you see that? 11:59:31

A. I do see that. 11:59:33

Q. Is it your understanding that those patents all share a common specification? 11:59:36

A. If I recall, I believe that's the case, that they all have the same specification with different claims later.

Q. If we go to Paragraph 40, just to confirm, I think you state there, I understand the asserted patent share a common specification, right?

A. I do see that.

(Document marked as Exhibit 2 for identification)

Q. I only say this to kind of, you know, streamline things today. I put the '484 patent, we'll talk about it shortly, as Exhibit 2. But if at any point you feel there's a reason we should look at one of the other patents if there's some difference you feel like, please let me know and we'll do that. Okay?

A. Sure.

Q. While I have you in Paragraph 40, I do have one question. There's a statement here that "Thus, the priority date of the asserted patents is September 24, 2003."

Do you see that?

A. Which line is that, Counsel?

Q. I believe the second to last line in Paragraph 40. 12:01:26 12:01:28

A. I do see that now. 12:01:29

Q. Is that still your opinion today? 12:01:30

A. I believe that's what I wrote in my report, so that would be my opinion. 12:01:32 12:01:35

Q. If we go to Paragraph 35, so it's a little bit above where you are now, there's another term that's used there that's "claimed priority date." 12:01:38 12:01:48 12:01:51 12:01:54

Do you see that? 12:01:55

A. Which paragraph was that, Counsel? I'm reading. 12:01:56 12:02:12

Q. It's in 35. I believe it also shows up in 36 -- 35 and 36. 12:02:13 12:02:15

A. Okay. Now I see that, Counsel. 12:02:18

Q. I believe those are the only two paragraphs where the term "claimed priority date" shows up. 12:02:24 12:02:27 12:02:31

Are you aware of any difference between the claimed priority date and the priority date that you mentioned in Paragraph 40? 12:02:32 12:02:33 12:02:35 12:02:37

A. To the best of my knowledge, no. 12:02:37

Q. You're a professor at Notre Dame; 12:02:51

is that right? 12:03:01

A. That is correct. 12:03:03

Q. Very nice school. What are you a professor of? 12:03:08

A. I'm a professor of computer science and engineering. 12:03:09

Q. When did you become a professor of computer science and engineering at Notre Dame? 12:03:13

A. Are you referring to the specific title or when I had originally joined Notre Dame? 12:03:23

Q. Let's go with the second. When did you first join Notre Dame? 12:03:29

A. So I had joined Notre Dame in January of 2003, and then I believe I had become -- and I'll have to check my report to get the date right -- I had become a what's called a full professor in May of 2018. 12:03:33

Q. As part of your academic work, are you familiar with VLANs? 12:03:54

A. I am, more broadly not only from my academic work, but also from other experience as well. 12:04:03

Q. And I think if we go to Paragraph 109, so maybe the last two or three sentences, 12:04:12

talk about your familiarity with VLAN, and even having worked extensively on projects involving VLANs, right? 12:04:18 12:04:23 12:04:27

A. I believe in this paragraph I do discuss that I'm familiar with particular network components, that include VLANs, something called ACLs, routers, firewalls, and switches, and then I continue with additional discussions beyond that. 12:04:27 12:04:42 12:04:43 12:04:48 12:04:50 12:04:54

Q. When you say you have extensively worked on projects involving VLANs, what kind of work are you discussing there? 12:04:55 12:04:56 12:05:00

A. So I'm discussing here, I had done work -- to get the timeline about right, it would have been circa, I'd like to say, 2002, I had done some work as part of Sun Microsystems working with -- this would have been what was called Project Neon, was looking at a rough, I guess equivalent at the time, something called software defined networking, and looking at was network processors, and as part of that work, it involved working with VLANs. 12:05:01 12:05:13 12:05:17 12:05:26 12:05:28 12:05:36 12:05:38 12:05:41 12:05:47 12:05:50

And then beyond that, my research group, which I direct, has also done a fair amount of work in term of looking at the 12:05:52 12:05:54 12:06:01

interplay of firewalls, VLANs, and routers in terms of enterprise network management. 12:06:02 12:06:05

Q. Is it fair to say, then, that VLANs, the concept, already existed prior to when you started working with it in 2002? 12:06:08 12:06:10 12:06:13

A. I would have to go through and look up the exact dates when VLANs had emerged from the standards. But the notion of trying to construct virtual LANs, I believe, would have existed, at least, conceptually. I don't recall the exact date for the particular VLAN standards and drafts. 12:06:23 12:06:25 12:06:28 12:06:32 12:06:38 12:06:42 12:06:44

Q. You mentioned a VLAN standard. What organization, I suppose, is in charge of the VLAN standard? 12:06:50 12:06:52 12:06:54

A. That's a little bit of a complicated question. So if we look at what might govern how VLANs might operate, we'll see, in particular, IEEE, when we're talking about things such as standards, and then we'll see various modifications and discussions on use cases with an organization typically called IETF, which would be the Internet Engineering Task Force. 12:06:55 12:06:56 12:07:06 12:07:08 12:07:12 12:07:14 12:07:20 12:07:25 12:07:27

So we might see various documents 12:07:30

looking at the interplay of VLAN, which is typically kind of a layer to centric focus, and there will be various interplay between, say, like a VLAN versus various label switching. 12:07:32 12:07:35 12:07:38 12:07:41

We'll see also there will be documentation as well with regards to 3GPP, which is one of the organizations, and its precursor, looking at the interplay of VLANs and cellular. 12:07:44 12:07:46 12:07:52 12:07:54 12:07:57

So there's a wide variety, which is why I say it's a little bit more complicated. 12:07:58 12:08:00 12:08:02

Q. In general terms to help guide our conversation, what do you understand "VLAN" to mean? 12:08:06 12:08:09 12:08:12

A. So in general terms, and in this case we're taking a very broad view in terms of what a VLAN is, VLAN stands for virtual LANs. It's a virtual local area network, which allows one effectively to logically partition a given LAN to basically be able to kind of deliver a particular separation. 12:08:12 12:08:15 12:08:18 12:08:26 12:08:29 12:08:42 12:08:43

In this case, if we think about, say, a physical set of connections versus a logical set of connections, much like the name 12:08:44 12:08:46 12:08:48

VLAN, it allows one to create logical partitions specifically geared towards LANs or local area networks.

Q. And when you mention "partitions," exactly what do you mean when you say "partitions"?

A. So when we talk about VLANs, and we talk about the notion of logical connections, when we talk about VLANs, one can set them up such that they are effectively partitioned.

There's a variety of techniques that one might use perhaps to transition between different VLANs, potentially involving, say, layer two or layer three when we talk about things like routers that might be involved, and there's a lot of different ways that one might use a VLAN to accomplish a variety of goals, and its usage has evolved considerably over time as we've seen the rise of the cloud and various data centers in terms of how a VLAN might be used in a variety of rules.

Q. So one of those ways if I understood that correctly, and tell me if I

didn't, is that you might have a network and it's partitioned into multiple VLAN segments; is that right? 12:10:11 12:10:13 12:10:16

MR. SCHWERIN: Object to form. 12:10:17

A. So a VLAN, as I had described earlier, could be used to logically separate or partition different networks, such that rather than everyone being part of the same LAN, would allow, say, across an enterprise or within a given switch, and again, it would depend on a particular configuration in how things are set up, to be able to effectively keep certain devices to certain parts of that while still having a single device or multiple devices. And as I had described earlier, the notion that it is effectively a virtual LAN, so a logical setup of this particular layer to network. 12:10:20 12:10:22 12:10:29 12:10:32 12:10:35 12:10:42 12:10:44 12:10:46 12:10:52 12:10:55 12:11:00 12:11:03 12:11:06

Q. When we discuss these partitions, is that the best phrase to use, would they be VLAN partitions? 12:11:17 12:11:19 12:11:22

A. I don't know if I would say partitions is perhaps the best way. Again, since we were speaking more generally, I was trying to describe it a bit more informally as opposed to the specific context in the report. 12:11:23 12:11:27 12:11:33 12:11:35 12:11:38

Generally if I were trying to teach, say, an undergraduate or something along those lines, that might be one way to kind of capture one of the particular pieces of functionality that you might use a VLAN for.

There are a variety of ways that you might use VLANs, so that's one way to kind of try to wrap your head around one of the kind of primary uses of a VLAN in terms of how might one, you would say within the context of, say, just to give it switch, and then from there one might build on how it might be used in an enterprise or a wide variety of other settings of which there are numerous different sort of configurations.

Q. When you have, let's say, two VLAN partitions, what distinguishes those partitions from each other?

A. So if I understand your question correctly, kind of going with the sort of informal partition, so operating on that kind of hypothetical or kind of more informal definition, there can be a variety of ways how you might configure it.

One way would be with regards to

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 301 of 1144
INFOEXPRESS, INC. - EX2572

how one might, say, tag a particular set of packets. How and where that tagging might take place can vary.

Again, VLANs can be used in a wide variety of ways. So depending upon how one might use VLANs, it could considerably vary. But one way might be through tags in terms of how one might try to, say, mark a packet.

That tagging, though, can have a wide variety of behaviors based on how one might configure or combine things together in, say, the LAN or if we get into specialized use cases, things like cellular or other places, data centers, it can often get a bit more complicated, but that's one kind of basic way.

Q. A term that I think gets used in your report at different points is the term "subset."

Are you familiar with that?

A. I am familiar with the term "subset."

Q. Is there such a thing as a VLAN subset?

A. Thinking about that, what's the context for that?

Q. I guess I'm just trying to understand whether -- we've discussed somewhat partitions and how you can use VLANs to partitions. I'm trying to understand if that's the same or similar context to having subsets for the network. 12:14:17 12:14:18 12:14:23 12:14:25 12:14:27 12:14:35

A. So the notion of a VLAN subset would largely depend upon the context on which one might view it. 12:14:35 12:14:40 12:14:42

Again, as I described earlier, there's many different ways that one might be able to apply VLANs in a network. And so, again, depending upon how, say, a given switch or how -- whether you're doing kind of layer two or layer three, there's kind of different ways conceptually that one might be able to combine things in the network. 12:14:45 12:14:48 12:14:51 12:14:55 12:14:58 12:15:02 12:15:05 12:15:12

So I don't know if I would say specifically that a VLAN subset would come to mind, but -- in terms of a general case. But the notion of depending upon how you might configure a VLAN, you could use it to try to deliver a subset or other ways. 12:15:13 12:15:16 12:15:23 12:15:27 12:15:30 12:15:32

Again, it depends upon how one might configure the VLAN itself. 12:15:35 12:15:38

Q. I see. So then, is it fair to say you can use a VLAN to define subsets of a network? 12:15:40 12:15:46 12:15:49

MR. SCHWERIN: Object to form. 12:15:50

A. So if I -- asking with regards to, say, using a VLAN to define a subset, again, it would depend upon how you're using the VLAN. But the nominal notion -- and again, we're talking about VLANs in general as opposed to a specific kind of window or context, by virtue of using a VLAN to choose which devices might be part of which logical network, that could potentially be viewed as a subset. 12:15:53 12:15:58 12:16:04 12:16:07 12:16:10 12:16:15 12:16:23 12:16:27 12:16:30

But again, it would depend upon how you might use it with regards to, say, like your layer two information or your layer three information, and kind of the broader logical construct one might bring to bear on, say, an enterprise network or other types of networks. 12:16:33 12:16:35 12:16:39 12:16:42 12:16:45 12:16:48

Q. If you could, let's turn to Page 18 in your report. Let me know when you're there. 12:16:51 12:17:00 12:17:02

A. Okay. 12:17:15

Q. There's a figure, Figure 2, sort of in the middle of the page. Do you see that? 12:17:16 12:17:18

A. I do see that. 12:17:19

Q. You're familiar with this figure, right? 12:17:20 12:17:21

A. I am. 12:17:21

Q. At the top of the page it says, "In some embodiments the less-restricted subset and the restricted subset are characterized by VLANs defined within the protected network." 12:17:26 12:17:29 12:17:33 12:17:36

Do you see that? 12:17:39

A. I do see that. 12:17:40

Q. When you use "subset" there, what do you mean? 12:17:46 12:17:49

A. In this case, I'm citing directly to the patent specification itself. As I can see at the end of the line, I see a mention of Column 5, 48 to 50, and the terms "less restricted subset" and "restricted subset" do appear throughout the specification. 12:17:49 12:17:58 12:18:02 12:18:04 12:18:09 12:18:12

Q. And you say that they are "characterized by VLANs." 12:18:13 12:18:15

Do you see that? 12:18:17

A. I do see where I use the term "characterized by VLANs." 12:18:18 12:18:21

Q. What did you mean when you wrote "characterized by VLANs" in that sentence? 12:18:24 12:18:26

A. So in this case, I'm directly citing from the specification as I list there. I can also see the same text reflected in the '484 patent on lines 48 to 50.

Q. I know the quotation marks aren't there, but you're saying this is a quote?

A. So if I read the patent, and this being the '484 patent, I see the text and some embodiments, the "less restricted subset" and the "restricted subset" are characterized by VLANs defined within the protected network.

Q. So what do you understand it to mean for the subset to be characterized by VLANs?

A. So this is describing here in some embodiments, so it's describing some of the embodiments from the patent, and one of the ways that one can try to configure the network to be able to provide a delineation, and we talked before the notion of partitioning a delineation between, say, a less restricted subset versus a restricted subset, would be to use a VLAN to perhaps put one set of devices on one VLAN or a different set of devices on another VLAN, with the caveat being that,

again, depending upon how you might configure the network, multiple levels of VLANs could be involved, as well as other aspects as well.

Q. Being able to define those subsets using VLANs, is that similar to the partitioning discussion we were just having about VLANs?

MR. SCHWERIN: Object to form.

A. Sorry, I think we had just talked about that a little bit earlier. The notion of being able to use a VLAN to try to make logical, say, constructs inside of a LAN is one of the types of functionality that a VLAN would offer.

Q. And would it be fair to say that that's something that the VLAN offered when you were first working with it back in 2002?

A. The notion -- going back to 2002, and again, working a little bit from memory on this, the notion of a VLAN, nominally speaking, is to try to logically group or try to rate, one might view the term perhaps as a subset or trying to create that separation, potentially between different aspects of a LAN.

Again, with the key caveat being

that in 2002, when we had looked at it, we had used it for a variety of roles in terms of what you might -- how you might choose to use a specific VLAN or even how one might try to combine VLANs to offer different types of functionality. 12:22:25 12:22:28 12:22:33 12:22:36 12:22:40 12:22:43

There's a lot of different things you can do, depending upon your vantage point in the network and where you might be trying to adapt in the blend of, say, smarter or more capable devices versus, say, less capable devices, and how you might construct your -- whether it's an enterprise network or other type of network, say, like a wireless network, it will all depend on how you might try to combine them. 12:22:46 12:22:48 12:22:51 12:22:54 12:22:57 12:23:00 12:23:04 12:23:07 12:23:10 12:23:13

Q. And when you would configure VLANs in that way, would it have been understood that you could configure the VLANs such that the devices might have access to one VLAN, but not another? 12:23:13 12:23:17 12:23:20 12:23:24 12:23:27

A. So it would depend, if I'm understanding your question correctly, depending upon what the goal for that configuration of a VLAN might be, again, when 12:23:27 12:23:38 12:23:40 12:23:45

we start looking at multiple devices and how we might combine them, there could be a variety of ways that one might choose to use VLANs to, say, perhaps offer kind of a quasi redirection where you might try to, say, send traffic along additional inspection. 12:23:48 12:23:52 12:23:55 12:23:58 12:24:06 12:24:09

Other ways that you might combine it, depending upon how you might, say, use strictly the VLAN or the VLAN, plus other functionality, depending upon the overarching security kind of policy or overall broadly kind of security stance that you would like to apply to the organization, so the answer would be more so, it depends on what you're trying to deliver. 12:24:11 12:24:14 12:24:17 12:24:20 12:24:25 12:24:28 12:24:30 12:24:34 12:24:36

Q. Could we go to Paragraph 42. 12:24:40

There's a section where you're describing the asserted patents, you say that, "Prior to the invention, several approaches to controlling external users' access to protected computing networks were known." 12:24:52 12:24:54 12:24:54 12:24:56 12:24:59

Do you see that? 12:25:00

A. I do see that. 12:25:01

Q. Is it your understanding that it was known at that time that one thing you could 12:25:02 12:25:07

do was use VLANs to segment access to a network? 12:25:08 12:25:13

MR. SCHWERIN: Object to form. 12:25:14

A. So in this case, I believe I'm citing to the specification that's, say, included in the patent, and the patent had noted in this case several different approaches, which are discussed later in that particular paragraph. I believe I mention most of them in my paragraph there. 12:25:15 12:25:19 12:25:22 12:25:24 12:25:26 12:25:28 12:25:34

Q. So your statement in 42 is strictly based on what you found in the patent and not your personal or professional experience? 12:25:35 12:25:38 12:25:41 12:25:43

A. I believe in this part of my report I'm presenting a broader overview of the patents themselves, and in this case I felt it important to describe what was discussed inside of the specification itself and what the asserted patents, given their common specification, were describing in terms of prior art or aspects prior to the invention. 12:25:43 12:25:54 12:25:56 12:25:59 12:26:00 12:26:05 12:26:07 12:26:12

Q. Is your education and experience consistent with that statement? 12:26:17 12:26:20

A. The statement in particular with 12:26:21

regards to "Prior to the invention, several approaches to controlling external users' access to protected computing networks were known," yes, I would say that was -- would comport with my education.

Q. And you had worked extensively with VLANs, right? We discussed that, I think.

A. We had discussed that earlier, and we had discussed it in a broad sense, and I talked about work that I had done, not only in 2002, but also some of the later work as well that my research group had done.

Q. So before the invention, were you aware of any approaches using VLAN that would control an external user's access to protected computer networks?

A. Is there a specific spot in my report that you're trying to point me to, Counsel? I'm not sure. The question seems a little broad, so I want to make sure.

Q. Yes, it's -- sorry, I didn't mean to cut you off.

A. I wanted to make sure we're staying in line with what I had done in my report.

Q. Absolutely. So Paragraph 42, in the first sentence, you say that there's several approaches prior to the invention, and you mentioned, of course, the ones that the patent specifically describes. 12:27:43 12:27:46 12:27:53 12:27:55 12:27:56

My question to you is, are you aware of any others? 12:27:58 12:27:59

A. Without going through and conducting a detailed review of the literature, I don't know if I would feel comfortable riffing on that in terms of thinking back to that. 12:28:00 12:28:07 12:28:11 12:28:15 12:28:19

I do discuss in this report what had been outlined in the patent and specification in terms of what the patent had described as other methods, and I felt those comported with my knowledge. 12:28:19 12:28:23 12:28:25 12:28:30 12:28:34

Q. But at least as we sit here right now, none come to mind that we can discuss? 12:28:35 12:28:38

A. I don't believe I opined on that in my report. 12:28:40 12:28:43

Q. So your report is, then, strictly limited to the citation -- for this Paragraph 42, strictly limited to the citation to the specification; is that right? 12:28:44 12:28:49 12:28:55 12:28:58

MR. SCHWERIN: Object to form. 12:29:02

A. I'm not sure I would agree to that, because I'm not sure what you're saying in terms of what is being limited. 12:29:04 12:29:06 12:29:07

Q. Well, what I'm asking is, it says here that "several approaches to controlling external users' access to protected computer networks were known." You cite the specification. 12:29:08 12:29:11 12:29:13 12:29:16 12:29:18

Aside from those that you discuss from the specification, are you aware of any others? 12:29:22 12:29:24 12:29:26

A. I'm not quite sure where your question is coming from, Counsel, because I was asked to opine in this case with regards to claim construction as opposed to conducting a broad literature survey with regards to prior art. So I used the materials that I had been provided as well to arrive at my opinion. 12:29:35 12:29:39 12:29:41 12:29:42 12:29:46 12:29:48 12:29:53

So I'm not sure I would have a specific opinion on that, nor was that necessarily part of my assignment. 12:30:01 12:30:03 12:30:05

So I wouldn't say I have a specific opinion on that, but I would be a bit more cautious in saying in terms of what it was 12:30:06 12:30:08 12:30:11

limited to, because I'm not quite sure whether I'm agreeing to say that it's being limited to.

Q. I see. If we go down in this Paragraph 42, right towards the end of Page 15, "A greater level of access control could be achieved by including a gatekeeper between the secure network and access device."

Do you see that?

A. I do see that at the bottom of Page 15, going on to Page 16.

Q. In this context when you say "a greater level of access control," what do you mean?

A. In this case, much as we had described before, this is, again, referencing the specification, and I include a citation of the specification afterwards.

Q. So is this paragraph just summarizing to you what the specification says?

A. I believe in this case, in this particular part of my report, I'm talking about the asserted patents and providing an overview of the asserted patents and discussions of that specification as it would be relevant to later parts of my report.

Q. I see. I think that helps. So then let me clarify so I can understand what the scope of your opinion is. 12:31:43 12:31:47 12:31:50

At the beginning of 42, we talked about "Prior to the invention, several approaches to controlling external users' access to protected computing networks were known," right? 12:31:51 12:31:53 12:31:55 12:31:58 12:32:00

A. We had discussed about that, yes. 12:32:01

Q. For this report, the entire basis for that statement is based on the specification; is that right? 12:32:05 12:32:09 12:32:10

A. I think I would more accurately state that as that in this case I'm citing to the specification, and describing that here, which would be relevant for the rest of my report. 12:32:14 12:32:29 12:32:31 12:32:32 12:32:34

So I don't know if I would say -- for this statement, I'm sharing that or basically citing that from the specification. 12:32:34 12:32:36 12:32:39

Q. And aside from that, do you have any other basis for that statement? 12:32:45 12:32:47

A. I believe in this case I'm citing to the specification to describe the asserted patents. Later in my report, as appropriate, 12:32:48 12:32:58 12:33:00

when discussing prior art, and the rationale or aspects of the patent, I appropriately discuss that.

But in this particular part of my report, I'm citing to the specification to appropriately discuss the asserted patents.

Q. Very similarly, the statement that "A greater level of access control could be achieved by including a gatekeeper between the secure network and the access device," you cite the specification.

Is the specification your only source for that statement?

A. In this case here, I'm restating what was contained in the specification. And then later in my report, I discuss things in the appropriate context with regards to prior art and terms as understood.

Q. You mention in the next sentence, "The gatekeeper could be configured to ensure that the access device conforms to a predetermined security policy."

Do you see that?

A. I do see that.

Q. What is your basis for that

statement? 12:34:24

A. I do see in this case, in the specification, the next line shortly thereafter, the specification includes, "The gatekeeper" is "configured to ensure that the access device conforms to a predetermined security policy." 12:34:24 12:34:36 12:34:39 12:34:43 12:34:45 12:34:48

So in this case, I probably should have added an additional citation for that as well. 12:34:50 12:34:52 12:34:55

Q. The next sentence discusses something that's referred to as an "'in-line' configuration." 12:34:55 12:34:59 12:35:02

Do you see that? 12:35:04

A. I do see that. 12:35:05

Q. What do you understand an in-line configuration to be in this context? 12:35:06 12:35:09

A. So as I mention in my report, in the next paragraph, there's a direct excerpt of Figure 1. 12:35:12 12:35:21 12:35:24

Figure 1 shows an example from the prior art which would have an in-line configuration where the gatekeeper could be directly in line. 12:35:25 12:35:33 12:35:36 12:35:39

Q. Before the priority date of the 12:35:46

asserted patents, is it your understanding that gatekeepers were always used in line? 12:35:48 12:35:53

A. I believe, when looking at this, is that this is -- the specification describes an in-line configuration. The term "gatekeeper" itself and its role, one way the patent specifically addresses, is that getting into what are the pitfalls or sort of drawbacks as part of the prior art for putting a gatekeeper and its specific role in an in-line configuration. 12:35:59 12:36:08 12:36:15 12:36:23 12:36:29 12:36:31 12:36:35 12:36:37 12:36:41

Q. I think you may have answered a slightly different question than I asked, so I'll try again. 12:36:42 12:36:45 12:36:47

Before the priority date of the asserted patents, is it your understanding that gatekeepers were always used in line? 12:36:48 12:36:51 12:36:53

A. Just to clarify, the patent describes the notion of what would happen if you try to put this type of gatekeeper functionality in line, describing that the patent itself, in terms of what the gatekeeper does, those outline specific functionality. But in terms of discussing the prior art, it mentions that looking at -- in 12:36:55 12:37:15 12:37:19 12:37:24 12:37:30 12:37:33 12:37:38 12:37:41

particular, talking about access control, as I described earlier, the notion of user names, passwords and Mac addresses, that trying to do that in line does not scale well.

Whereas, the patent describes its particular version of the gatekeeper, and the types of functionality that it brings and its components, it describes and articulates, then, how that would be -- how one would be able to deliver that type of functionality, not in an in-line configuration.

Q. So it's your understanding that before the invention of the asserted patents, a POSITA would have understood the ordinary meaning of "gatekeeper" to also include configurations that are not in line?

A. Could you repeat that question? I'm not sure I totally followed it.

Q. Sure, I can. So it's your understanding that before the invention of the asserted patents, a POSITA would have understood the ordinary meaning of "gatekeeper" to also include configurations that are not in-line?

A. No, I don't think so, because I

think the type of functionality described by the patent and how it operates, that is the core novelty, which is to -- necessarily it needs to be out of line or not in line, to be more precise, in order for it to operate. 12:39:16 12:39:20 12:39:23 12:39:30 12:39:33

Otherwise, as I've described in my report, the various drawbacks of having it in line made it extremely difficult to offer that type of functionality without a prohibitive cost. 12:39:36 12:39:38 12:39:44 12:39:47 12:39:51

And one of the key novelties or key thing that the patent teaches is how to do this out of band and how this configuration allows the type of functionality that's going to be offered, while still meeting the various security needs of the organization, and to do so in a way that is reasonable in terms of its cost and reasonable in terms of its approach to the various embodiments and the various claims that are articulated in the patents. 12:39:52 12:39:55 12:39:59 12:40:03 12:40:09 12:40:11 12:40:13 12:40:15 12:40:22 12:40:25

Q. If we go to Paragraph 45 you have a statement that says, "Using a single gatekeeper to support numerous access devices 160 was limited by bandwidth and required sophistication (e.g., cost) of the gatekeeper 12:40:27 12:40:54 12:40:57 12:41:02 12:41:06

110." 12:41:11

Do you see that? 12:41:11

A. I do see that. 12:41:12

Q. And you cite the specification for that. Do you see that? 12:41:13 12:41:14

A. I do. 12:41:14

Q. Besides the patent specification, do you have any basis for that statement? 12:41:16 12:41:18

A. So I do describe in this, in my citations to the specification, some of the drawbacks of these what are termed disadvantages. These do comport with my understanding in terms of when one is looking to try to offer the type of functionality described, that it would be difficult due to the cost and sophistication. 12:41:19 12:41:19 12:41:35 12:41:35 12:41:40 12:41:44 12:41:49 12:41:56

Getting back to earlier our discussions of some of the work that I had done as part of Sun Microsystems, I was very keenly aware of many of those limitations of trying to offer what one could kind of informally dub as higher level types of functionality, bringing in things such as users and the notion of policies can be difficult, particularly when we focus on, say, upper layer types of aspects, 12:41:59 12:42:01 12:42:03 12:42:07 12:42:10 12:42:13 12:42:16 12:42:20 12:42:25

getting into the cost, as the specification describes the sophistication that would need to be in place to try to deliver functionality as described more broadly for the gatekeeper. 12:42:29 12:42:33 12:42:35 12:42:39

Q. If we go to the next paragraph, 46, there's a statement at the beginning that says, "The asserted patents solved these shortcomings in the prior art by reconfiguring a communication port within the access point such that initial communication from an external access device could be passed to a restricted subset of the protected network." 12:42:50 12:42:52 12:42:52 12:42:56 12:42:57 12:43:00 12:43:03 12:43:07

Do you see that? 12:43:11

A. I do. 12:43:11

Q. So I want to break this up into a few parts and ask you about them since it's a little bit long. When you say "reconfiguring a communication port" here, what do you mean? 12:43:11 12:43:13 12:43:16 12:43:19

A. So in this case, much as we had described earlier, I'm citing this case as I note to the abstract, as well as to Column 5, lines 29 and 30. 12:43:21 12:43:23 12:43:26 12:43:30

Q. Do you have any understanding as a person of skill in the art of what it means to reconfigure a communication port? 12:43:31 12:43:34 12:43:35

A. Yes, I would. 12:43:44

Q. What would that be? 12:43:45

A. So as a person of ordinary skill, I would see -- I would be able to interpret what reconfiguring a communication port would mean. 12:43:45 12:43:49 12:43:51 12:43:55

Q. And what would you understand that to be? 12:43:55 12:43:57

A. So I believe that's also described later in my report as well with regards to that particular -- those particular claims that use that specific verbiage. 12:43:57 12:44:02 12:44:06 12:44:11

But speaking in this case, more informally, the patents itself describes the notion of reconfiguration within the access point. And the idea of this reconfiguration would be the gatekeeper through its respective module, then reconfiguring that access point. 12:44:14 12:44:17 12:44:23 12:44:28 12:44:33 12:44:36

Just as described in the specification and also described here, I, from a POSA, would be able to read that and understand what's going on, as well as reading that text, in turn, to know that, if we go later, talking about the notion of a restricted subset, and that also later in my report I talk 12:44:41 12:44:43 12:44:46 12:44:49 12:44:55 12:44:59 12:45:03

about the nuance of a less restricted subset versus a restricted subset as well.

Q. So when you talk about communication port in this context, what do you mean by "communication port"?

A. Well, in this case, from the communication port, one can draw from the patent specification itself, looking at the claim language.

For instance, later in my report, I talk a bit -- I discuss also Figure 3A, Figure 3B, which specifically mentions ports as well, and how those might be relevant in the context of the patent or the patents themselves.

Q. As a POSITA, what are the communication ports?

A. Well, so, I think we want to be careful that the report is opining specifically how the communication ports is being used in the context of the patent.

And in this case, it uses it -- we see it being used in Figure 3A, we see in Figure 3A nominally the notion of port 305A versus port 305B versus port 305C.

From that there could be a variety of meanings, though, that we want to be careful of, because the notion of a port, as it might be, say, like in a physical switch, if that were the access device in question, might have physical ports themselves. 12:46:38 12:46:39 12:46:41 12:46:43 12:46:46 12:46:49

If I have a wireless LAN, say, like in this case being a wireless access point, nominally there's the notion of sort of logical channels, if you will. 12:46:52 12:46:56 12:46:58 12:47:03

And getting back to our earlier discussion about partitioning and that being a bit of an informal term and what that means, in the context of, say, like a wireless sort of setup, it might also depend upon how you might apply encryption on that in terms of point to, say, the endpoint or the access point, say, is derived from an 802.1X session versus like a preshared key on that in terms of does it look more like a bus or does it look more like a port. So kind of the meaning on that. 12:47:06 12:47:07 12:47:09 12:47:15 12:47:17 12:47:22 12:47:25 12:47:28 12:47:34 12:47:37 12:47:40

A POSA would be able to understand in the appropriate context, on that I would read the specification and be able to understand when the patent talked about a 12:47:43 12:47:48 12:47:49 12:47:50

communication port, what was meant. 12:47:54

Q. So when we talked about VLANs earlier, you just alluded to that informal discussion about partitions. Can communication ports be used to define VLANs? 12:47:54 12:47:57 12:48:00 12:48:05

MR. SCHWERIN: Object to form. 12:48:08

A. I'm not sure I would use it in that specific phrase. 12:48:09 12:48:15

Q. What would be a better way to phrase that? 12:48:16 12:48:20

A. So I believe the phrase you used was could communication ports be used to define VLANs? 12:48:20 12:48:23 12:48:28

Typically one would define a VLAN and a particular port could be associated with a VLAN. A VLAN could also be associated exclusively with a device. 12:48:35 12:48:39 12:48:43 12:48:47

So it would depend upon the type of configuration and type of networks that might be going on in that particular application. 12:48:51 12:48:53 12:48:55 12:48:59

So as much as the patent shows in terms of the specification showing a VLAN associated with the port or a port being associated with a VLAN, a similar kind of 12:49:01 12:49:03 12:49:07 12:49:08

relationship would exist as well. 12:49:15

Q. I see. So an individual port could be associated with a VLAN; is that right? 12:49:16 12:49:18

A. There's one configuration where one could have a port that might be associated with a VLAN. 12:49:23 12:49:27 12:49:30

There's other configurations as well in terms of how you might use a VLAN where, depending upon, say, the hierarchy of switches and how you might have your network set up, that a port could actually receive traffic from multiple VLANs. 12:49:32 12:49:34 12:49:37 12:49:43 12:49:45 12:49:50

And then there's further kind of more complex arrangements where you might have things like aggregated ports and other aspects, which also get far more complicated in terms of VLANs and routing and resiliency and robustness. 12:49:53 12:49:55 12:49:57 12:50:00 12:50:02 12:50:06

Q. Understood. Okay. So if you have, let's say, two VLANs, you could have a port that's associated with the first VLAN, but that port could be reconfigured to be associated with the second VLAN; is that fair? 12:50:08 12:50:10 12:50:14 12:50:17 12:50:19

A. So in a very broad sense, saying that a port is associated with a VLAN, and then 12:50:21 12:50:28

later on it would be reconfigured, then, to be associated with a second VLAN, that's one of the particular discussions that the patent has. I believe that's articulated, if we look at, say, like Figure 3A and 3B, it shows a specific reconfiguration of a port and a change from one VLAN to a different VLAN. 12:50:30 12:50:40 12:50:42 12:50:44 12:50:48 12:50:55 12:50:58

Q. And would that have been true at the time you were doing your work with Oracle back in 2002? 12:51:00 12:51:01 12:51:03

MR. SCHWERIN: Object to form. 12:51:08

A. So to clarify that, this would be now Oracle, formerly Sun Microsystems, which would have been acquired by Oracle. I think at the time everyone's stock pricing would have wished they were acquired sooner, based on some of the folks I was working with. 12:51:08 12:51:13 12:51:19 12:51:22 12:51:26 12:51:31

But the notion of setting a port to be associated with a VLAN at the time could have been done through various management interfaces, which could have been associated with directly logging into the device itself and accomplishing those goals as part of the configuration directly. 12:51:32 12:51:35 12:51:43 12:51:49 12:51:52 12:51:56 12:52:01

On the device one might use, say, 12:52:04

protocols, such as something like a Telnet or at the time things like SSH, to be able to deliver or to directly on the switch or the router itself to try to manipulate it, there would have been mechanisms that would have been part of that particular management to interface that one could use with regards to a VLAN to try to choose which parts go which -- I guess you could say, kind of which port might be associated with a given VLAN at the time.

We also see that reflected in the patent where the patent talks about the notion of reconfiguring those VLANs to the gatekeeper and the appropriate module that's associated with the gatekeeper to do that.

Q. That may have been something you had to do manually through that process you were talking about?

A. In terms of the time looking at when I was at -- doing the work for Sun, I would have had to look at the exact -- it's a little hazy on the exact mechanisms we were using.

We also had network processors, which were a little bit of a different kind of

a beast at the time, if you will, and the types of interfaces, whether or not they were open at the time. 12:53:25 12:53:33 12:53:36

Q. So let's go to Paragraph 50, if you would. That's right under the heading that says "Gatekeeper." Just let me know when you're there. 12:53:36 12:53:43 12:53:45 12:53:47

A. This is Page 19, Counsel? 12:53:56

Q. Page 19, yes. Do you see that? 12:53:58

A. I do see that. 12:53:58

Q. The very first sentence in Paragraph 50 says, "In my opinion, a POSITA would understand the claim scope for the term 'gatekeeper' with reasonable certainty, and would afford it plain and ordinary meaning." Do you see that? 12:54:00 12:54:00 12:54:01 12:54:06 12:54:07 12:54:10

A. I do see that. 12:54:11

Q. Is that still your opinion? 12:54:12

A. That is still my opinion, yes. 12:54:13

Q. Is it your opinion that "gatekeeper" was a known term in the art before the asserted patents were filed? 12:54:14 12:54:20 12:54:23

A. So the term "gatekeeper," as I described in my report, had been used both with regards to what the patent had described, as 12:54:26 12:54:36 12:54:38

well as I describe later, I believe, one of the particular references that was contained within the prosecution history.

I discuss a bit later the notion of gatekeeper and kind of how it has been used in a couple of the literature pieces at the time in terms of kind of mental models, if you will, in terms of describing that.

But in terms of a POSITA understanding that is they would be able to read the specification and read the claims and understand what the scope of the term "gatekeeper" would mean.

Q. So I'm going to reask that, because I'm not sure I got an answer to my question, which was, is it your opinion that "gatekeeper" was a known term in the art before the asserted patents were filed?

MR. SCHWERIN: Object to form.

A. So in this case, you know, as I had described earlier, I would stand by my previous answers. I do think it answered your question in terms of the extent to which gatekeeper would be known.

Q. So it is your opinion that it was

a known term in the art, right? 12:55:57

MR. SCHWERIN: Same objection. 12:55:59

A. So as I describe in here in my report, as I say that a POSITA would understand the claim scope, which I think is important for the purposes of the specification in terms of by reading the specification and reading the claims that a POSITA would be able to know what was covered -- what did "gatekeeper" mean and it's articulated in the specification and its respective documentation as well in terms of what a gatekeeper does. 12:56:00 12:56:04 12:56:08 12:56:13 12:56:15 12:56:17 12:56:22 12:56:25 12:56:28 12:56:30

Q. So I'm going to try one more time anyway. 12:56:31 12:56:40

When the specification -- when the application that became the asserted patents was filed, do you have any understanding of whether the term "gatekeeper" was a known term in the art at that time? 12:56:42 12:56:44 12:56:46 12:56:49 12:56:53

MR. SCHWERIN: Same objection. 12:56:55

A. I think I had answered your question again, Counsel, and I include in my report where I had seen "gatekeeper" used in terms of other pieces of the literature, as well as other extrinsic pieces as well, that a 12:56:56 12:57:02 12:57:05 12:57:09 12:57:14

POSITA would be able to understand within the specification what's meant by a gatekeeper. 12:57:18 12:57:22

MR. LOGAN: Objection. 12:57:27

Nonresponsive. 12:57:28

Q. Do you think that "gatekeeper" is used in the patent in a unique way that's different than how it was used in the art beforehand? 12:57:28 12:57:34 12:57:40 12:57:41

MR. SCHWERIN: Object to form. 12:57:44

A. Well, as I described in my report, and as I -- as the patent specification goes into, it describes the notion of a prior art gatekeeper being in line for the types of functionality that would be delivered, as articulated for a gatekeeper. 12:57:52 12:57:53 12:57:57 12:58:00 12:58:06 12:58:09

So in that case, I don't know if I would necessarily agree with saying -- with your definition as provided as saying that it was uniquely used for this patent, but again, that a POSITA would be able to understand and grasp what is meant by the gatekeeper by reading the specification and understand its scope, again, through what's contained in there, and their understanding of its placement, its particular role and functions. 12:58:11 12:58:14 12:58:18 12:58:22 12:58:27 12:58:29 12:58:32 12:58:35 12:58:36 12:58:39

Q. At the end of this paragraph you say, "As I understand the intrinsic evidence, the gatekeeper in reference here refers to its application with the claimed technology space for protected networks and controlling access thereto." 12:58:43 12:58:46 12:58:48 12:58:51 12:58:53 12:58:56

Do you see that? 12:58:58

A. I do. 12:58:59

Q. When you say "its application with the claimed technology space," what do you mean by that? 12:59:07 12:59:09 12:59:10

A. As I describe later in that same sentence, I talk about the claimed technology space for protected networks and controlling access thereto. So I believe that's reasonably explanatory in terms of what the application is for the gatekeeper. 12:59:11 12:59:18 12:59:20 12:59:22 12:59:27 12:59:31

Q. And if I understand that correctly, what you're saying is that you understand gatekeeper to be given its meaning in this sense within the technology space for protected networks and controlling access to them; is that fair? 12:59:32 12:59:35 12:59:39 12:59:43 12:59:46 12:59:50

MR. SCHWERIN: Object to form. 12:59:52

A. So I believe, as I described in my 12:59:53

sentence here, that this is -- its application in this particular space, and that particular space being with regards to particular network controlling access in a broad sense, but then there's also what's actually described in the specification, as well as what are the types of, when we get into protected networks and what it means to control access and how that access is controlled and what it's derived from. 12:59:57 13:00:04 13:00:06 13:00:09 13:00:12 13:00:14 13:00:17 13:00:22 13:00:24 13:00:27

Q. So you didn't apply the meaning of "gatekeeper" in any other context like, let's say, telephony, right? 13:00:27 13:00:29 13:00:33

A. I'm not sure what you're getting at with saying telephony. 13:00:36 13:00:38

Q. Do you understand what telephony is? 13:00:41 13:00:47

A. I do. 13:00:47

Q. Do you know whether "gatekeeper" as used in the context of telephony? 13:00:48 13:00:53

MR. SCHWERIN: Object to form. 13:00:57

A. So I think we want to be a little careful. You mentioned telephony. Telephony often involves a network, networking -- telephony networks would be something that one 13:00:59 13:01:01 13:01:05 13:01:11

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 335 of 1144
INFOEXPRESS, INC. - EX2572

would like to protect, hence my confusion with regards to asking broadly about telephony. 13:01:13 13:01:15

Q. So that helps tremendously. Thank you. So when you say "protected networks" here, what do you mean by that? 13:01:18 13:01:24 13:01:27

A. So in this case, when referring to protected networks, this is getting to the broader goal of trying to -- where you have a particular network that has perhaps sensitive or perhaps information or perhaps services that one does not want to expose to everyone, how can one go about restricting access or protecting that particular network, just as I described here, the notion of a protected network, something that I wish to protect or defend, if you will on that. 13:01:29 13:01:30 13:01:34 13:01:38 13:01:41 13:01:45 13:01:50 13:01:54 13:01:57 13:02:01 13:02:03

And then how should access be controlled to ensure that that network is appropriately protected, which, in turn, is subject to the broader organizational policies that would be in place that I'm trying to -- the gatekeeper is one of the tools that I might use to try to deliver this overall body of protection. 13:02:07 13:02:10 13:02:12 13:02:15 13:02:18 13:02:23 13:02:25 13:02:29

Q. So a protected network is not 13:02:29

necessarily a computer network, right? 13:02:32

MR. SCHWERIN: Object to form. 13:02:41

A. I think one needs to be really careful on that, because one can view a computer network versus, say, if we say something like a voice network, I think getting the -- what type of network might be involved, and the fact that oftentimes if we look at, say, like a pure voice network or other networks, that they also have computers as well. 13:02:42 13:02:47 13:02:49 13:02:53 13:02:55 13:02:59 13:03:02 13:03:04 13:03:04

And they, in turn, may be also utilizing data and many of the same protocols if we're looking at something like, say, a VOIP or other types of videoconferencing which may traverse a similar kind of network, so I think one wants to be careful in terms of what that means. 13:03:08 13:03:11 13:03:15 13:03:20 13:03:23 13:03:26 13:03:29

Q. So when you say "protected networks" here, you mean computer networks; is that fair? 13:03:29 13:03:31 13:03:34

A. So in the sense that I'm describing and noting the application where we have access devices and we have routers and access points, which would often be viewed as 13:03:35 13:03:45 13:03:48 13:03:51

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 337 of 1144
INFOEXPRESS, INC. - EX2572

protected, one could view that as being a network that one wanted to protect, to that extent, generally, informally one might view it as being a computer network. But as I described earlier, it would also be subject to the many devices. 13:03:55 13:03:58 13:04:03 13:04:08 13:04:10 13:04:13

In particular, if we looked at, say, that timeframe, often were -- involved computational devices that might have delivered other services that could have been, say, like a pure telephony network that might be, say, more circuit switched or things along those lines where you had like the PSTN, public switch telephone network, and we're looking at, say, pure telephony, even at that time there had already been transitions over to more kind of a VOIP or SIP type of arrangement where one had devices as well that were delivering, say, like other services, but also were necessarily using that same computer network as well that one would want to protect. 13:04:16 13:04:18 13:04:22 13:04:25 13:04:28 13:04:36 13:04:38 13:04:41 13:04:44 13:04:46 13:04:47 13:04:53 13:04:55 13:04:57 13:05:03

Q. So a protected network may be, but is not necessarily a computer network; fair? 13:05:04 13:05:12

A. So I think I would scope appropriately to say that it would be a network 13:05:14 13:05:26

that generally has computing devices that were connecting as described, again, in the specification and the notion nominally connected by a LAN or other types of -- in this case what's dubbed the access points and the routers.

So networks that would necessarily be governed by those devices.

Q. And networks that would be governed by those devices, those would be computer networks, right?

MR. SCHWERIN: Objection. That's been asked and answered.

A. So networks that would be governed by those devices or would be protected, I guess -- scratch that.

There would be a network that would be composed of devices, such as routers and access points that would provide the connectivity between the respective end devices, some of those being access devices, others being, say, other types of devices that are described also in the specification, in a broad sense one would view that as potentially a computer network.

But I wanted to be careful that many devices have computation and are connected to that network using typical network protocols that we would associate, say, with like a LAN.

Q. So it depends?

A. I would say, yes, it depends as the systems faculty that would depend upon the configuration. But as I described here, there's a network that I wish to protect, which is a LAN, and that's the application space, if you will, where the gatekeeper would be applied as one of the elements of the security solution.

Q. If we go to the next paragraph, which is Paragraph 51, the first sentence, the end of it says, "that it could refer to a device that would assist in determining whether an endpoint (that is, an 'Access Device') complied with a security policy, before granting that endpoint access to network resources."

Do you see that?

A. I do see that.

Q. Do you understand that to comport with your understanding of what a gatekeeper

is? 13:08:01

A. Well, in this case, as I describe is that it could refer to that device that would assist with determining whether an endpoint complied with a security policy, just as I state in my report. 13:08:01 13:08:15 13:08:17 13:08:18 13:08:21

Q. So it could include that, but not necessarily; is that fair? 13:08:23 13:08:25

MR. SCHWERIN: Object to form. 13:08:32

A. Well, I believe that the term "gatekeeper" could refer to that. In a general sense, if we're looking at the particular application space, protected networks, and reading the specification, one would be able to ascertain, again, what is the scope of the gatekeeper as used in the specification, drawing on one's knowledge as a POSA. 13:08:33 13:08:44 13:08:47 13:08:49 13:08:53 13:08:55 13:08:58 13:09:01

Q. I guess I'm just trying to make sure I understand your opinion since you used the word "could." So my question to you is, is that definitional or is that just something that the gatekeeper could be? 13:09:09 13:09:11 13:09:13 13:09:17 13:09:19

A. I think it's important when one looks at that to read the specification, what a POSA would understand in reading that 13:09:20 13:10:00 13:10:02

specification.

I do describe later in my report where the term "gatekeeper" had been used in extrinsic parts in terms of understanding it is sort of a mental model of what a gatekeeper, what its role might be.

But in reading, in terms of reading the specification, and understanding the invention, it's my opinion that a POSA would know with reasonable certainty what a gatekeeper is by reading the specification, and also in the claim language itself.

MR. LOGAN: Objection.

Nonresponsive.

Q. So I understand your more general opinion, and actually your conclusion about gatekeeper. I'm just really trying to ask you questions about the basis for that opinion.

Here what I'd really like to know is, it says it could refer. And all I want to know from you, my question is very simple, is does it necessarily refer to that or is that just something it could be?

A. I think I've -- I think I've answered your question, though, Counsel. As I

described in my report, I described on here, both I walked through how it's used in the specification, how a POSA would interpret it. 13:11:21 13:11:26 13:11:28

I also cite later on several other pieces of intrinsic evidence in terms of things that were considered during the prosecution history, I discuss several of the other patents that talk about gatekeepers. 13:11:31 13:11:34 13:11:37 13:11:40 13:11:43

And then later on I also mention several other extrinsic pieces of evidence that a POSA would be able to arrive at what a gatekeeper would be or what its role would be, and it would appropriately -- a POSA would be able to read the specification and understand the scope and what a gatekeeper is trying to do. 13:11:49 13:11:51 13:11:53 13:11:58 13:12:00 13:12:03 13:12:05 13:12:08

We had had a long discussion earlier with regards to what was the prior art gatekeeper versus what the gatekeeper as proposed in the invention would do. 13:12:09 13:12:11 13:12:13 13:12:16

It's my opinion that a POSA would see the term "gatekeeper" and be able to then, with the specification, to understand, you know, what is a -- what is the gatekeeper doing and how is the gatekeeper used. 13:12:18 13:12:20 13:12:23 13:12:26 13:12:29

MR. LOGAN: Objection. 13:12:34
Nonresponsive. 13:12:35
Q. So I'm going to try again. My 13:12:35
question to you is, you have a statement in 13:12:40
your report that I've shown you, Paragraph 51, 13:12:41
first sentence, that explains that a gatekeeper 13:12:46
could refer to a device that would assist in 13:12:49
determining whether an endpoint, that is an 13:12:52
access device, complied with the security 13:12:54
policy before granting that endpoint access to 13:12:56
network resources. 13:13:01
My question to you is, must that 13:13:02
necessarily be the case or is that just an 13:13:05
example? 13:13:07
MR. SCHWERIN: Object to form. 13:13:11
A. I guess I'm not parsing the nuance 13:13:12
you're trying to get at, Counsel, with regards 13:13:20
to your question. I'm not totally following. 13:13:22
Q. Well, let me is it this way. Why 13:13:25
did you use the word "could"? 13:13:29
A. To go back to what I had described 13:13:31
earlier, as I describe in my report, I do talk 13:13:41
about here is how the patent describes the 13:13:46
gatekeeper and the type of functionality, and 13:13:52
then I walked through several of the other 13:13:53

cited pieces that were in the prosecution history in terms of how they had used "gatekeeper."

Then later on, I described -- cited several pieces in the extrinsic evidence that had also used the term "gatekeeper" as well.

I would stand by my opinion that a POSA would be able to know that with reasonable certainty by reading the specification, the plain language, and understand what is the scope of the gatekeeper on that, and I used the term "could" specifically to highlight later on when we see the gatekeeper described in various other pieces of the literature.

Q. So is it your opinion that a gatekeeper necessarily refers to a device that would assist in determining whether an endpoint, that is an access device, complied with the security policy before granting that endpoint access to network resources; yes or no?

MR. SCHWERIN: Object to form.

A. Are you asking in the context of the patent itself, because given the

specification, as I described earlier, a POSA would be able to read that, understand the specification, and know what it means with reasonable certainty, just as I wrote in my report. 13:15:04 13:15:08 13:15:14 13:15:16 13:15:19

MR. LOGAN: Objection. Nonresponsive. 13:15:19 13:15:20

Q. I appreciate that you keep giving me the conclusion, but I'm actually asking about the analysis you provided. You say right here, "a gatekeeper was both known with reasonable certainty," and you say it could refer to something. 13:15:21 13:15:22 13:15:25 13:15:27 13:15:30 13:15:33

I'm just wanting to know whether that's a example of what a gatekeeper could be or if you're saying that's what a gatekeeper is. It's actually a real simple question. Will you please let me know what your opinion is? 13:15:34 13:15:36 13:15:38 13:15:40 13:15:45 13:15:47

MR. SCHWERIN: Same objection. 13:15:47

A. As I described earlier, I think I've answered your question, Counsel. 13:15:55 13:15:57

MR. LOGAN: Objection. Nonresponsive. 13:15:58 13:15:59

Q. I'll try one more time and then 13:15:59

we'll put this one on a list of things that maybe we can get an answer to later. 13:16:02 13:16:04

You have a statement in Paragraph 51 at the beginning that says what a gatekeeper could refer to. I've asked you multiple times. I don't feel I've been able to get a direct answer. 13:16:06 13:16:08 13:16:10 13:16:14 13:16:16

I would just like to know whether that is your opinion of what a gatekeeper is or if it is just an example of what a gatekeeper could be? 13:16:17 13:16:18 13:16:21 13:16:23

Would you please give me an answer to that question? 13:16:26 13:16:29

MR. SCHWERIN: Object to form. 13:16:29

A. Counsel, I think I've answered the question again, and I -- yeah, I think I've answered the question. 13:16:30 13:16:33 13:16:40

MR. LOGAN: Objection. 13:16:41

Nonresponsive. 13:16:41

Q. Let's move along to Paragraph 53. 13:16:44

A. Counsel, I don't mean to interject, but since we have been going over an hour, I don't know if this would be a good time for taking a break. 13:16:48 13:16:50 13:16:53 13:16:55

Q. Oh, sure, I'm happy to take a 13:16:57

break. Five minutes okay? Ten minutes? What do you need? 13:17:00 13:17:03

A. I think five is fine. 13:17:03

Q. Okay. Sounds great. Let's do that. 13:17:06 13:17:09

THE VIDEOGRAPHER: Off the record at 1:17 p.m. 13:17:10 13:17:10

(Recess taken at 1:17 p.m. and reconvening at 1:29 p.m.) 13:17:12 13:17:15

THE VIDEOGRAPHER: Back on the record at 1:29 p.m. 13:29:03 13:29:04

BY MR. LOGAN: 13:29:07

Q. Dr. Striegel, I know we're coming back from a break. I just wanted to ask, is there any of your prior testimony that you would like to go back and address? 13:29:07 13:29:14 13:29:18 13:29:20

A. Not as far as I know right now. 13:29:21

Q. During the break did you confer with your counsel? 13:29:24 13:29:25

A. In the sense of general discussions, yes. 13:29:26 13:29:27

Q. Did you discuss your answers to any of the questions today? 13:29:27 13:29:29

A. No, we had not. 13:29:30

Q. Let's move ahead, then, to 13:29:33

Paragraph 52. We had discussed this just a little bit, but at the end of this paragraph, which is the beginning of Page 22, if that helps, "Thus, the present invention improves upon the in-line gatekeeper by using one in an out of line configuration." 13:29:37 13:29:49 13:29:51 13:29:53 13:29:56 13:29:59

Do you see that? 13:30:01

A. I'm sorry, Counsel, I'm a little confused. 52 starts on 20? 13:30:02 13:30:04

Q. You're right. Apologies. Paragraph 53. 13:30:06 13:30:08

A. Okay. I got it now. 13:30:14

Q. Paragraph 53, you have a statement that says, "Thus, the present invention improves upon the in-line gatekeeper by using one in an out-of-band situation." 13:30:15 13:30:17 13:30:19 13:30:25

Do you see that? 13:30:29

A. You're referring to Page 22, right? 13:30:30 13:30:32

Q. Yes. 13:30:32

A. Okay. I do see that. 13:30:39

Q. When you say "out-of-band configuration" here, what do you mean by that? 13:30:40 13:30:42

A. So we can see this reflected in the specification and the respective figures in 13:30:45 13:30:48

terms of contrasting the prior art, conceptual gatekeeper with the gatekeeper that's defined in the invention, the notion of being out of band. 13:30:53 13:30:57 13:30:59 13:31:06

So if we look at kind of the distinction is in line is where traffic passes through it. We had talked about earlier the notion of some of the disadvantages of having an in-line gatekeeper. 13:31:06 13:31:08 13:31:10 13:31:10 13:31:13

In this case, as shown in the figure, which is mentioned or, I guess, I don't know, mentioned or directly copy pasted on that, there's the notion of an out of band where all of the data does not pass through the gatekeeper. And I'll say there is a typo I see "'without the passing the date through the gatekeeper.'" So I'm pretty sure that should be data on that with respect to that. 13:31:15 13:31:16 13:31:19 13:31:23 13:31:26 13:31:32 13:31:34 13:31:38 13:31:41

So for the out of band, now the gatekeeper itself in most of the embodiments and its core functionality ends up residing out of band or not in line with the access. 13:31:43 13:31:48 13:31:54 13:31:58

Q. So is it your opinion that before the asserted patents, a POSITA would not have understood gatekeepers to be used out of band? 13:32:02 13:32:04 13:32:08

MR. SCHWERIN: Object to form. 13:32:13

A. I'm sorry, I believe, as I had described earlier, a POSITA would have understood or seen, as described in the patent specification, the notion of generally the type of functionality as being in line. And the patent specification further continues by describing some of the disadvantages of trying to put that type of functionality in line, and it recites, what would have comported with my understanding several of the disadvantages of trying to have this type of functionality in line. 13:32:19 13:32:21 13:32:25 13:32:31 13:32:37 13:32:41 13:32:44 13:32:47 13:32:55 13:32:58 13:33:00 13:33:02

Q. So before the asserted patents, a POSITA would have understood "gatekeeper" to mean in line; fair? 13:33:03 13:33:06 13:33:10

MR. SCHWERIN: Object to form. 13:33:12

A. I think it would be more accurate to say that the prior art for a typical approach that would have been undertaken would have envisioned the gatekeeper type of functionality or the gatekeeper functionality as described as being in line with regard to being in line on the access points to try to deliver that type of higher level functionality 13:33:13 13:33:21 13:33:28 13:33:32 13:33:34 13:33:37 13:33:43 13:33:47

in that particular application space. 13:33:52

Q. In the next paragraph, 54, you 13:33:54
state "the concept of the gatekeeper was known 13:34:06
both in the prior art as well as during the 13:34:10
time of the invention." 13:34:13
Do you see that? 13:34:14

A. I do. 13:34:15

Q. Is it your opinion that the 13:34:16
concept of a gatekeeper that was known in the 13:34:18
prior art was an in-line gatekeeper? 13:34:18
MR. SCHWERIN: Object to form. 13:34:21

A. As I describe in my report, and as described in the patent specification, it describes how prior art would have viewed type of functionalities being delivered in line that a gatekeeper would deliver. 13:34:21 13:34:34 13:34:37 13:34:43 13:34:46

Q. And before the asserted patents, 13:34:47
are you aware of any gatekeepers that would 13:34:53
have been out of band? 13:34:56
MR. SCHWERIN: Object to form. 13:34:58

A. I don't believe I would have conducted a survey in terms of trying to exhaustively explore whether a gatekeeper would have been out of band. 13:34:58 13:35:05 13:35:08 13:35:11

Q. Are you aware of any? 13:35:12

A. Given that I haven't conducted that analysis, I can't say whether I'm aware or not.

Q. That confuses me a little, so I'm going to try again. I understand you haven't connected the analysis. So is it fair to say, as you sit here, you're not aware of any?

A. Thank you, Counsel, for pointing out my extreme inelegance in answering the question there. Since I haven't conducted the analysis, I don't have an opinion with regard to exhaustively exploring if a gatekeeper would have referred to out of band.

Q. In Paragraph 55 you say, "The specification and claims consistently afford gatekeeper the same (plain and ordinary) meaning."

Is that still your opinion?

A. Yes, it is.

Q. And that's the same plain and ordinary meaning that existed in the art before?

MR. SCHWERIN: Object to form.

A. I believe as I describe here, I say that the specification and claims

consistently afford "gatekeeper" the same plain and ordinary meaning.

Q. In 57 you say that "the gatekeeper can include, for example," and then you list several things, "a security policy, policy auditor, access control."

Do you see that?

A. I do.

Q. Is it fair to say that a gatekeeper does not have to include those things?

MR. SCHWERIN: Object to form.

A. I believe, as I show here, I'm referring to the fact that Figures 3A and 3B have a -- they show a picture of the gatekeeper and included inside of the gatekeeper are the respective elements that are enumerated there in that same figure.

Q. So as a POSITA, do you know with reasonable certainty whether a gatekeeper must include those things?

MR. SCHWERIN: Object to form.

A. Sorry, Counsel, could you repeat that question? I just wanted to make sure I followed it.

Q. Sure. As a person of ordinary skill in the art, do you know with reasonable certainty whether a gatekeeper must include those things? 13:37:55 13:37:57 13:37:58 13:38:00

MR. SCHWERIN: Same objection. 13:38:02

A. I believe in order to deliver the type of functionality as might be needed for that, that we would see, in particular, the security policy. In order to be able to audit that, we would have to have security policies that, in turn, are used by the policy auditor. 13:38:03 13:38:26 13:38:31 13:38:34 13:38:38 13:38:43

Then the notion of how to remotely reconfigure or how we had talked about the notion of reconfiguration would be what is further described in the patent with regards to access control, which can encompass a variety of things, at a high level those conceptual components would be present in a gatekeeper. 13:38:46 13:38:49 13:38:52 13:38:55 13:38:57 13:39:02 13:39:08

Q. What the about a policy auditor? 13:39:10

MR. SCHWERIN: Object to form. 13:39:15

A. In what sense? Just to clarify, what do you mean by a policy auditor? 13:39:16 13:39:25

Q. Well, in that same sentence, you say a gatekeeper can include, and one of the examples is a policy auditor. So as a person 13:39:27 13:39:28 13:39:31

of ordinary skill in the art, would you understand a gatekeeper to necessarily include a policy auditor? 13:39:33 13:39:35 13:39:36

MR. SCHWERIN: Same objection. 13:39:43

A. So if I understand your question correctly, a policy auditor is going to be needed to take what's -- to be able to take the view of the particular access device and its respective system data, or data that's being shared, to evaluate it for the purposes and understanding what is the right security policy or policies that would be needed, and in turn, then, to audit appropriately based on -- again, there's nuance in terms of the claims, so I'm talking a bit more in terms of a high level. Each claim has particular aspects that it governs. 13:39:44 13:39:48 13:39:56 13:40:04 13:40:08 13:40:12 13:40:17 13:40:19 13:40:23 13:40:27 13:40:30 13:40:36 13:40:38

The auditor is, in turn, able to take those security policies, and then audit the respective device as to what security policy applies, and then from that is able to appropriately apply or direct that access control with respect to that broader goal, which we had talked about earlier, with regards to protecting the network that we're trying to 13:40:39 13:40:44 13:40:50 13:40:53 13:40:57 13:41:06 13:41:11 13:41:13

protect, which is kind of why the gatekeeper is involved in the first place. 13:41:19 13:41:25

Q. If I understand your answer correctly, it's your opinion that a POSITA would understand a gatekeeper to necessarily include a policy auditor? 13:41:25 13:41:28 13:41:31 13:41:33

MR. SCHWERIN: Object to form. It's misstating the witness' testimony. 13:41:36 13:41:37

A. That would, if I understand your question correct, would depend upon the security policies that would be in play with regards to the device and the type of access, but in a very broad sense, in order to be able to interpret, take the security policy, and then be able to assess whether the access device as the appropriate posture or the appropriate system data to the appropriate policy with respect to the type of -- I guess not the type, the particular elements of the protected network or that less restricted subset on that, that system data would need to be then assessed by the policy auditor bringing in the respective security policies, and then a decision would need to be made with regards to how that might manifest itself in access 13:41:41 13:41:59 13:42:03 13:42:09 13:42:14 13:42:20 13:42:25 13:42:29 13:42:34 13:42:37 13:42:40 13:42:46 13:42:49 13:42:58 13:43:00 13:43:03 13:43:05

control for appropriately controlling access. 13:43:08

Q. And that's how a POSITA would understand "gatekeeper"? 13:43:10 13:43:14

A. A POSITA would understand "gatekeeper" in the context of the specification and the claims, but also being careful in terms of the nuance of the specific claim language as relevant, given that there are multiple permutations and discussions of what would be necessary as per the claim language in tandem with the specification. 13:43:20 13:43:26 13:43:28 13:43:33 13:43:37 13:43:40 13:43:42 13:43:47

Q. You've reviewed the claims as part of your analysis, right? 13:43:50 13:43:58

A. Sorry, Counsel, you kind of jumped a little bit. I don't know if it's on my side or your side, but it appeared to kind of hiccup a little. 13:43:59 13:44:02 13:44:06 13:44:11

Q. You reviewed the claims as part of your analysis, correct? 13:44:11 13:44:14

A. I did look through the claims as part of my analysis, thought I would confess I don't have them memorized. 13:44:15 13:44:23 13:44:26

Q. Do you have any opinions that any of these terms that you've opined on are used in an atypical way in the claims? 13:44:27 13:44:33 13:44:34

MR. SCHWERIN: Object to form. 13:44:41

A. I don't recall opining in my report as to an atypical usage. I do opine with respect to claim construction, and the terms themselves and my opinion with regard to those terms as disputed as part of the case. 13:44:42 13:44:45 13:44:52 13:44:57 13:45:02

Q. Well, let me try to be more specific. Let's go back up to Page 19, Paragraph 50. It is your opinion regarding "gatekeeper" that it would be given its plain and ordinary meaning by a POSITA, right? 13:45:04 13:45:06 13:45:08 13:45:12 13:45:15

A. Looking at that in my report, I do agree it would be its plain and ordinary meaning for "gatekeeper." 13:45:18 13:45:31 13:45:33

Q. And there's a list of claims under "Claim Terms." Do you see that? 13:45:33 13:45:36

A. I do. 13:45:39

Q. And you did analyze those claims as part of reaching the opinion about "gatekeeper," right? 13:45:39 13:45:39 13:45:41

A. I did, as part of my analysis. 13:45:41

Q. And the conclusion you reached is that they're used in those claims consistent with the plain and ordinary meaning, right? 13:45:45 13:45:47 13:45:51

MR. SCHWERIN: Object to form. 13:45:54

A. Yes. Could you repeat that question, Counsel? I accidentally talked over my counsel. 13:45:55 13:46:02 13:46:05

Q. Absolutely. And you reached the conclusion that the term "gatekeeper" as used in those claims is consistent with its plain and ordinary meaning, correct? 13:46:05 13:46:06 13:46:10 13:46:12

MR. SCHWERIN: Same objection. 13:46:19

A. So I had reviewed each of the claims, and as I described in my report, a POSITA would understand it with reasonable certainty and would afford a plain and ordinary meaning. 13:46:20 13:46:21 13:46:28 13:46:30 13:46:34

Q. If we go to Paragraph 60. The first sentence says, "Indeed, the gatekeeper can gather information to assess the access device's compliance with a security policy." 13:46:35 13:46:52 13:46:54 13:46:56

Do you see that? 13:46:59

A. I do. 13:47:00

Q. Is that something, in your opinion, a POSITA would understand that a gatekeeper must be able to do? 13:47:01 13:47:02 13:47:04

MR. SCHWERIN: Object to form. 13:47:10

A. So I do see earlier in the prior paragraph, and this would be 59, on the same 13:47:47 13:47:50

page, going into the notion of obtaining, where it must obtain the metrics, and this is talking about the provisional patent with regard to determining whether the EP meets the audit criteria and that it must obtain the metrics associated with the EP. 13:47:52 13:48:02 13:48:04 13:48:10 13:48:15 13:48:18

And so, it would need to be able to obtain that data in order to be able to audit and determine whether a particular access device is in compliance with the security policy to then, in turn, be able to apply the appropriate access control with respect to the broader organizational policy and the goal of protecting the network. 13:48:22 13:48:24 13:48:27 13:48:31 13:48:35 13:48:40 13:48:44 13:48:49

Q. In your opinion, that's a function, as a person of ordinary skill in the art, would understand a gatekeeper, that a gatekeeper would need to be able to perform? 13:48:50 13:48:57 13:48:59 13:49:01

MR. SCHWERIN: Object to form. 13:49:06

A. So if I understand your question correctly, in light of the specification, and the claims, in order to be able to perform its tasks, that it would need to be able to obtain that information, that audit data, as I described up above in that earlier paragraph, 13:49:08 13:49:16 13:49:19 13:49:27 13:49:31 13:49:35

obtaining the audit data, and then applying an appropriate security policy as being one of the embodiments that's present in the respective inventions.

Q. Paragraph 61 you say "another aspect of the invention lies in the gatekeeper's ability to reconfigure an access point (and the ports thereupon), depending on whether the endpoint meets the network's security criteria."

Do you see that?

A. I do.

Q. Is it your opinion that that's how a POSITA would understand a gatekeeper, that it would need to be able to reconfigure an access point and the ports thereupon?

MR. SCHWERIN: Object to form.

A. I think it's important to understand that phrase in its entirety, because the specification explains that the gatekeeper needs to be able to reconfigure an access point and the ports, depending upon whether the endpoints meet the network's security criteria, and that, in turn, determination of the network's security criterion is based on the

security policy, and then the audit of that data and determining the type of access that should be granted or whether that access should be granted, again, subject to the claims and the specific order and how it's discussed in the nuance of each claim. 13:51:05 13:51:07 13:51:12 13:51:16 13:51:20 13:51:29

Q. You considered the specification in forming your opinions about how a POSITA would understand "gatekeeper," right? 13:51:30 13:51:32 13:51:33

A. I believe -- and again, I'm not a lawyer, but as I understand, one would need to consider the claim language itself, as well as the specification when arriving at the understanding that a POSITA would have with regards to particular terms and what that might mean. 13:51:34 13:51:44 13:51:46 13:51:48 13:51:51 13:51:55 13:51:58

Q. And you did that? 13:51:59

A. I believe so, as I described in my report. 13:52:00 13:52:05

Q. So, then, you say here the specification explains that as another aspect of the invention, right? 13:52:05 13:52:10 13:52:13

A. I do see where I say "the asserted patents' specification explains that another aspect of the invention lies in" -- 13:52:13 13:52:20 13:52:21

Q. And then it says "the gatekeeper's ability," right? 13:52:25 13:52:28

A. I do see that. 13:52:29

Q. So is it your opinion, then, that a POSITA, with the background of the specification, the prior art, all of the other things you've discussed and analyzed, would understand that a gatekeeper needs the ability to reconfigure access points and the ports thereupon? 13:52:29 13:52:33 13:52:35 13:52:38 13:52:40 13:52:43 13:52:47

MR. SCHWERIN: Object to form. 13:52:48

A. Could you repeat that? That was a fairly long question, Counsel, and I want to make sure I understood it. 13:52:49 13:52:58 13:53:00

Q. Sure. So is it your opinion, then, that a POSITA, with the background of the specification, the prior art, all of the other things you've discussed and analyzed, would understand that a gatekeeper needs the ability to reconfigure access points and the ports thereupon? 13:53:01 13:53:04 13:53:06 13:53:09 13:53:12 13:53:14 13:53:19

MR. SCHWERIN: Same objection. 13:53:19

A. So again, if I'm following your question correctly, the patent and the specification describes the gatekeeper, as we 13:53:20 13:53:33 13:53:42

talked about with respect to the access control module, the notion of being able to reconfigure an access point, and as appropriate in the ports thereupon.

But getting back to the nuance of some of the claim language and the specification, reconfiguration could involve ports, as well as potentially ports, but also thinking about ports, logical ports, and also thinking about firewalls and firewall aspects, such as access control lists, that the gatekeeper would be then, in turn, manipulating or reconfiguring that particular access point based on the results of the audits.

And the audits which, in turn, the policy auditor is looking at the security policy and the specific endpoint that one might be trying to reach and the types of services and various other aspects of the security policy, to then, in turn, be able to drive that access control element, which then, in turn, allows one to deliver the type of functionality that's described for a gatekeeper.

Q. So, then, a POSITA would understand that a gatekeeper needs the ability

to reconfigure an access point; fair? 13:55:22

MR. SCHWERIN: Object to form. 13:55:26

A. So a POSITA would understand that the gatekeeper, as described in the specification, the gatekeeper described in the invented gatekeeper, would be able to reconfigure the access point as I described in my report, being careful to note that distinguishing the notion of the prior art gatekeeper versus the gatekeeper as described in the invention. 13:55:26 13:55:34 13:55:40 13:55:46 13:55:50 13:55:55 13:56:01 13:56:04 13:56:07

Q. You then have -- let me ask you this question before we move on. 13:56:08 13:56:23

Can an access point be a gatekeeper? 13:56:25 13:56:27

MR. SCHWERIN: Object to form. 13:56:28

A. Which gatekeeper are you referring to? Are you referring to the prior art gatekeeper or the invented gatekeeper? 13:56:29 13:56:36 13:56:38

Q. So you determined that a POSITA would understand a plain and ordinary meaning for purposes of forming your -- 13:56:41 13:56:43 13:56:50

A. I apologize, I caught about 10 percent of that. 13:57:15 13:57:17

Q. I will try again. Apologies. So 13:57:17

you've opined that based on your analysis, gatekeeper should be given a plain and ordinary meaning. Based on the plain and ordinary meaning that you've derived, can an access point be a gatekeeper? 13:57:21 13:57:26 13:57:29 13:57:31 13:57:36

A. So I think it's important to be accurate with what I have -- as I've described with regards to the plain and ordinary meaning. I would say that the POSITA would understand the claim scope for the term "gatekeeper" with reasonable certainty and for the plain and ordinary meaning in light of the intrinsic evidence, which includes the specification as well, in addition to the claim language, with respect to the gatekeeper. 13:57:38 13:57:39 13:57:44 13:57:48 13:57:52 13:57:54 13:57:57 13:57:59 13:58:01 13:58:04

I'm sorry, Counsel, I kind of -- I'm trying to recall as we kind of repeated again. Would you possibly repeat that again so I can understand? 13:58:18 13:58:20 13:58:22 13:58:25

Q. Well, let me ask it this way. Do you know with reasonable certainty whether or not an access point can be a gatekeeper? 13:58:27 13:58:31 13:58:33

A. Thanks for the clarification, Counsel. I apologize on that. 13:58:35 13:58:39

MR. SCHWERIN: Object to form. 13:58:43

A. So in the prior art, gatekeeper -- a gatekeeper was effectively in line, which means it could be effectively coexisting on that same access point, if you will, because it was sitting in line as described on there.

It's important to distinguish the invented gatekeeper, which as we described earlier with regards to the distinction between in line and out of band, where the invented gatekeeper is now out of band as opposed to in line.

So in the invented gatekeeper, an access point would not be a gatekeeper, and even in the prior art, an access point would not be a gatekeeper either.

You can see evidence of that as well in the specification where if we look at the prior art for Figure 1, we can see there is 110 is shown as the gatekeeper, and 120 is shown as a different element, although sitting in line kind of the same device, if you will, potentially, or potentially in line where we see the gatekeeper is next to the access point or in line that the traffic passes through creating the disadvantages that we had talked

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 368 of 1144
INFOEXPRESS, INC. - EX2572

about earlier. 14:00:25

Q. Let's skip ahead to Paragraph 73, 14:00:25

on Page 33. 14:00:37

A. Counsel, you got a little fast 14:00:42

there. That was 73, right? 14:00:43

Q. Yes. Paragraph 73, Page 30. 14:00:46

A. Zoom has an annoying habit when it 14:00:50

gets a little behind of kind of speeding up. 14:00:52

So I apologize on that and we'll try to -- 14:00:55

Q. No worries. All right. Are you 14:00:58

there? 14:01:11

A. I am on -- this is Page 33, 14:01:11

Paragraph 73? 14:01:12

Q. Yes. Let's go to 72 first. I 14:01:12

think this is just reaffirming your opinion, 14:01:14

but that "gatekeeper" would be "afforded its 14:01:15

plain and ordinary meaning as known in the 14:01:17

art"; that's your opinion, right? 14:01:19

A. It is my opinion, as I described 14:01:22

there and as I described earlier with regards 14:01:24

to in light of the specification an 14:01:26

understanding of what the invented gatekeeper 14:01:32

means. 14:01:34

Q. In Paragraph 73 you're discussing 14:01:34

the prosecution history, and you mention that 14:01:39

"InfoExpress disclosed Heintz as relevant to 'gatekeeper' recited in the '645 patent." 14:01:43 14:01:55

Do you see that? 14:01:56

A. I do see that. 14:01:58

Q. And you say "The portion of Heintz" -- (Mr. Logan's Zoom connection malfunctions) 14:01:58 14:01:59 14:02:44

A. Counsel, would you like to take a five-minute break, if that would be helpful? 14:02:44 14:02:46

Q. All right. I've done a little network configuration. No ports involved. But Let's see if that helped at all. All right. I'll try this again. 14:02:48 14:02:48 14:02:48 14:02:48

We're in Paragraph 73, there's a discussion of Heintz. Do you see that? 14:03:18 14:03:21

A. I do. This is spelled H-e-i-n-t-z. 14:03:22 14:03:23

Q. Your report says, "The portion of Heintz that InfoExpress cited, Paragraph 24, disclosed the 'network perimeter security device or provision, such as a software firewall.'" 14:03:27 14:03:29 14:03:32 14:03:35 14:03:37

Do you see that? 14:03:38

A. I do. 14:03:39

Q. And is that consistent with your 14:03:39

understanding of "gatekeeper" that it can also encompass things such as a software firewall? 14:03:41 14:03:44

MR. SCHWERIN: Object to form. 14:03:54

A. So I think it's important in this case not to conflate these aspects on here. As I describe on here, I describe in Paragraph 24 where it had disclosed the network perimeter security device or provision. One example could be a software firewall. 14:03:55 14:03:58 14:04:03 14:04:08 14:04:11 14:04:14

And then I further continue where I say that the examiner did not have an issue in light of the specification, understanding the term "gatekeeper." So I don't think it would be accurate to say that a gatekeeper is a firewall. 14:04:18 14:04:21 14:04:25 14:04:29 14:04:32 14:04:34

Q. Do you agree that a firewall can be an example of a gatekeeper? 14:04:34 14:04:39

MR. SCHWERIN: Object to form. 14:04:43

A. I don't know if I would agree with that characterization. In a very broad sense, I know in some of the extrinsic literature that one could use the term "gatekeeper" to try to understand what a firewall -- one of the types of things that a firewall might do. 14:04:44 14:04:48 14:04:54 14:04:59 14:05:03 14:05:08

But the patent and the 14:05:12

specification is quite clear in terms of describing in its specification what are the types of functionality that a gatekeeper is trying to offer, and in my opinion, I would view it as being distinctive from a firewall.

Q. In Paragraph 74 you discuss another piece of prior art called Mann. Do you see that, M-a-n-n?

A. I do.

Q. That was also cited during prosecution, correct?

A. I believe so, given that I put it here, but I don't remember 100 percent.

Q. At least your report says it was cited during prosecution. Fair enough?

A. That is correct, and I trust that I had written it down correctly when examining the evidence.

Q. You have an excerpt from Mann like a block quote. It says, "The gatekeeper 104 may be implemented as a security management software agent."

Do you see that?

A. I do.

Q. Is that consistent with your

understanding of the plain and ordinary meaning of "gatekeeper" that it can be a security management software agent? 14:06:21 14:06:23 14:06:25

MR. SCHWERIN: Object to form. 14:06:26

A. As we had talked about earlier, when understanding the term "gatekeeper," one would read the specification, and the types of broader functionality that one might want a gatekeeper to perform. 14:06:33 14:06:35 14:06:37 14:06:40 14:06:46

In this case, it talks about the notion of a gatekeeper, and then it goes into further detail in Mann in terms of how a gatekeeper might be implemented on that, providing one way, in their view, for a gatekeeper how it might be implemented to provide the type of solutions that the particular publication, in this case we referred to it as Mann, would be trying to deliver. 14:06:49 14:06:50 14:06:54 14:06:57 14:07:02 14:07:04 14:07:06 14:07:10 14:07:14 14:07:16

Q. A POSITA applying the plain and ordinary meaning of "gatekeeper" would understand that it could be a security management software agent? 14:07:16 14:07:20 14:07:22 14:07:23

MR. SCHWERIN: Object to form. 14:07:28

A. So if a POSITA was reading Mann 14:07:28

and reading the specification, would be able to understand that the term "gatekeeper," as described in the Mann publication, would be one way that it could be implemented. 14:07:35 14:07:41 14:07:52 14:07:54

Whereas, conversely, they would also read the specification and understand in reading the patents, the asserted patents, to understand the meaning of "gatekeeper" as well, as we've discussed in great detail. 14:07:57 14:07:59 14:08:01 14:08:05 14:08:11

Q. Another sentence towards the middle of that block says, "In the local mode, the gatekeeper 104 executable operates on desktop and laptop computers forming a security layer on top of personal synchronization tools." 14:08:12 14:08:14 14:08:14 14:08:19 14:08:23 14:08:25

Do you see that? 14:08:25

A. I do. 14:08:26

Q. Is that consistent with what you understand to be the plain and ordinary meaning of "gatekeeper"? 14:08:26 14:08:28 14:08:30

A. Well, in this case it's describing the in local mode. It's also talking about earlier the notion of a gatekeeper operating in two modes to support local and network synchronization. 14:08:42 14:08:44 14:08:47 14:08:51 14:08:55

And here, it's describing the local mode of what's viewed as the gatekeeper for the particular local -- in this case, they're viewing a gatekeeper as being in a local mode in this particular patent application. 14:08:56 14:08:58 14:09:02 14:09:06 14:09:08 14:09:12

Q. And you included this excerpt because it was part of your analysis about how a person of ordinary skill in the art would understand the term "gatekeeper," right? 14:09:13 14:09:17 14:09:19 14:09:22

A. I included this in my analysis because this was part of the intrinsic references. And as I understand, intrinsic references do include, and I'm not a lawyer, so apologies if I get that a bit wrong, but the prosecution history does include various references that are cited, that is part of the intrinsic evidence. 14:09:25 14:09:32 14:09:35 14:09:40 14:09:43 14:09:47 14:09:51 14:09:54

And in this case, I had looked through intrinsic references that it also used the term "gatekeeper," and described in their specification the types of functionality and aspects of a gatekeeper that would be delivered as part of either those applications or other documents that I had considered. 14:09:55 14:09:58 14:10:01 14:10:04 14:10:07 14:10:11 14:10:16

Q. Is it fair to say that within the scope of the plain and ordinary meaning of "gatekeeper," it would include software running on an access device, like a laptop? 14:10:18 14:10:21 14:10:23 14:10:25

MR. SCHWERIN: Objection. It's misstating the reference. 14:10:33 14:10:35

A. So I think in this case, as we've talked about in a fair amount of detail, taking into account the specification, and in this case, the specification discusses how a gatekeeper might be implemented, and it talks about the notion of a security management software agent that forms a virtual security layer on existing third-party synchronization systems, such as, and it provides several examples. 14:10:39 14:10:41 14:10:45 14:10:48 14:10:52 14:10:54 14:10:57 14:11:01 14:11:04 14:11:07

And then that particular, I believe it's paragraph, continues onward in describing a local mode as well as a network mode of a gatekeeper as envisioned in that particular patent application. 14:11:07 14:11:11 14:11:14 14:11:18 14:11:22

Q. And a POSITA would understand that to be within the scope of the plain and ordinary meaning of the term "gatekeeper," correct? 14:11:24 14:11:29 14:11:30 14:11:33

MR. SCHWERIN: Object to form. 14:11:33

A. I think it's important to go back to what I had described in terms of the plain and ordinary meaning, and it was the plain and ordinary meaning in light of the claims themselves, and the respective specification, particularly when we had been discussing nuance with regards to the invented gatekeeper, and how it delivered that particular functionality as described in the specification and described in the claim language. 14:11:45 14:11:47 14:11:49 14:11:52 14:11:57 14:12:01 14:12:05 14:12:10 14:12:12

Q. Do you know with reasonable certainty as a POSITA whether a gatekeeper could be an executable operating on a laptop computer? 14:12:14 14:12:17 14:12:20 14:12:25

MR. SCHWERIN: Objection. That's a misstatement of the testimony. 14:12:26 14:12:27

A. I guess I'm not totally following your line of questioning, Counsel. Could you maybe restate that? 14:12:28 14:12:41 14:12:48

Q. I'll try. Mann discusses a gatekeeper as an executable that may be operating on a laptop. Is that fair? Can we agree with that? 14:12:49 14:12:58 14:13:00 14:13:03

MR. SCHWERIN: Objection to form. 14:13:04

A. I think it would be more accurate to say that Mann describes in a local mode an executable -- the gatekeeper is an executable that operates in a desktop and laptop computer forming a security layer on top of, in this case, on top of personal synchronization tools. 14:13:05 14:13:08 14:13:13 14:13:18 14:13:22 14:13:25

Q. Would a POSITA, such as yourself, understand that arrangement to be within the plain and ordinary meaning of the term "gatekeeper"? 14:13:28 14:13:36 14:13:38 14:13:41

MR. SCHWERIN: Same objection. 14:13:42

A. I think, as we discussed earlier, Counsel, when considering the plain and ordinary meaning, that does involve considering the specification and the claim language itself. 14:13:44 14:13:52 14:13:54 14:13:56 14:13:58

So I guess I'm not totally following your question. 14:13:58 14:14:00

Q. Considering those things, and all the things you used to reach your conclusion about the plain and ordinary meaning of "gatekeeper," would what's described here in Mann, the gatekeeper is an executable operating in a laptop, be within the scope of the plain and ordinary meaning of this term? 14:14:01 14:14:04 14:14:07 14:14:09 14:14:13 14:14:17 14:14:20

MR. SCHWERIN: Same objection. 14:14:22

A. I think I answered your question, Counsel. 14:14:23 14:14:26

Q. I didn't understand it, so if you could answer it for me directly, I'd sure appreciate it. 14:14:26 14:14:30 14:14:32

A. I guess I'm not quite following what you're getting at, Counsel. 14:14:33 14:14:39

Q. Okay. You do have an opinion as to -- I'll try again. 14:14:41 14:14:44

You do have an opinion as to there's a plain and ordinary meaning of the term "gatekeeper," right? 14:14:45 14:14:47 14:14:49

A. I do say, based on the claims in the specification, I understand the scope of gatekeeper to be affording its plain and ordinary meaning, being careful it's drawing upon both the claim and the specification to afford the plain and ordinary meaning. 14:14:50 14:14:58 14:15:00 14:15:03 14:15:06 14:15:08

Q. This is just yes or no. Can you answer with reasonable certainty whether or not this arrangement described in Mann, where a gatekeeper is an executable operating on a laptop computer, would be within the scope of your understanding of the plain and ordinary 14:15:10 14:15:17 14:15:19 14:15:23 14:15:23 14:15:27

meaning of "gatekeeper"; yes or no? 14:15:28
MR. SCHWERIN: Objection to form. 14:15:31
It's misstating what the reference says. 14:15:33
A. I'm not sure I would agree that's a yes or no question, Counsel. I think, as I described earlier, said that it's the plain and ordinary meaning is afforded with the claims and specification. That's how one arrives at the plain and ordinary meaning, taking into account those aspects. 14:15:35 14:15:36 14:15:39 14:15:42 14:15:44 14:15:48 14:15:50
I think, as I've said several times, I think I've answered that question. 14:15:54 14:15:57
Q. I'm going to try again and object as nonresponsive. 14:15:59 14:16:01
Applying all the different things that you applied to reach your opinion that you put forth that there's a plain and ordinary meaning of "gatekeeper," the claims, the specification, the prior art, all the things that went into reaching that opinion, my question for you is just very, very simple. Does the plain and ordinary meaning encompass a gatekeeper executable that operates on a laptop computer as described here in Mann; yes or no? 14:16:02 14:16:03 14:16:05 14:16:07 14:16:12 14:16:14 14:16:16 14:16:18 14:16:21 14:16:24
MR. SCHWERIN: Same objection. 14:16:31

Misstates the reference.

A. As I said before, I think I've answered that question as I described in my report, and I used to say that the plain scope of "gatekeeper" is based on the claims and the specification that it would be afforded its plain and ordinary meaning.

Q. So you cannot answer that question with a yes or no?

A. I think as I described earlier, Counsel, it's important to take into, as I understand it, the claims and specification when arriving at the plain and ordinary meaning. And as I described in my report, the plain and ordinary meaning is evident from the claims and specification for the event of gatekeeper.

Q. And applying all of that, you cannot answer this question yes or no; is that fair?

A. I don't know if that's fair, Counsel. As we described before, taking into account the claims and specification is appropriate for determining the plain and ordinary meaning.

Q. But you do understand I'm asking you to take that into account, right? 14:17:33 14:17:35

A. I do understand that you're asking that, but I also understand that you're adding in a few extra words, Counsel, and I'm answering your question as I understand it. 14:17:36 14:17:40 14:17:43 14:17:46

Q. And applying all of that, you cannot answer for me whether or not the gatekeeper arrangement we're discussing here in Mann is within the scope of the plain and ordinary meaning; is that true? 14:17:47 14:17:49 14:17:54 14:17:56 14:17:58

MR. SCHWERIN: Objection. That's been asked and answered. 14:18:00 14:18:04

A. I'm not sure I would agree with that, Counsel, as I think I've answered your question. 14:18:04 14:18:05 14:18:07

Q. And I want to make sure that I'm not asking this maybe too directly, maybe you feel like I'm trying to, you know, ask you to tell me with absolute certainty. Can you even answer that question with reasonable certainty? 14:18:07 14:18:13 14:18:17 14:18:19 14:18:22

MR. SCHWERIN: Object to form. 14:18:26

A. I guess I'm not getting your distinction between absolute and reasonable certainty on the question, Counsel. 14:18:27 14:18:34 14:18:36

Q. I see. So you don't understand what "reasonable certainty" means? 14:18:37 14:18:39

MR. SCHWERIN: Object to form. 14:18:41

A. I do understand that "absolute" and "reasonable" probably has a legal meaning. I'm not a lawyer, so I want to be careful not pretending to be a lawyer for the purposes of this deposition. 14:18:42 14:18:49 14:18:52 14:18:55 14:18:59

Q. What's your understanding of what "reasonable certainty" means within the context of your report? 14:19:00 14:19:01 14:19:04

A. I don't know if I have a specific section that talks about the difference between "reasonable" or "absolute certainty." I'm not a linguist, and again, I'm not a lawyer, so I don't know if it would be appropriate for me to expound upon that, outside of recognizing the difference between "absolute" and "reasonable certainty." 14:19:04 14:19:12 14:19:14 14:19:18 14:19:23 14:19:25 14:19:28 14:19:31

Q. All right. Let's move ahead to Paragraph 79. Paragraph 79 says, "Wood thus demonstrates one in the art would readily understand a gatekeeper to mean a component that obtains or maintains information regarding the endpoint, and then can assess that 14:19:32 14:19:33 14:19:39 14:19:42 14:19:43 14:19:46

information as needed by the system." 14:19:49
Do you see that? 14:19:51
A. I do. 14:19:52
Q. Do you still agree with that 14:19:53
statement? 14:20:01
A. Yes, I would. 14:20:01
Q. And is that what "gatekeeper" 14:20:02
would mean to a person of ordinary skill in the 14:20:04
art at the time in your opinion? 14:20:06
MR. SCHWERIN: Object to form. 14:20:09
A. I think, as I wrote here, Wood 14:20:21
demonstrated that someone would -- that one in 14:20:22
the art would understand a gatekeeper to mean a 14:20:24
component that obtains or maintains information 14:20:26
regarding the endpoint. 14:20:29
We had had a discussion earlier 14:20:31
with regards to obtaining information, and then 14:20:33
assessing that information as needed by the 14:20:36
system, a gatekeeper is not just that, 14:20:39
describing some of the components that would be 14:20:45
present inside of a gatekeeper. 14:20:47
Q. So applying, then, that 14:20:55
understanding that you've put forth here in 14:20:56
Paragraph 79, could a gatekeeper be a router? 14:20:59
MR. SCHWERIN: Object to form. 14:21:03

A. I would not term it as saying a gatekeeper is a router. 14:21:03 14:21:08

Q. Could a switch be a gatekeeper? 14:21:09

MR. SCHWERIN: Same objection. 14:21:13

A. I think we had described earlier the distinction between, say, like an access point or a router or a gatekeeper, and that they are distinctive entities, that they could be present in line as envisioned in the prior art, or that it could be out of band for the gatekeeper as discussed in the invented gatekeeper. 14:21:14 14:21:17 14:21:21 14:21:25 14:21:29 14:21:32 14:21:37 14:21:39

Q. Well, let's just try to apply the definition you have here in Paragraph 79. Would it be fair to say that an access point obtains information about endpoints? 14:21:40 14:21:42 14:21:46 14:21:48

MR. SCHWERIN: Object to form. 14:21:52

A. I think on here what I'm describing is that it's broader being a component, and some of the types of functionality that would deliver, but I wouldn't say that this is only the things that the invented gatekeeper provides. 14:21:52 14:22:02 14:22:10 14:22:12 14:22:14 14:22:15

MR. SCHWERIN: I don't want to break up your line of questioning, but 14:22:19 14:22:20

could we go off the record for a second to discuss timing? 14:22:22 14:22:24

MR. LOGAN: Yeah, sure. Give me just a minute. 14:22:26 14:22:28

Q. All right. What about applying, you know, this definition we discussed, "firewall" earlier? Are you saying this firewall does not meet what you've put in Paragraph 79; is that true? 14:22:30 14:22:31 14:22:33 14:22:38 14:22:41

MR. SCHWERIN: Object to form. 14:22:43

A. As I described here in the paragraph is that these are some of the elements that a gatekeeper would do in terms of some of the types of functionality that it would have, and I also describe elsewhere in my report, and as described in the specification, different elements that would be present in a gatekeeper to be able to deliver the overall functionality that was intended. 14:22:44 14:22:46 14:22:53 14:22:55 14:22:57 14:23:00 14:23:03 14:23:05 14:23:08

Q. Could a gatekeeper be a server? 14:23:10

MR. SCHWERIN: Object to form. 14:23:14

A. So I believe in the specification it talks about a notion of a gatekeeper running on a server that may be present in that restricted subset that one could have one or 14:23:15 14:23:26 14:23:28 14:23:30

more servers providing the gatekeeper functionality as part of one of the embodiments.

Q. What about, does it have to be software?

MR. SCHWERIN: Object to form of the question.

A. I'm not sure what you're getting at, Counsel, with regards to software?

Q. Does it gatekeeper have to be software? Can it be hardware?

MR. SCHWERIN: Object to form.

A. Could you define that a bit more precisely, Counsel?

Q. I guess if you can help tell me which part of it is you don't understand, hardware or software, I'll do my best?

A. Well, Counsel, most hardware would end up running some sort of software, which is where I'm struggling a bit with your questions.

Q. Fair enough. So it's fair to say that a gatekeeper is going to be some software; is that fair?

MR. SCHWERIN: Object to form. Misstatement of the witness' testimony.

A. I think one wants to be careful when looking at a system, such as the gatekeeper, that would be running, say, on the restricted subset that it would involve running software, and software typically would run on some sort of hardware, as typical for a computing system where one is delivering this type of functionality in this particular application domain. 14:24:41 14:24:43 14:24:44 14:24:49 14:24:52 14:24:55 14:25:00 14:25:03 14:25:06

Q. And is it your understanding that a gatekeeper can be on a client machine? 14:25:07 14:25:11

MR. SCHWERIN: Object to form. 14:25:15

A. I think getting back to our earlier discussion, Counsel, with regard to understanding the gatekeeper in light of the specification and the claim language, the invented gatekeeper exists out of band, and understanding that, it would be appropriate for understanding the plain and ordinary meaning of the term "gatekeeper." 14:25:16 14:25:21 14:25:25 14:25:28 14:25:31 14:25:37 14:25:42 14:25:44

MR. LOGAN: All right. This might be a good time to take a break, Andrew, if you want to discuss the timing. 14:25:47 14:25:48 14:25:50

MR. SCHWERIN: Yeah. 14:25:52

THE VIDEOGRAPHER: Going off the 14:25:55

record at 2:25 p.m. 14:25:56
(Recess taken at 2:25 p.m. and 14:25:59
reconvening at 2:36 p.m.) 14:26:04
THE VIDEOGRAPHER: Back on the 14:36:39
record at 2:36 p.m. 14:36:40
BY MR. LOGAN: 14:36:44
Q. Dr. Striegel, we'll go to 14:36:44
Paragraph 123 of your report. It's on Page 53. 14:36:48
Let me know when you're there. 14:36:52
A. Yes, I'm there, Counsel. 14:36:54
Q. The first sentence says, "To date, 14:37:05
there have been four versions of the 802.1X 14:37:07
standard: 2001, 2004, 2010 and 2020." 14:37:11
Do you see that? 14:37:17
A. I do. 14:37:19
Q. And it said you reviewed these 14:37:19
four versions of the standard, right? 14:37:21
A. Correct. 14:37:22
Q. Did you review them by comparing 14:37:23
them with each other? 14:37:25
A. I had compared them to each other, 14:37:31
in addition to having previous familiarity with 14:37:33
them. I compared them as well as read back 14:37:35
through them. 14:37:41
Q. And if you -- in Paragraph 144 you 14:37:41

say, "As set forth above, the various versions of the 802.1X are consistent over the years." 14:37:56 14:37:59

Do you see that? 14:38:06

A. Which wage is that, Counsel? 14:38:08

Q. Paragraph 144, which falls on Page 68. 14:38:12 14:38:15

A. Thank you. So which paragraph -- sorry, Counsel. I was flipping through. What was the paragraph number again in the question? 14:38:24 14:38:26 14:38:28

Q. You know, just to keep us actually close to where we were, I guess we could just go back to 117, Paragraph 117, Page 51. It's the same statements there. We'll stay where we are. 14:38:30 14:38:32 14:38:40 14:38:40 14:38:44

A. No problem. You're testing my memory, Counsel. 14:38:44 14:38:46

Q. Yeah, we're just bouncing around. 14:38:48

A. Hence the -- 14:38:48

Q. And agility. Paragraph 117 says the standard "has been interoperable and consistent over the years." 14:38:51 14:38:54 14:38:56

Do you see that? 14:38:57

A. I do. 14:38:58

Q. How did you determine it was consistent over the years? 14:38:59 14:39:01

A. So as I had described earlier, I had reviewed the four standards, the four kind of years, if you will, that there had been 802.1X standards. In reading through it, I browsed back through the documentation, and then also my own personal understanding of 802.1X and the core functionality that was present as I describe here in terms of it being consistent, in terms of its underlying principles of how it works.

And then also, in reach of the respective standard years, once we get beyond 2001, discussions with regards to interoperability, as well as my own understanding of interoperability amongst the different standard years.

Q. In doing that, you reviewed both versions of the standard, for instance, from 2001 to 2020, and compared certain sections; is that fair?

MR. SCHWERIN: Object to the form.

A. I think I would just clarify that there's more than two, so I don't know if I would use both in the sense. So I had compared the respective standards across the years, as

well as the core of how 802.1X works. 14:40:23

I described in my report how it 14:40:28

evolved, and some of the reasons on why it had 14:40:29

evolved over the years, some of the changes. 14:40:32

But as I describe in my report, the core of the 14:40:34

functionality, these like EAP, the notion of a 14:40:38

supplicant, an authenticator, an 14:40:45

authentication, I've stayed consistent, because 14:40:46

the goal of what 802.1X is trying to provide, 14:40:48

that has stayed consistent. 14:40:56

What has happened is based on 14:40:58

newly emergent threats that have occurred in 14:40:59

the general ecosystem, the standard itself has 14:41:02

seen various modifications. We talked about 14:41:05

earlier like the IETF and some of the different 14:41:08

changes that have been proposed, those have 14:41:13

gradually been incorporated into the different 14:41:15

standard years. 14:41:18

Q. The most recent one you reviewed 14:41:19

was 2020, correct? 14:41:21

A. Correct. That's what I stated in 14:41:23

my report. 14:41:24

Q. Before the 2020 version was 14:41:24

published, you would have had no way to make 14:41:26

that comparison; is that fair? 14:41:28

MR. SCHWERIN: Object to form. 14:41:30

A. In the sense of when you look at various standards, these standards documents often have working groups that are assembled to arrive at said standards. 14:41:31 14:41:39 14:41:43 14:41:45

Often as a prelude to many of the standards, these working groups which might construct drafts, remember, kind of going way back to our earlier discussion today on some of the nuances of VLANs, there's oftentimes these working groups look at a particular niche or borderline cases, and those sorts of drafts, we talked about the IETF body, would go through and basically propose changes as part of those working groups to usually typically address broader problems that had been identified, and then those, in turn, may eventually become part of the standard if they're deemed worthy or appropriate by the overall standards body and through their ratification process in terms of how something becomes a standard. 14:41:51 14:41:55 14:41:57 14:41:58 14:42:01 14:42:04 14:42:06 14:42:11 14:42:16 14:42:18 14:42:21 14:42:24 14:42:27 14:42:29 14:42:33 14:42:35

Q. Just for an example, in Paragraph 125 you talk about how the "standard defines a mechanism for port-based access control." 14:42:37 14:42:42 14:42:45

Do you see that? 14:42:49

A. I do describe that where there's a definition of a mechanism for port-based access control. 14:42:49 14:42:51 14:42:56

Q. Do you understand that, for instance, the '484 and '444 patents don't expire until 2027? 14:42:56 14:42:58 14:43:01

A. I'm not a lawyer, so I couldn't tell you the exact mechanics and expiration. 14:43:05 14:43:07

Q. Okay. Do you know whether future versions will use the same port access control from now until 2027? 14:43:09 14:43:14 14:43:17

MR. SCHWERIN: Object to form. 14:43:19

A. I think as I describe in my report, and one can see this kind of repeating current as one goes through with regards to interoperability, and how standards operate, I describe a bit later in my report very specifically operability is called out, and given the wide variety of devices that are deployed, and the significant, I don't know if I would call it sort of need or just general inertia from the existing deployed devices, to try to maintain that backwards compatibility, I don't have a crystal ball, and I couldn't say exactly what might go in or even if there will 14:43:20 14:43:27 14:43:29 14:43:32 14:43:35 14:43:41 14:43:43 14:43:45 14:43:49 14:43:51 14:43:55 14:44:00 14:44:02

be a new revision of the standard before 2027.
I do feel reasonably confident in my expert opinion in that the core components that I've described that have stayed consistent in terms of how they operate between 2001, all the way through 2020, those core components will remain the same, and some parts will adapt, but those core, specifically that core, is highly relevant to the event of gatekeeper on some of its claims, those components will remain the same on essentially what it rides on top of.

Q. And then if we go to paragraph 136, you talk about the use of EAP. Do you see that?

A. I do.

Q. Do you know whether the use of EAP will change in future versions of 802.1X?

MR. SCHWERIN: Object to form.

A. So I think it's important to remember, EAP is usually how we would pronounce it, E-A-P, or the extensible authentication protocol, basically outlines kind of a foundational framework on the types of messages and how they're exchanged, but can adapt on top

of EAP. And we see later where I mention EAPOL, E-A-P-O-L, which is EAP over LAN. There's a wide variety of other types of EAP where essentially you build on the EAP framework to define protocols, so things I mentioned like PEAP and others, various higher level protocols build on the fundamentals of EAP, and the fundamentals of EAP dictate when you have a supplicant or a client when it connects up to the authenticator, nominally that access device, and then how it would appropriately authenticate to the authentication mechanism, and the back end typically being something like radius, that EAP governs the sequence of messaging, and oftentimes the nuance are specifics of how you might encrypt or who you might trust or how it might work, those will be dictated by the particular sort of protocol.

In its very nature, EAP is extensible. So it's intentionally built to allow one to extend that protocol appropriately.

MR. SCHWERIN: William, by my count, I think we're at time.

14:45:20
14:45:24
14:45:28
14:45:31
14:45:33
14:45:36
14:45:40
14:45:43
14:45:47
14:45:47
14:45:53
14:45:55
14:45:57
14:46:00
14:46:03
14:46:06
14:46:09
14:46:12
14:46:15
14:46:20
14:46:24
14:46:26
14:46:27
14:46:29
14:46:29

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 396 of 1144
INFOEXPRESS, INC. - EX2572

MR. LOGAN: Okay. All right. I'm wrapping up and then we'll go off the record. 14:46:31 14:46:32 14:46:34

Q. If I understand your opinion correctly, Dr. Striegel, what you're telling me is that a POSITA, in your opinion, in 2003, for instance, would have known what was going to be in the standard in 2020; is that fair to say? 14:46:35 14:46:37 14:46:43 14:46:45 14:46:48

MR. SCHWERIN: Object to form. 14:46:54

A. No. I don't think that's a fair statement. As I describe in my report, EAP dictates that framework. It was very intentionally meant to be extensible. A POSITA, who would have known 802.1X, would have already seen at the time different variations of EAP that were already running on that. 14:46:54 14:46:57 14:47:00 14:47:03 14:47:05 14:47:10 14:47:12

So to a POSITA, the fact that a new protocol writing on EAP were to come out, they might say, yes, I would expect something else to perhaps come out down that road, but they would also understand, based on the types of information exchanges and the sequence of events that typically occurs, as described in the 802.1X document, in terms of the general sequence, and I outline in my report that those 14:47:13 14:47:16 14:47:19 14:47:23 14:47:26 14:47:29 14:47:31 14:47:36 14:47:40

would be well known.

As I talked about earlier a little bit, the notion of how you encrypted, who signs what, public keys, private keys, and how you go about that, EAP was very intentionally built to allow one to architect protocols effectively writing EAP, things like optional fields, I describe that in my report, the specification looking at different counters, and kind of optionality that happens to be there, knowing that things may need to evolve on it.

And I think if you look at sort of the general evolution and seeing that the core components as I've described here stay consistent, which is what the invented gatekeeper and some of its claims leverages, have stayed remarkably consistent across the respective standards.

MR. LOGAN: Objection. Nonresponsive everything after "No." With that, I would say, Doctor, thank you for your time today. It has been a pleasure talking with you, and I pass the witness.

MR. SCHWERIN: No redirect. He

will read and sign. 14:48:56
THE VIDEOGRAPHER: Shall we go off the record? 14:48:57
MR. LOGAN: Andrew, I don't think there's anything in this one we need to designate, right? I'm just double-checking with you to make sure you don't have anything? 14:48:58
MR. SCHWERIN: You know, out of abundance of caution, Dr. Striegel was talking about his prior work with Sun, and, you know, I would like to stick to 30 days and just check that to see if we do need to designate it. Let's designate it for now and then we'll confirm that. 14:49:05
COURT REPORTER: Designate it as what, Counsel? 14:49:27
MR. SCHWERIN: Confidential. Let's do it highly confidential attorneys' eyes only. 14:49:30
THE VIDEOGRAPHER: Shall we go off the record? 14:49:49
MR. SCHWERIN: Yes. 14:49:51
THE VIDEOGRAPHER: Off the record 14:49:52

at 2:49 p.m. 14:49:53

COURT REPORTER: Could I have your orders, please? 14:50:12 14:50:13

MR. LOGAN: I know we'll want a rough, and then I'm not sure if we put an order in when we did this, but I can have somebody follow up with that. 14:50:18 14:50:19 14:50:21 14:50:23

MR. SCHWERIN: Yeah, we'll take the rough as well. I guess the final whenever they're done. 14:50:27 14:50:29 14:50:33

MR. DOTSON: Yeah, we'll do a rough, and let me get back to you on the final as well. 14:50:39 14:50:42 14:50:45

MR. LOGAN: What's the standard turnaround on the final? 14:50:48 14:50:49

COURT REPORTER: Two weeks. 14:50:55

MR. LOGAN: I think that will be fine for our purposes. We do want video synched for what that's worth. 14:50:56 14:50:58 14:51:08

(Whereupon the deposition concluded at 2:49 p.m.)

E R R A T A

I, AARON D. STRIEGEL, Ph.D., do hereby certify that I have read the foregoing transcript of my testimony, and further certify that it is a true and accurate record of my testimony (with the exception of the corrections listed below):

Page	Line	Correction

_

Signed under the pains and penalties of perjury this day of , 2024.

AARON D. STRIEGEL, Ph.D.

C E R T I F I C A T E

I, Michael O'Connor, Registered Merit Reporter/Certified Realtime Reporter, do hereby certify:

That AARON D. STRIEGEL, Ph.D., the witness whose testimony is hereinbefore set forth, was duly sworn by me and that such testimony is a true and accurate record of my stenotype notes taken in the foregoing matter to the best of my knowledge, skill and ability.

IN WITNESS WHEREOF, I have hereunto set my hand and Notarial Seal this 1st day of August 2024.

MICHAEL O'CONNOR, RMR, CRR, CRC
Notary Public

My Commission expires:
November 9, 2029

A
a.m 2:8 7:14
Aaron 1:23 2:13 6:3,10 7:4 8:13,22 120:3,23 121:6
ability 81:7 83:2,8,19 84:25 121:12
able 11:5 17:21 19:12 22:12,16 25:19 26:4 26:11 38:9 42:4,21 44:22,24 48:2 50:10 51:8 52:1,20 60:14 62:11 62:14,22 64:9 65:2 66:6 74:9 75:7,18,21 76:13,15 79:22 80:7,8 80:11,18,22 80:23 81:15 81:21 84:2 84:20 85:6 93:1 105:18
absolute 101:20,24 102:4,14,18
Absolutely 31:1 79:4
abstract 41:21
abundance 118:10
academic 14:19,22
access 27:20 28:20 29:1 30:3,15 32:7 33:5,7,12 34:7 35:8,10 35:21 36:6 38:1 39:23 41:9,11 42:15,18 44:5,8,17 53:5,15,22 54:4,8,9 55:12,17 56:24,25 58:5,19,21 59:18,20 63:9,10 64:19,21 69:22 70:24 73:6 74:16 75:8,22 76:12,15,25 77:1 79:16 80:9,12 81:7 81:15,21 82:2,3 83:9 83:20 84:1,3 84:11,13,21 85:1,7,14 86:4,22 87:4 87:13,14,23 95:4 104:6 104:15 112:24 113:2 113:10 115:11
accidentally 79:2
accomplish 18:18
accomplishi... 47:23
account 95:9 99:10 100:23 101:2
accurate 70:18 86:7 90:14 97:1 120:6 121:9
accurately 34:13
achieved 33:6 35:9
ACLs 15:7
acquired 47:14,16
adapt 27:10 114:8,25
added 36:9
adding 101:4
addition 86:14 108:22
additional 15:8 28:6 36:9
address 10:9 67:16 112:15
addresses 37:7 38:3
administer 8:11
afford 49:15 72:15 73:1 79:12 98:19
afforded 88:16 99:7 100:6
affording 98:16
agent 91:22 92:3,23 95:13
aggregated 46:15
agility 109:19
agree 32:2 52:17 78:13 90:16,19 96:24 99:4 101:14 103:4
agreeing 33:2
ahead 67:25 88:2 102:20
allow 19:9 115:22 117:6
allows 17:19 18:1 39:14 84:22
alluded 45:3
amount 15:25 95:8
analysis 65:10 72:2,6,11 77:13,19,21 78:21 86:1 94:8,11
analyze 78:18
analyzed 83:7 83:18
Andrew 3:18 8:6 9:9 107:22 118:4
andrew.sch... 3:19
annoying 88:7
answer 28:13 50:15 66:2,7 66:12 76:3 98:5,21 100:8,19 101:8,21
answered 37:12 50:22 51:21 58:13 61:25 65:22 66:15,17 98:2 99:12 100:3 101:13 101:15
answering 72:9 101:6
answers 50:22 67:22
anyway 51:14
apologies 68:10 85:25 94:15
apologize 85:23 86:24 88:9
appear 11:9,12 24:18
appeared 77:16
application 45:21 51:16 53:4,9,16 54:1 56:23 59:10 60:13 71:1 94:6 95:21 107:9
applications 94:24
applied 59:11 99:16
applies 75:21
apply 22:12 28:12 44:16 54:11 75:22 80:11 104:13
applying 81:1 92:20 99:15 100:18 101:7 103:22 105:5
appreciate 9:23 65:8 98:6
approach 39:18 70:20
approaches 28:19 29:8 30:2,14 31:3 32:6 34:6
appropriate 34:25 35:17

44:23 48:14 76:16,17,17 80:12 81:2 84:3 100:24 102:16 107:18 112:19
appropriately 10:4 35:2,6 55:19 57:25 62:13 75:13 75:22 77:1 115:12,23
architect 117:6
area 17:19 18:3
arrangement 57:17 97:8 98:22 101:9
arrangements 46:14
arrive 32:19 62:11 112:5
arrives 99:8
arriving 82:13 100:13
art 29:22 32:18 35:1,18 36:22 37:9 37:25 41:8 41:24 49:21 50:17 51:1 51:19 52:7 52:12 62:18 69:1 70:19 71:4,10,14 72:21 74:2 75:1 80:17 83:6,17 85:9 85:18 87:1 87:14,18 88:18 91:7 94:9 99:19 102:22 103:9 103:13 104:10
articulated 39:20 47:4 51:10 52:15
articulates 38:8
ascertain 60:15
aside 32:10 34:21
asked 32:15 37:13 58:13 66:5 101:13
asking 23:5 32:5 55:2 64:24 65:9 101:1,3,18
aspect 81:6 82:21,25
aspects 26:3 26:24 29:22 35:2 40:25 46:15 75:16 84:10,19 90:5 94:23 99:10
assembled 112:4
asserted 12:6 12:23 28:18 29:20 33:22 33:23 34:24 35:6 37:1,16 38:13,21 41:7 49:22 50:18 51:16 69:24 70:14 71:17 82:23 93:7
assess 76:15 79:16 102:25
assessed 76:22
assessing 103:18
assignment 32:22
assist 59:17 60:4 63:7 64:18
associate 59:4
associated 45:15,16,24 45:25 46:3,5 46:21,23,25 47:2,19,21 48:10,14 80:6
Atlanta 5:7
Attending 3:4 3:12 4:4,12 5:4
attention 10:9
attorneys 3:3 4:3 5:3 9:10
attorneys' 1:20 2:10 118:21
atypical 77:25 78:3
audit 74:9 75:13,19 80:4,9,24 81:1 82:1
auditor 73:6 74:11,19,22 74:25 75:3,6 75:18 76:6 76:22 84:16
audits 84:14 84:15
August 2:7 7:13 121:15
authenticate 115:12
authentication 111:8 114:22 115:13
authenticator 111:7 115:10
aware 13:20 30:14 31:7 32:11 40:20 71:18,25 72:2,7

B

B 6:7
back 26:17,18 31:11 40:17 44:11 47:10 63:21 67:10 67:14,16 78:8 84:5 96:2 107:13 108:4,23 109:12 110:5 112:9 115:13 119:12
background 83:5,16
backwards 113:23
ball 113:24
band 39:13 69:4,13,19 69:22,25 71:19,24 72:13 87:9 87:10 104:10 107:17
bandwidth 39:24
based 21:10 29:12 34:11 47:16 75:13 81:25 84:14 86:1,3 98:14 100:5 111:11 116:21
basic 21:15
basically 17:21 34:20 112:14 114:23
basis 34:10,22 35:25 40:8 61:18
bear 23:18
beast 49:1
beginning 34:4 41:6 66:4 68:3
begins 7:3
behalf 7:19,25 8:4
behaviors 21:10
believe 10:15 10:22 12:1 13:1,5,14,17 14:15 15:4 16:9 29:4,9 29:15 31:20 33:20 34:23 37:3 42:9 45:11 47:4 50:1 53:15 53:25 60:10 70:2 71:21 72:24 73:13 74:6 82:10 82:18 91:12 95:18 105:22
best 10:1 13:24 19:19 19:22 106:17 121:11
better 45:9

beyond 15:9 15:23 110:12
bit 13:8 16:16 17:11 19:24 21:14 26:10 26:19 32:24 41:17 43:11 44:13 48:25 50:4 68:2 75:15 77:15 94:15 106:13 106:20 113:17 117:3
blend 27:10
block 91:20 93:11
body 55:23 112:13,19
borderline 112:12
bottom 33:9
bouncing 109:17
break 41:15 66:24 67:1 67:14,18 89:9 104:25 107:22
bring 23:18
bringing 40:22 76:22
brings 38:7
broad 17:17 30:9,20 32:17 46:24 54:4 58:24 76:13 90:20
broader 23:17 29:16 55:8 55:20 75:23 80:13 92:8 104:19 112:16
broadly 14:21 28:11 41:4 55:2
browsed 110:5
build 20:12 115:4,7
built 115:21 117:5
bus 44:20

C

C 3:1 4:1 5:1 7:1 121:1,1
California 1:3 7:9
call 10:8,18 113:21
called 14:18 15:7,18,19 16:22 91:7 113:18
capable 27:11 27:11
Capitol 4:6
caption 7:11
Captioner 2:18
capture 20:4
careful 43:19 44:2 54:23 56:4,17 59:1 77:7 85:8 98:17 102:6 107:1
case 1:8,14 7:10,11,12 10:13,19 11:10,13 12:2 17:17 17:23 22:20 24:13 25:1 29:4,7,17 32:15 33:14 33:20 34:14 34:23 35:14 36:2,8 41:19 41:20 42:13 43:6,22 44:8 50:20 52:16 55:6 58:5 60:2 63:13 69:10 78:6 90:5 92:10 92:17 93:21 94:3,19 95:7 95:10 97:6
cases 16:22 21:13 112:12
caught 85:23
caution 118:10
cautious 32:25
caveat 25:25 26:25
CDT 2:8
cellular 17:9 21:13
centers 18:21 21:14
central 7:14
Centre 3:14
centric 17:2
certain 19:12 19:13 110:19
certainty 49:14 61:10 64:10 65:4,12 73:20 74:3 79:12 86:11 86:21 96:13 98:21 101:20 101:21,25 102:2,10,14 102:19
Certified 2:17 2:17
certify 120:4,6 121:5
change 47:6 114:18
changes 111:4 111:16 112:14
channels 44:10
characteriza... 90:20
characterized 24:7,20,23 24:25 25:10 25:13
charge 16:14
check 14:16 118:13
Chicago 1:24 2:14 3:7 9:5
choose 23:11 27:3 28:3 48:8
circa 15:15
circuit 57:12
Cisco 1:10 4:3 7:6,25
citation 31:23 31:24 33:16 36:9
citations 40:10
cite 32:8 35:10 40:4 62:4
cited 64:1,5 89:19 91:10 91:15 94:17
citing 24:13 25:2 29:5 34:14,20,23 35:5 41:20
claim 6:12 10:13,21 11:11 32:16 43:9 49:13 51:5 61:12 75:16 77:8 77:10 78:4 78:16 82:6 82:12 84:6 86:10,14 96:11 97:15 98:18 107:16
claimed 13:9 13:18,21 53:4,10,13
claims 12:3 39:19 42:11 50:11 51:8 72:15,25 75:14 77:6 77:12,18,20 77:25 78:15 78:18,23 79:6,10 80:22 82:4 96:5 98:14 99:7,18 100:5,12,16 100:23 114:10 117:16
clarification 9:23 86:23
clarify 11:15 34:2 37:18 47:12 74:21 110:22
Clark 3:6 4:17 8:2
clear 91:1
client 107:11 115:9
close 109:11
cloud 18:21
coexisting 87:3
Column 24:16 41:21

combine 21:11 22:17 27:5 27:16 28:2,7
come 22:19 31:19 116:18 116:20
comfortable 31:10
coming 32:14 67:13
Commission 121:22
common 11:25 12:6 29:20
communicat... 41:9,10,18 41:25 42:5 43:4,5,7,17 43:20 45:1,4 45:12
compared 108:21,23 110:19,24
comparing 108:19
comparison 111:25
compatibility 113:23
complex 46:14
compliance 79:17 80:10
complicated 16:17 17:12 21:15 46:16
complied 59:19 60:5 63:9 64:19
component 102:23 103:14 104:20
components 15:6 38:8 74:18 103:20 114:3,6,10 117:14
comport 30:5 40:12 59:24
comported 31:17 70:10
composed 58:18
computation 59:2
computational 57:9
computer 14:5 14:8 30:16 32:7 56:1,5 56:20 57:4 57:20,23 58:11,25 96:15 97:4 98:24 99:24
computers 56:10 93:13
computing 28:20 30:3 34:7 58:1 107:7
concept 16:4 71:3,9
conceptual 69:1 74:17
conceptually 16:10 22:16
concluded 119:21
conclusion 61:16 65:9 78:22 79:5 97:20
conducted 71:22 72:1 72:10
conducting 31:9 32:16
confer 67:18
confess 77:21
confident 114:2
confidential 1:20 2:10 118:19,20
configuration 19:11 27:25 36:13,17,23 37:5,11 38:11 39:13 45:19 46:4 47:24 59:8 68:6,23 89:11
configuratio... 20:15 38:16 38:23 46:7
configure 20:24 21:11 22:22,25 25:18 26:1 27:17,19
configured 35:20 36:5
confirm 12:5 118:16
conflate 90:5
conforms 35:21 36:6
confused 68:9
confuses 72:4
confusion 55:1
connected 58:4 59:2 72:6
connecting 58:2
connection 89:6
connections 17:24,25 18:9
connectivity 58:20
connects 115:10
consider 82:12
considerably 18:20 21:6
considered 62:6 82:7 94:25
considering 97:13,14,19
consistent 29:24 78:23 79:6 89:25 91:25 93:18 109:2,21,25 110:9 111:8 111:10 114:4 117:15,17
consistently 72:15 73:1
construct 16:9 23:18 27:12 112:8
construction 10:14,21 11:11 32:16 78:4
Constructions 6:13
constructs 26:12
Cont'd 4:1 5:1
contained 35:15 50:2 52:23
context 19:25 20:10 21:25 22:5,8 23:10 33:11 35:17 36:17 43:4 43:14,21 44:14,23 54:12,20 64:24 77:5 102:10
continue 15:8 90:10
continues 70:7 95:18
contrasting 69:1
control 30:15 33:5,12 35:8 38:1 54:8 73:6 74:16 75:23 77:1 80:12 84:1 84:11,21 112:24 113:3 113:10
controlled 54:9 55:18
controlling 28:19 30:2 32:6 34:6 53:5,14,22 54:4 77:1
conversation 17:14
conversely 93:5
copy 11:13 69:12
core 39:3 69:21 110:7 111:1,5 114:3,6,8,8 117:13

correct 8:25 9:1,11 10:14 10:15 14:2 76:10 77:19 79:7 91:11 91:16 95:25 108:18 111:20,21
Correction 120:9
corrections 120:8
correctly 18:25 20:20 27:23 53:19 75:6 76:4 80:21 83:24 91:17 116:5
cost 39:10,18 39:25 40:16 41:1
counsel 7:21 11:13,15 12:25 13:12 13:16 30:19 32:14 49:8 51:22 61:25 63:17 65:22 66:15,21 67:19 68:8 72:8 73:23 77:14 79:2,3 83:13 86:16 86:24 88:4 89:8 96:19 97:13 98:3,8 99:5 100:11 100:22 101:5 101:15,25 106:9,14,18 107:14 108:10 109:4 109:8,16 118:18
count 115:25
counters 117:9
couple 50:6
course 31:4
court 1:2 7:8 7:16 8:10 118:17 119:2 119:16
covered 51:9
CRC 1:25 121:19
create 18:1 26:23
creating 87:25
criteria 80:5 81:10,23
criterion 81:25
CRR 1:25 121:19
crystal 113:24
current 113:15
Currently 9:8
cut 30:22

D

D 1:23,25 2:13 2:15 6:1,3 7:1 8:13 120:3,23 121:6
Dallas 4:15
Dame 13:25 14:8,11,13 14:14
data 18:21 21:14 56:13 69:14,18 75:9,9 76:17 76:21 80:8 80:24 81:1 82:2
date 7:13 12:22 13:10 13:19,21,22 14:17 16:11 36:25 37:15 69:16 108:11
dates 16:7
David 5:9 8:3
day 10:7 120:19 121:14
daylight 7:14
days 118:13
dcdotson@... 5:10
decision 76:24
declaration 6:9 10:16,20 11:10
deemed 112:18
defend 55:16
Defendants 1:11,17
define 23:2,6 26:4 45:5,12 45:14 106:13 115:5
defined 15:20 24:8 25:11 69:2
defines 112:23
definition 20:23 52:18 104:14 105:6 113:2
definitional 60:21
delineation 25:19,21
deliver 17:21 22:23 28:15 38:10 41:3 48:3 55:23 70:25 71:16 74:6 84:22 92:19 104:21 105:18
delivered 52:14 57:9 71:15 94:23 96:9
delivering 57:18 107:7
demonstrated 103:12
demonstrates 102:22
denote 10:4
depend 19:10 22:8 23:7,14 27:15,22 44:15 45:18 59:7 76:10
depending 21:5 22:13 22:21 26:1 27:8,24 28:8 28:10 46:9 81:8,22
depends 22:24 28:14 59:5,6
deployed 113:20,22
deposition 1:22 2:12 6:2 7:4,15 102:8 119:20
depositions 9:14
derived 44:18 54:9 86:4
describe 19:24 29:18 34:24 40:9 50:1 51:3 53:12 60:2 61:2 63:22 71:12 72:24 90:6,6 105:15 110:8 111:5 113:1 113:13,17 116:11 117:8
described 19:5,15 22:10 31:16 33:15 38:2 39:1,6 40:15 41:4,20 42:9 42:19,20 49:24,25 50:21 52:10 53:25 54:5 55:14 57:5 58:2,23 59:8 62:1,1 63:21 64:4,14 65:1 65:21 70:3,4 70:23 71:13 74:15 79:10 80:25 82:18 84:23 85:4,5 85:7,10 86:7 87:5,7 88:19 88:20 93:3 94:21 96:3 96:10,10 97:22 98:22 99:6,24 100:3,10,14 100:22 104:5 105:11,16 110:1 111:2 114:4 116:23 117:14
describes 31:5 37:4,19 38:5 38:8 41:2 42:14 52:12

63:23 71:14 83:25 97:2
describing 25:15,16 28:17 29:21 34:15 37:21 50:8 56:23 70:8 91:2 93:21 94:1 95:19 103:20 104:19
designate 118:6,14,15 118:17
desktop 93:13 97:4
detail 92:12 93:9 95:8
detailed 31:9
determination 81:24
determine 80:9 109:24
determined 85:20
determining 59:17 60:4 63:8 64:18 80:4 82:2 100:24
device 19:14 33:7 35:10 35:21 36:6 41:11 44:5 45:17 47:22 47:25 59:17 60:3 63:7,9 64:17,19 75:8,20 76:12,16 80:10 87:21 89:21 90:8 95:4 115:11
Device' 59:18
device's 79:17
devices 19:13 19:14 23:11 25:23,24 27:11,12,20 28:1 39:23 56:24 57:6,9 57:18 58:1,8 58:10,15,18 58:21,21,22 59:2 113:19 113:22
dictate 115:8
dictated 115:18
dictates 116:12
difference 12:16 13:20 102:13,18
different 12:3 18:14,17 19:7 20:14 21:17 22:11 22:15 25:24 26:24 27:5,7 29:7 37:13 47:7 48:25 52:7 87:20 99:15 105:17 110:16 111:15,17 116:15 117:9
difficult 39:8 40:15,24
direct 15:24 36:19 66:6 75:22
directly 24:13 25:1 36:24 47:22,24 48:3 69:12 98:5 101:18
disadvantag... 40:12 69:8 70:8,11 87:25
disclosed 89:1 89:20 90:7
discuss 15:5 19:18 31:13 31:19 32:10 35:2,6,16 43:11 50:4 62:7 67:22 91:6 105:2 107:23
discussed 22:2 29:8,18 30:7,8,9 34:9 68:1 82:5 83:7,18 93:9 97:12 104:11 105:6
discusses 36:11 95:10 96:21
discussing 15:12,13 35:1 37:24 88:24 96:7 101:9
discussion 26:6 44:12 45:4 62:17 89:15 103:16 107:14 112:9
discussions 15:9 16:21 33:23 40:18 47:3 67:21 77:9 110:13
disputed 78:6
distinction 69:6 87:8 101:24 104:6
distinctive 91:5 104:8
distinguish 87:6
distinguishes 20:17
distinguishing 85:9
District 1:2,3 7:8,9
Division 1:4 7:10
Doctor 117:21
document 11:2 12:9 116:24
documentati... 17:6 51:11 110:5
documents 16:25 94:25 112:3
doing 22:14 47:9 48:20 62:24 110:17
domain 107:9
Dotson 5:9 8:3 8:3 119:11
double-chec... 118:7
Dr 6:9 8:24 9:2 9:13 10:12 11:19 67:13 108:7 116:5 118:10
drafts 16:12 112:8,12
draw 43:7
drawbacks 37:8 39:7 40:11
drawing 60:17 98:17
drive 84:20
Duane 5:5 8:4
dub 40:21
dubbed 58:5
due 40:15
duly 8:15 121:8

E

E 3:1,1 4:1,1 5:1,1 6:1,7 7:1,1 120:1 121:1,1
E-A-P 114:22
E-A-P-O-L 115:2
e.g 39:25
EAP 111:6 114:14,17,21 115:1,2,3,4,8 115:8,14,20 116:11,16,18 117:5,7
EAPOL 115:2
earlier 10:8 19:6,15 22:10 26:10 30:8 38:2 40:17 41:20 44:11 45:3 50:21 57:5 62:18 63:22 65:1,21 69:7 70:3 75:24 79:24 80:25 87:8 88:1,20 92:5 93:23 97:12 99:6 100:10 103:16 104:5 105:7 107:14 110:1 111:15

112:9 117:2
ecosystem 111:13
education 29:23 30:5
effectively 17:20 18:10 19:12,16 87:2,3 117:6
either 87:15 94:24
element 84:21 87:20
elements 59:12 73:17 76:19 105:13 105:17
embodiments 24:6 25:9,16 25:17 39:19 69:20 81:3 106:3
emerged 16:7
emergent 111:12
encompass 74:16 90:2 99:22
encrypt 115:17
encrypted 117:3
encryption 44:16
endpoint 44:17 59:18 59:20 60:5 63:8,10 64:19,21 81:9 84:17 102:25 103:15
endpoints 81:23 104:16
ends 69:21
engineering 14:6,8 16:23
ensure 35:20 36:5 55:18
enterprise 16:2 19:9 20:13 23:19 27:13
entire 34:10
entirety 81:19
entities 104:8
enumerated 73:17
envisioned 70:21 95:20 104:9
EP 80:4,6
equivalent 15:19
ESQ 3:9,18 4:9 4:17 5:9
essentially 114:11 115:4
evaluate 75:10
event 100:16 114:9
events 116:23
eventually 112:17
everyone's 47:15
evidence 53:2 62:5,10 64:5 86:13 87:16 91:18 94:18
evident 100:15
evolution 117:13
evolve 117:11
evolved 18:19 111:3,4
Ewing 3:5,13 8:7 9:6
exact 11:7 16:7,11 48:21,22 113:8
exactly 18:5 113:25
EXAMINATI... 8:18
examined 8:16
examiner 90:11
examining 91:17
example 36:21 63:14 65:15 66:10 73:4 90:8,17 112:22
examples 74:25 95:16
exception 120:7
excerpt 36:19 91:19 94:7
exchanged 114:25
exchanges 116:22
exclusively 45:17
executable 93:12 96:14 96:22 97:3,3 97:23 98:23 99:23
exhaustively 71:23 72:12
Exhibit 6:9,14 10:25 11:2 12:9,13
exist 46:1
existed 16:4 16:10 72:21
existing 95:14 113:22
exists 107:17
expect 116:19
experience 14:23 29:14 29:23
expert 6:9 10:13,19 11:9 114:3
expiration 113:8
expire 113:6
expires 121:22
explains 63:6 81:20 82:21 82:24
explanatory 53:16
explore 71:23
exploring 72:12
expose 55:11
expound 102:17
extend 115:22
extensible 114:22 115:21 116:13
extensively 15:2,10 30:6
extent 50:23 57:3
external 28:20 30:2,15 32:7 34:6 41:11
extra 101:5
extreme 72:9
extremely 39:8
extrinsic 51:25 61:4 62:10 64:5 90:21
eyes 1:20 2:10 118:21

F

F 121:1
fact 56:8 73:14 116:17
faculty 59:7
fair 9:25 10:1 10:18,21 15:24 16:3 23:1 26:15 46:23 53:23 56:21 57:23 60:8 70:16 72:6 73:9 85:1 91:15 95:1,8 96:23 100:20,21 104:15 106:21,21,23 110:20 111:25 116:8 116:10
fairly 83:13
falls 109:5
familiar 9:16 14:20 15:5 21:19,20 24:2
familiarity 15:1 108:22
far 46:16 67:17
fast 88:4
feel 12:14,16 31:10 66:6 101:19 114:2
felt 29:17 31:16
fields 117:7
figure 23:24 23:24 24:2

36:20,21 43:11,12,23 43:24 47:5 69:11 73:18 87:18
figures 68:25 73:14
file 10:25 11:4 11:6,7
filed 49:22 50:18 51:17
final 119:9,13 119:15
fine 11:17 67:3 119:18
firewall 84:10 90:2,9,15,16 90:23,24 91:5 105:7,8
firewall.' 89:22
firewalls 15:7 16:1 84:10
firm 8:4,7
first 7:10 14:13 26:17 31:2 46:21 49:11 59:15 63:6 76:2 79:15 88:14 108:11
five 67:1,3
five-minute 89:9
flipping 109:8
Floor 3:15
focus 17:2 40:25
folks 47:17
follow 119:7
followed 38:18 73:25
following 63:18 83:23 96:18 97:18 98:7
follows 8:16
Force 16:24
foregoing 120:4 121:10
form 19:4 23:4 26:8 29:3 32:1 45:6 47:11 50:19 52:9 53:24 54:21 56:2 60:9 63:15 64:23 66:14 70:1,17 71:11,20 72:23 73:12 73:22 74:20 76:7 78:1,25 79:23 80:19 81:17 83:11 85:2,16 86:25 90:3 90:18 92:4 92:24 96:1 96:25 99:2 101:22 102:3 103:10,25 104:17 105:10,21 106:6,12,24 107:12 110:21 112:1 113:12 114:19 116:9
formerly 47:13
forming 82:8 85:22 93:13 97:5
forms 95:13
forth 99:17 103:23 109:1 121:8
Fortinet 1:16 5:3 7:7 8:5
found 29:12
foundational 114:24
four 108:12,17 110:2,2
framework 114:24 115:5 116:12
front 11:8
full 14:18
function 80:16
functionalities 71:15
functionality 20:5 26:13 27:6 28:10 37:21,23 38:7,10 39:1 39:9,14 40:14,22 41:3 52:14 63:24 69:21 70:6,9,12,22 70:22,25 74:7 84:22 91:3 92:8 94:22 96:9 104:21 105:14,19 106:2 107:8 110:7 111:6
functions 52:25
fundamentals 115:7,8
further 10:2 46:13 70:7 74:15 90:10 92:12 120:5
future 113:9 114:18

G

G 7:1
gatekeeper 33:6 35:9,20 36:5,23 37:6 37:10,20,22 38:6,15,22 39:23,25 41:4 42:17 48:13,15 49:6,21,23 50:5,13,17 50:24 51:9 51:12,18,23 52:2,5,13,15 52:21 53:3 53:17,20 54:12,19 55:22 59:11 59:25 60:11 60:16,22 61:3,5,11,17 62:12,15,19 62:19,22,24 62:25 63:6 63:24 64:3,6 64:12,14,17 65:11,15,16 66:4,9,10 68:5,15 69:2 69:2,9,15,20 70:15,21,22 71:3,9,10,16 71:23 72:12 72:16 73:1,3 73:10,15,16 73:20 74:3 74:18,24 75:2 76:1,5 77:3,5 78:10 78:14,20 79:5,15,22 80:17,18 81:14,20 82:9 83:8,19 83:25 84:12 84:23,25 85:4,5,6,10 85:10,15,17 85:19,19 86:2,5,11,15 86:22 87:1,2 87:7,10,12 87:13,15,19 87:23 88:16 88:22 90:1 90:13,14,17 90:22 91:3 91:20 92:2,6 92:9,11,13 92:15,21 93:2,8,12,20 93:23 94:2,4 94:10,21,23 95:3,11,20 95:24 96:8 96:13,22 97:3,10,22 97:23 98:13 98:16,23 99:1,18,23 100:5,17 101:9 102:23 103:7,13,19 103:21,24 104:2,3,7,11 104:12,23 105:13,18,20 105:23 106:1 106:10,22 107:3,11,15 107:17,20 114:9 117:16
gatekeeper' 49:14 89:2
gatekeeper's

81:7 83:1
gatekeeper.' 69:17
gatekeepers 37:2,17 62:8 69:25 71:18
gather 79:16
geared 18:2
general 17:13 17:16 22:20 23:9 60:11 61:15 67:20 111:13 113:21 116:24 117:13
generally 19:23 20:1 57:3 58:1 70:5
Georgia 5:7
getting 37:7 40:17 41:1 44:11 54:14 55:7 56:6 84:5 98:8 101:23 106:8 107:13
give 20:11 66:12 105:3
given 9:13 17:20 19:10 22:13 29:20 48:10 53:20 64:25 72:1 77:8 78:10 86:2 91:12 113:19
giving 65:8
go 11:19 12:4 13:7 14:12 14:24 16:6 28:16 33:3 39:21 41:5 42:23 48:8 49:4 55:12 59:14 63:21 67:16 78:8 79:14 88:14 96:2 105:1 108:7 109:12 112:13 113:25 114:13 116:2 117:4 118:2 118:22
goal 27:24 55:8 75:23 80:13 111:9
goals 18:19 47:23
goes 52:11 92:11 113:15
going 9:20,21 20:20 26:18 31:8 33:10 39:14 42:22 45:20 50:14 51:13 63:3 66:22 72:5 75:6 80:1 99:13 106:22 107:25 112:8 116:7
good 8:20 66:23 107:22
govern 16:18
governed 58:8 58:10,14
governs 75:17 115:15
gradually 111:17
granted 82:3,4
granting 59:20 63:10 64:20
grasp 52:21
great 67:4 93:9
greater 33:5 33:12 35:8
greatly 9:23
group 15:24 26:21 30:12
groups 112:4 112:7,11,15
guess 15:19 22:1 48:8 58:15 60:18 63:16 69:11 76:18 96:18 97:17 98:7 101:23 106:15 109:11 119:9
guide 17:13

H

H 6:7
H-e-i-n-t-z 89:17
habit 88:7
hand 121:14
happen 37:19
happened 111:11
happens 117:10
happy 10:18 66:25
hardware 106:11,17,18 107:6
hazy 48:22
head 20:8
heading 49:5
Heintz 89:1,6 89:15,19
held 2:13 7:15
help 17:13 106:15
helped 89:12
helpful 89:9
helps 34:1 55:3 68:4
Henderson 7:19
hereinbefore 121:7
hereunto 121:13
hiccup 77:16
hierarchy 46:9
high 74:17 75:15
higher 40:22 70:25 115:6
highlight 9:19 64:13
highly 1:20 2:10 114:9 118:20
history 50:3 62:7 64:2 88:25 94:16
hour 66:23
Houston 4:7
hypothetical 20:22

I

idea 42:16
identification 11:3 12:10
identified 112:16
IEEE 16:19
IETF 16:23 111:15 112:13
Illinois 1:24 2:14 3:7
implemented 91:21 92:13 92:15 93:4 95:11
important 29:18 51:5 60:23 81:18 86:6 87:6 90:4 96:2 100:11 114:20
improves 68:4 68:15
in-line 36:16 36:22 37:5 37:10 38:11 38:24 68:5 68:15 69:9 71:10
in-line' 36:12
include 15:6 33:16 38:15 38:23 51:22 60:7 73:4,10 73:21 74:3 74:24 75:2 76:6 94:14 94:16 95:3
included 29:6 73:16 94:7 94:11
includes 36:4 86:13
including 33:6 35:9
incorporated 111:17
individual 46:2
inelegance 72:9
inertia 113:22
InfoExpress 1:7,13 3:3 7:5,6 8:8

InfoExpress' 10:20
InfoExpress's 6:11
informal 20:21 20:22 44:13 45:3
informally 19:24 40:21 42:14 57:3
information 23:16,17 55:10 79:16 80:24 102:24 103:1,14,17 103:18 104:16 116:22
initial 41:10
inside 26:12 29:18 73:16 103:21
inspection 28:6
instance 43:10 110:18 113:5 116:7
intended 105:19
intentionally 115:21 116:13 117:5
interface 48:6
interfaces 47:21 49:2
interject 66:22
Internet 16:23
interoperabi... 110:14,15 113:16
interoperable 109:20
interplay 16:1 17:1,3,8
interpret 42:4 62:3 76:14
intrinsic 53:2 62:5 86:13 94:12,13,18 94:20
introduce 7:21
invented 85:6 85:19 87:7,9 87:12 88:22 96:8 104:11 104:23 107:17 117:15
invention 28:19 29:22 30:1,13 31:3 34:5 38:13 38:20 61:9 62:20 68:4 68:14 69:3 71:5 81:6 82:22,25 85:11
inventions 81:4
involve 84:7 97:14 107:4
involved 15:22 18:17 26:3 56:7 57:8 76:2 89:11
involves 54:24
involving 15:2 15:11 18:14
issue 90:11
issued 11:10

J

January 14:15
Joe 7:17
join 14:13
joined 14:10 14:14
joining 9:3,3,5
Joseph 3:9 5:12 9:9
joseph.kuo... 3:10
jumped 77:14

K

keenly 40:19
keep 19:12 65:8 109:10
key 26:25 39:11,12 44:19
keys 117:4,4
kind 9:17 12:11 15:11 17:2,21 20:3 20:7,8,20,21 20:22 21:15 22:14,15 23:10,17 28:4,11,11 40:21 44:21 45:25 46:13 48:9,25 50:5 50:7 56:16 57:16 69:5 76:1 77:14 77:16 86:16 86:17 87:21 88:8 110:2 112:8 113:14 114:23 117:9
know 9:3,16 9:17,19,24 11:7 12:12 12:17 19:21 22:18 23:21 25:5 31:10 34:18 42:23 49:6 50:20 51:8 52:16 54:19 61:10 61:19,21 62:24 64:9 65:3,14,18 66:8,23 67:13,17 69:12 73:19 74:2 77:15 86:21 90:19 90:21 96:12 100:21 101:19 102:12,16 105:6 108:9 109:10 110:23 113:9 113:20 114:17 118:9 118:12 119:4
knowing 117:10
knowledge 13:24 31:17 60:17 121:11
known 28:21 28:25 30:4 32:8 34:8 49:21 50:17 50:24 51:1 51:18 65:11 71:3,9 88:17 116:7,14 117:1
Kuo 3:9 9:9

L

label 17:4
LAN 17:21 19:8,16 21:12 26:12 26:24 44:7 58:4 59:4,10 115:2
language 43:9 61:12 64:11 77:8,11 82:12 84:6 86:15 96:11 97:15 107:16
LANs 16:9 17:18 18:2
laptop 93:13 95:4 96:14 96:23 97:4 97:24 98:24 99:23
largely 22:8
law 8:4,7
lawyer 82:11 94:14 102:6 102:7,15 113:7
layer 17:2 18:15,15 19:17 22:14 22:15 23:16 23:16 40:25 93:14 95:14 97:5
legal 7:20 102:5
less-restrict... 24:6
let's 14:12 20:16 23:20 46:20 49:4 54:12 66:20 67:4,25 78:8 88:2,14 89:12 102:20 104:13 118:14,20
level 33:5,12 35:8 40:22

70:25 74:17 75:15 115:7
levels 26:2
leverages 117:16
lies 81:6 82:25
light 80:21 86:12 88:21 90:12 96:5 107:15
limitations 40:20
limited 31:23 31:24 32:4 33:1,2 39:24
line 12:25 13:1 24:15 30:24 36:3,24 37:2 37:17,21 38:4,16 39:4 39:4,8 52:13 68:6 69:6,22 70:6,9,13,16 70:23,24 71:15 87:2,5 87:9,11,21 87:22,24 96:19 104:9 104:25 120:9
lines 20:3 25:4 41:22 57:13
linguist 102:15
list 25:2 66:1 73:4 78:15
listed 120:8
lists 11:20 84:11
literature 31:9 32:17 50:6 51:24 64:15 90:21
little 13:8 16:16 17:11 26:10,19 30:20 41:17 48:22,25 54:22 68:2,8 72:4 77:15 77:17 88:4,8 89:10 117:2
LLP 3:5,13 4:5 4:13
loaded 10:24
local 17:19 18:3 93:11 93:22,24 94:2,3,5 95:19 97:2
Logan 4:9 6:4 7:24,24 8:19 52:3 61:13 63:1 65:6,23 66:18 67:12 105:3 107:21 108:6 116:1 117:19 118:4 119:4,14,17
Logan's 89:6
logging 47:22
logical 17:25 18:1,8 19:16 23:12,17 26:12 44:10 84:9
logically 17:20 19:6 26:21
long 41:17 62:17 83:13
look 12:15 16:7,17 44:19,20 47:4 48:21 56:8 69:5 77:20 87:17 112:2,11 117:12
looked 27:1 57:7 94:19
looking 15:18 15:20,25 17:1,8 28:1 37:3,25 40:13 43:8 48:19 56:14 57:14 60:12 78:12 84:16 107:2 117:9
looks 60:24
lot 18:17 27:7

M

M 3:9
M-a-n-n 91:8
Mac 38:3
machine 107:11
maintain 113:23
maintains 102:24 103:14
malfunctions 89:7
management 16:2 47:20 48:6 91:21 92:3,23 95:12
manifest 76:25
manipulate 48:4
manipulating 84:12
Mann 91:7,19 92:12,18,25 93:3 96:21 97:2,23 98:22 99:24 101:10
manually 48:17
mark 21:8
marked 11:2 12:9
Market 3:15
marks 25:5
materials 32:18
matter 7:5 11:8 121:11
mean 17:15 18:5 24:12 24:24 25:13 30:21 33:13 41:18 42:6 43:5 50:13 51:9 53:10 55:5 56:20 66:21 68:23 70:16 74:22 82:16 102:23 103:8,13
meaning 38:15 38:22 44:21 49:15 53:20 54:11 72:17 72:21 73:2 78:11,14,24 79:7,13 85:21 86:3,4 86:8,12 88:17 92:1 92:21 93:8 93:19 95:2 95:24 96:4,5 97:9,14,21 97:25 98:12 98:17,19 99:1,7,9,18 99:22 100:7 100:14,15,25 101:11 102:5 107:19
meanings 44:2
means 41:24 44:13 54:8 56:18 65:3 87:3 88:23 102:2,10
meant 45:1 52:2,21 116:13
mechanics 113:8
mechanism 112:24 113:2 115:13
mechanisms 48:5,22
meet 81:23 105:8
meeting 39:15
meets 80:4 81:9
memorized 77:22
memory 26:19 109:16
mental 50:7 61:5
mention 18:4 24:15 29:9 35:19 36:18 62:9 88:25 115:1
mentioned 13:22 16:13 31:4 54:23 69:11,12 115:6
mentions 37:25 43:12
Merit 2:16 121:4
messages

114:24
messaging 115:15
methods 31:16
metrics 80:2,5
Michael 1:25 2:15 7:17 121:3,19
Microsystems 15:16 40:19 47:13
middle 23:25 93:11
mind 22:20 31:19
minute 105:4
minutes 67:1,1
misstatement 96:17 106:25
Misstates 100:1
misstating 76:8 95:6 99:3
misunderstо... 10:7
mode 93:11,22 94:2,5 95:19 95:20 97:2
model 61:5
models 50:7
modes 93:24
modifications 16:21 111:14
module 42:18 48:14 84:2
morning 8:20
Morris 5:5 8:4
move 66:20 67:25 85:13 102:20
multiple 19:2 19:14 26:2 28:1 46:12 66:5 77:9

N

N 3:1 4:1 5:1 6:1 7:1
name 7:17 8:21,22 11:8 17:25
names 38:2
nature 115:20
NE 5:6
necessarily 32:22 39:3 52:17 56:1 57:19,23 58:7 60:8 61:22 63:13 64:17 75:2 76:5
necessary 77:10
need 9:22 41:2 67:2 76:21 76:24 80:7 80:18,23 81:15 82:11 113:21 117:11 118:5 118:14
needed 74:7 75:7,12 103:1,18
needs 39:4,16 56:3 81:21 83:8,19 84:25
Neon 15:18
network 15:6 15:21 16:2 17:19 19:1 19:17 22:6 22:12,17 23:3,12,19 24:8 25:11 25:18 26:2 27:9,13,14 27:14 29:2 33:7 35:10 41:12 46:10 48:24 54:3 54:24 55:9 55:13,15,18 55:25 56:1,5 56:6,7,9,16 57:2,4,11,14 57:20,22,23 57:25 58:17 58:25 59:3,3 59:9,20 63:11 64:21 75:25 76:20 80:14 89:11 89:20 90:7 93:24 95:19
network's 81:9 81:23,25
networking 15:20 54:24
networks 18:3 19:7 23:19 28:21 30:3 30:16 32:8 34:7 45:19 53:5,14,22 54:7,25 55:4 55:7 56:10 56:20,20 58:7,9,11,14 60:13
new 114:1 116:18
newly 111:12
nice 14:3
niche 112:11
nominal 23:8
nominally 26:20 43:24 44:9 58:3 115:10
nonresponsi... 52:4 61:14 63:2 65:7,24 66:19 99:14 117:20
North 3:6 4:14
Northern 1:3 7:8
Notarial 121:14
Notary 8:15 121:20
note 41:21 85:8
noted 29:7
notes 121:10
notice 2:15
noting 56:23
notion 16:8 18:8 19:15 22:7,21 23:8 25:20 26:10 26:18,20 37:19 38:2 40:23 42:15 42:24 43:24 44:3,9 47:18 48:12 50:4 52:12 55:14 58:3 69:3,8 69:13 70:5 74:12,14 80:1 84:2 85:9 92:11 93:23 95:12 105:23 111:6 117:3
Notre 13:25 14:8,10,13 14:14
novelties 39:11
novelty 39:3
November 121:23
nuance 43:1 63:16 75:14 77:7 82:6 84:5 96:7 115:16
nuances 112:10
number 109:9
numerous 20:14 39:23

O

O 7:1
O'Connor 1:25 2:16 7:17 121:3,19
Oakland 1:4 7:9
oath 8:11
object 19:4 23:4 26:8 29:3 32:1 45:6 47:11 50:19 52:9 53:24 54:21 56:2 60:9 63:15 64:23 66:14 70:1 70:17 71:11 71:20 72:23 73:12,22 74:20 76:7 78:1,25 79:23 80:19 81:17 83:11 85:2,16

90:18 92:4 92:24 96:1 99:13 101:22 102:3 103:10 103:25 104:17 105:10,21 106:6,12,24 107:12 110:21 112:1 113:12 114:19 116:9
objection 51:2 51:20 52:3 58:12 61:13 63:1 65:6,20 65:23 66:18 74:5 75:4 79:8 83:22 95:5 96:16 96:25 97:11 98:1 99:2,25 101:12 104:4 117:19
obtain 80:2,5,8 80:23
obtaining 80:1 81:1 103:17
obtains 102:24 103:14 104:16
occurred 111:12
occurs 116:23
offer 26:14 27:5 28:4 39:8 40:14 40:21 91:4
offered 11:21 26:16 39:15
offices 9:6
oftentimes 56:8 112:10 115:16
Oh 66:25
okay 11:4,16 12:18 13:16 23:23 46:19 67:1,4 68:12 68:21 98:9 113:9 116:1
once 110:12
one's 60:17
ones 31:4
onward 95:18
open 10:25 11:5 49:2
operability 113:18
operate 16:18 39:5 113:16 114:5
operates 39:2 93:12 97:4 99:23
operating 20:21 93:23 96:14,23 97:23 98:23
operator 7:18
opine 32:15 78:3
opined 31:20 77:24 86:1
opining 43:19 78:2
opinion 13:4,6 32:19,21,24 34:3 49:12 49:18,19,20 50:16,25 60:19 61:9 61:16,18 62:21 64:8 64:16 65:18 66:9 69:23 71:8 72:11 72:18 76:4 78:5,9,19 79:21 80:15 81:13 83:4 83:15 88:15 88:18,19 91:4 98:9,11 99:16,20 103:9 114:3 116:4,6
opinions 11:21 77:23 82:8
opposed 19:25 23:9 32:16 87:10
optional 117:7
optionality 117:10
Oracle 47:9,13 47:14
order 39:5 74:6,9 76:13 80:8,22 82:5 119:6
orders 119:3
ordinary 38:14 38:22 42:3 49:15 72:16 72:21 73:2 74:1 75:1 78:11,13,24 79:7,12 80:16 85:21 86:2,3,8,12 88:17 92:1 92:21 93:19 94:9 95:2,24 96:4,5 97:9 97:14,21,25 98:12,17,19 98:25 99:7,9 99:17,22 100:7,13,15 100:25 101:11 103:8 107:19
organization 16:14,22 28:13 39:16
organizational 55:20 80:13
organizations 17:7
originally 14:10
out-of-band 68:16,22
outline 37:23 116:25
outlined 31:14
outlines 114:23
outside 102:17
overall 28:11 55:23 105:18 112:19
overarching 28:10
overview 29:16 33:22

P

P 3:1,1 4:1,1 5:1,1 7:1
p.m 67:7,8,9 67:11 108:1 108:2,3,5 119:1,21
packet 21:8
packets 21:2
page 6:2,8 23:20,25 24:5 33:4,10 33:10 49:8,9 68:3,18 78:8 80:1 88:3,6 88:12 108:8 109:5,12 120:9
pains 120:18
paragraph 11:20 12:4 12:20 13:2,7 13:12,22 14:24 15:4 28:16 29:9 29:10 31:1 31:23 33:4 33:18 36:19 39:21 41:5 49:4,12 53:1 59:14,15 63:5 66:3,20 68:1,2,11,13 71:2 72:14 78:9 79:14 79:25 80:25 81:5 88:2,6 88:13,24 89:14,19 90:6 91:6 95:18 102:21 102:21 103:24 104:14 105:9 105:12 108:8 108:25 109:5 109:7,9,12 109:19 112:22 114:13
paragraphs 13:18
parsing 63:16
part 14:19 15:16,21 19:8 23:12

29:15 32:22 33:21 35:4 37:9 40:19 47:23 48:6 77:12,18,21 78:6,19,21 94:8,12,17 94:24 106:2 106:16 112:14,17
particular 15:5 16:11,19 17:22 19:11 19:17 20:4 21:1 29:9,25 33:21 35:4 38:1,6 42:11 42:11 45:15 45:20 47:3 48:6 50:2 52:25 54:2,2 54:3 55:9,13 57:7 60:12 71:1 74:8 75:8,16 76:19 80:9 82:15 84:13 92:17 94:3,5 95:17,21 96:9 107:8 112:11 115:19
particularly 40:24 96:7
partition 17:20 19:7 20:21
partitioned 18:11 19:2
partitioning 25:20 26:6 44:12
partitions 18:2 18:4,6 19:18 19:20,22 20:17,17 22:3,4 45:4
parts 19:13 33:25 41:16 48:8 61:4 114:7
pass 69:14 117:23
passed 41:11
passes 69:6 87:24
passing 69:16
passwords 38:3
pasted 69:12
patent 6:14 12:6,13 24:14 25:4,7 25:8,17 29:6 29:6,12 31:5 31:14,15 35:2 37:7,18 37:22 38:5 39:2,12 40:7 43:8,14,21 44:25 45:22 47:3 48:12 48:12 49:25 52:6,11,19 63:23 64:25 70:4,7 71:13 74:15 80:3 83:24 89:2 90:25 94:5 95:21
patents 11:20 11:25 12:16 12:23 28:18 29:17,20 33:22,23 34:25 35:6 37:1,16 38:13,21 39:20 41:7 42:14 43:14 49:22 50:18 51:16 62:7 69:24 70:14 71:17 93:7,7 113:5
patents' 82:24
Patrick 4:17 8:1
PClark@win... 4:18
Peachtree 5:6
PEAP 115:6
Pearl 4:14
penalties 120:18
Pennsylvania 3:16
percent 85:24 91:13
perfectly 11:17
perform 80:18 80:22 92:9
perimeter 89:20 90:7
perjury 120:19
permutations 77:9
person 41:24 42:3 74:1,25 80:16 94:9 103:8
personal 29:13 93:14 97:6 110:6
Ph.D 1:23 2:13 6:3,10 8:13 120:3,23 121:6
Philadelphia 3:16
phrase 19:19 45:8,10,11 81:19
physical 17:24 44:4,6
picture 73:15
piece 91:7
pieces 20:4 50:6 51:24 51:25 62:5 62:10 64:1,5 64:15
pitfalls 37:8
place 21:3 41:3 55:21 76:2
placement 52:25
places 21:13
plain 49:15 64:11 72:16 72:20 73:1 78:10,13,24 79:6,12 85:21 86:2,3 86:8,12 88:17 92:1 92:20 93:19 95:2,23 96:3 96:4 97:9,13 97:21,24 98:12,16,19 98:25 99:6,9 99:17,22 100:4,7,13 100:15,24 101:10 107:19
Plaintiff 1:8,14 8:8
play 76:11
please 7:21 8:11,20 10:8 12:17 65:18 66:12 119:3
pleasure 117:23
plus 28:9
point 9:22 12:14 27:8 30:18 41:9 42:16,18 44:9,16,17 81:8,16,21 84:3,13 85:1 85:7,14 86:5 86:22 87:4 87:13,14,23 104:7,15
pointing 72:8
points 21:17 56:25 58:5 58:19 70:24 83:9,20
policies 40:24 55:20 74:10 75:12,19 76:11,23
policy 28:11 35:22 36:7 59:19 60:5 63:10 64:20 73:5,5 74:9 74:11,19,22 74:25 75:3,6 75:11,21 76:6,14,18 76:22 79:17 80:11,13 81:2 82:1 84:16,17,20
poorly 9:21
port 41:9,18 41:25 42:5 43:4,5,7,24 43:25,25

44:3,21 45:1 45:15,24,24 46:2,5,11,21 46:22,25 47:6,18 48:9 113:10
port-based 112:24 113:2
portion 89:5 89:18
ports 43:12,17 43:20 44:6 45:5,12 46:15 81:8 81:16,22 83:9,20 84:4 84:8,8,9,9 89:11
POSA 42:21 44:22 60:17 60:25 61:9 62:3,11,13 62:21 64:9 65:1
POSITA 38:14 38:21 43:16 49:12 50:9 51:4,8 52:1 52:20 69:24 70:3,15 73:19 76:4 77:2,4 78:11 79:11,21 81:14 82:8 82:14 83:5 83:16 84:24 85:3,20 86:9 92:20,25 95:22 96:13 97:7 116:6 116:14,17
possibly 86:18
posture 76:16
potentially 18:14 23:13 26:23 58:24 84:8 87:22 87:22
precise 39:5
precisely 106:14
precursor 17:8
predetermin... 35:22 36:6
prelude 112:6
present 5:12 68:4,14 74:18 81:3 103:21 104:9 105:17,24 110:8
presenting 29:16
preshared 44:19
pretending 102:7
pretty 69:17
previous 50:22 108:22
pricing 47:15
primary 20:9
principles 110:10
printed 11:13
prior 16:4 28:18 29:22 29:22 30:1 31:3 32:17 34:5 35:1,17 36:22 37:9 37:25 41:8 52:12 62:18 67:15 69:1 70:19 71:4 71:10,14 79:24 83:6 83:17 85:9 85:18 87:1 87:14,18 91:7 99:19 104:9 118:11
priority 12:22 13:10,18,21 13:22 36:25 37:15
private 117:4
probably 9:16 9:20 36:8 102:5
problem 109:15
problems 112:16
procedures 9:18
process 48:17 112:20
processors 15:21 48:24
produced 10:12,19
professional 29:13
professor 13:25 14:4,5 14:7,18
prohibitive 39:9
Project 15:18
projects 15:2 15:11
pronounce 114:21
propose 112:14
proposed 6:12 10:20 62:20 111:16
prosecution 50:3 62:6 64:1 88:25 91:11,15 94:16
protect 55:1 55:15 57:2 57:21 59:9 76:1
protected 24:8 25:11 28:20 30:3,15 32:7 34:7 41:12 53:5,14,22 54:7 55:4,7 55:14,19,25 56:19 57:1 57:22 58:15 60:13 76:20
protecting 55:13 75:25 80:14
protection 55:24
protocol 114:23 115:19,22 116:18
protocols 48:1 56:13 59:3 115:5,7 117:6
provide 25:19 58:19 92:16 111:9
provided 11:14 32:19 52:18 65:10
provides 95:15 104:23
providing 33:22 92:14 106:1
provision 89:21 90:8
provisional 80:3
PSTN 57:13
public 8:15 57:13 117:4 121:20
publication 92:17 93:3
published 111:24
pure 56:9 57:11,15
purposes 51:6 75:10 85:22 102:7 119:18
pursuant 2:15
put 12:12 25:23 37:20 66:1 70:9 91:12 99:17 103:23 105:8 119:5
putting 37:9

Q

quasi 28:4
question 9:22 12:21 16:17 20:19 27:23 30:19 31:6 32:14 37:13 38:17 44:5 50:16,23 51:22 60:20 61:21,25 63:4,12,18 65:17,22 66:13,16,17 72:10 73:24 75:5 76:10 79:2 80:20

83:13,24 85:13 97:18 98:2 99:5,12 99:21 100:3 100:8,19 101:6,16,21 101:25 106:7 109:9
questioning 96:19 104:25
questions 9:20 61:18 67:23 106:20
quite 32:13 33:1 91:1 98:7
quotation 25:5
quote 25:6 91:20

R

R 3:1 4:1 5:1 7:1 120:1,1 121:1
radius 115:14
rate 26:21
ratification 112:20
rationale 35:1
reach 84:18 97:20 99:16 110:11
reached 78:22 79:4
reaching 78:19 99:20
read 25:7 42:21 44:24 50:11,11 60:24 62:14 65:2 92:7 93:6 108:23 118:1 120:4
readily 102:22
reading 13:13 42:22 51:7,7 52:22 60:14 60:25 61:7,8 61:11 64:10 92:25 93:1,7 110:4
reaffirming 88:15
real 65:17
realize 10:6
really 56:3 61:17,19
Realtime 2:17 2:18 121:4
reask 50:14
reason 12:15
reasonable 39:17,18 49:14 61:10 64:9 65:4,12 73:20 74:2 79:11 86:11 86:21 96:12 98:21 101:21 101:24 102:2 102:5,10,14 102:18
reasonably 53:15 114:2
reasons 111:3
recall 12:1 16:11 78:2 86:17
receive 46:11
Recess 67:8 108:2
recited 89:2
recites 70:10
recognize 11:6
recognizing 102:17
reconfigurat... 42:15,16 47:6 74:14 84:7
reconfigure 41:25 74:13 81:7,15,21 83:9,20 84:2 85:1,7
reconfigured 46:22 47:1
reconfiguring 41:8,17 42:5 42:18 48:13 84:13
reconvening 67:9 108:3
record 8:21 67:6,11 105:1 108:1 108:5 116:3 118:3,23,25 120:7 121:9
redirect 117:25
redirection 28:4
refer 11:16 59:16 60:3 60:11 61:20 61:22 63:7 65:13 66:5
reference 53:3 95:6 99:3 100:1
references 50:2 94:13 94:14,17,20
referencing 33:15
referred 36:12 72:13 92:18
referring 14:9 55:6 68:18 73:14 85:17 85:18
refers 53:3 64:17
reflected 25:3 48:11 68:24
reflection 10:3
regard 70:23 72:11 78:5 80:3 107:14
regarding 78:9 102:24 103:15
regards 17:6 20:25 23:5 23:15 30:1 32:15,17 35:17 42:10 48:7 49:25 54:3 55:2 62:18 63:17 74:15 75:24 76:12,24 82:15 86:8 87:8 88:20 96:8 103:17 106:9 110:13 113:15
Registered 2:16 121:3
relationship 46:1
relevant 33:24 34:16 43:13 77:8 89:1 114:9
remain 114:7 114:11
remarkably 117:17
remember 91:13 112:8 114:21
REMOTE 1:22 2:12
remotely 3:4 3:12 4:4,12 5:4 7:16 9:4 74:12
repeat 38:17 73:23 79:1 83:12 86:18
repeated 86:17
repeating 113:14
report 10:13 10:23 13:6 14:16 19:25 21:17 23:21 29:16 30:18 30:25 31:13 31:21,22 33:21,25 34:10,17,25 35:5,16 36:18 39:7 42:10,25 43:10,19 49:24 51:4 51:23 52:10 60:6 61:2 62:1 63:5,22 65:5 71:12 78:3,12 79:10 82:19 85:8 89:18 91:14 100:4 100:14 102:11 105:16 108:8 111:2,5,22 113:14,17 116:11,25 117:8

reporter 1:25 2:16,17 7:16 8:11 118:17 119:2,16 121:4
Reporter/Ce... 121:4
represent 7:23
representing 8:8
required 39:24
research 15:23 30:12
reserve 10:2
residing 69:21
resiliency 46:17
resources 59:21 63:11 64:21
respect 69:18 75:23 76:18 78:4 80:12 84:1 86:15
respective 42:17 51:11 58:20 68:25 73:17 75:9 75:20 76:23 81:3 96:6 110:12,25 117:18
rest 34:16
restate 96:20
restating 35:14
restricted 24:7 24:17,17 25:9,10,21 25:22 41:12 42:24 43:1,2 76:20 105:25 107:4
restricting 55:12
results 84:14
review 31:9 108:19
reviewed 77:12,18 79:9 108:16 110:2,17 111:19
revision 114:1
rides 114:11
riffing 31:11
right 10:2,24 12:7 14:1,17 15:3,14 19:3 24:3 30:7 31:18,25 33:4 34:8,12 46:3 49:5 51:1 54:13 56:1 58:11 65:10 67:17 68:10,19 75:11 77:13 78:11,20,24 82:9,22 83:2 88:5,10,18 89:10,12 94:10 98:13 101:2 102:20 105:5 107:21 108:17 116:1 118:6
rise 18:20
RMR 1:25 121:19
road 116:20
robustness 46:18
role 37:6,10 52:25 61:6 62:12
roles 27:2
room 9:7,8
rough 15:18 119:5,9,12
router 48:4 103:24 104:2 104:7
routers 15:7 16:1 18:16 56:24 58:6 58:18
routing 46:17
rules 9:18 18:23
run 107:5
running 95:3 105:23 106:19 107:3 107:4 116:16

S

S 3:1 4:1 5:1 6:7 7:1
S-t-r-i-e-g-e-l 8:23
Saul 3:5,13 8:7 9:6
saying 25:6 32:3,25 46:24 52:17 52:18 53:19 54:15 65:16 104:1 105:7
says 24:5 32:5 33:19 39:22 41:7 49:6,12 59:16 61:20 66:4 68:14 79:15 83:1 89:18 91:14 91:20 93:11 99:3 102:21 108:11 109:19
scale 38:4
school 14:3
Schwerin 3:18 8:6,6 9:9 19:4 23:4 26:8 29:3 32:1 45:6 47:11 50:19 51:2,20 52:9 53:24 54:21 56:2 58:12 60:9 63:15 64:23 65:20 66:14 70:1 70:17 71:11 71:20 72:23 73:12,22 74:5,20 75:4 76:7 78:1,25 79:8,23 80:19 81:17 83:11,22 85:2,16 86:25 90:3 90:18 92:4 92:24 95:5 96:1,16,25 97:11 98:1 99:2,25 101:12,22 102:3 103:10 103:25 104:4 104:17,24 105:10,21 106:6,12,24 107:12,24 110:21 112:1 113:12 114:19 115:24 116:9 117:25 118:9 118:19,24 119:8
science 14:6,8
scope 34:3 49:13 50:12 51:5 52:23 57:24 60:15 62:15 64:12 86:10 95:2 95:23 97:24 98:15,24 100:4 101:10
scratch 58:16
Seal 121:14
second 7:11 13:1 14:12 46:23 47:2 105:1
section 28:17 102:13
sections 110:19
secure 33:7 35:10
security 28:11 28:12 35:22 36:7 39:16 59:12,19 60:5 63:9 64:20 73:5 74:9,10 75:11,19,20 76:11,14,23 79:17 80:10 81:2,10,23 81:25 82:1 84:16,19 89:20 90:8 91:21 92:2 92:22 93:13 95:12,13 97:5
see 11:22,23 12:8,24 13:3

13:11,16 16:19,21,25 17:5 23:1,25 24:1,9,10,15 24:15,21,22 25:3,8 28:22 28:23 33:3,8 33:9 34:1 35:23,24 36:2,14,15 40:2,3,5 41:13 42:4 43:23,23 46:2 48:11 49:9,10,16 49:17 53:7 59:22,23 62:22 64:14 68:7,17,21 68:24 69:15 71:6 73:7 74:8 78:16 79:18,24 81:11 82:23 83:3 87:16 87:18,23 89:3,4,12,15 89:23 91:8 91:23 93:16 102:1 103:2 108:14 109:3 109:22 112:25 113:14 114:14 115:1 118:13
seeing 117:13
seen 18:20 51:23 70:4 111:14 116:15
segment 29:1
segments 19:2
send 28:5
sense 30:9 46:24 53:21 54:4 56:22 58:24 60:12 67:20 74:21 76:13 90:20 110:24 112:2
sensitive 55:9
sentence 24:25 31:2 35:19 36:11 49:11 53:13 54:1 59:15 63:6 74:23 79:15 93:10 108:11
sentences 14:25
separate 19:6
separation 17:22 26:23
September 12:23
sequence 115:15 116:22,25
server 105:20 105:24
servers 106:1
services 7:20 55:10 57:10 57:19 84:18
session 44:18
set 17:24,25 18:10 19:11 21:1 25:23 25:24 46:11 109:1 121:7 121:14
setting 47:18
settings 20:13
setup 19:17 44:15
share 10:25 11:25 12:6
shared 75:10
sharing 34:19
shortcomings 41:8
shortly 12:13 36:3
show 73:13,15
showing 45:23
shown 63:5 69:10 87:19 87:20
shows 13:15 13:19 36:21 45:22 47:5
side 77:15,16
sign 118:1
Signed 120:18
significant 113:20
signs 117:3
similar 22:5 26:5 45:25 56:16
similarly 35:7
simple 61:21 65:17 99:21
single 19:14 39:22
SIP 57:17
sir 11:18
sit 31:18 72:7
sitting 87:5,20
situation 68:16
six 11:20
skill 41:24 42:3 74:2 75:1 80:16 94:9 103:8 121:11
skip 88:2
slightly 37:13
smarter 27:10
software 15:20 89:21 90:2,9 91:22 92:3 92:23 95:3 95:13 106:5 106:9,11,17 106:19,22 107:5,5
solution 59:13
solutions 92:16
solved 41:7
somebody 119:7
somewhat 22:2
sooner 47:16
sophistication 39:25 40:16 41:2
sorry 26:9 30:21 68:8 70:2 73:23 77:14 86:16 109:8
sort 20:14,20 23:24 37:8 44:9,14 61:5 106:19 107:6 113:21 115:19 117:12
sorts 112:12
Sounds 67:4
source 35:13
space 53:4,10 53:14,21 54:2,3 59:10 60:13 71:1
speaking 19:23 26:20 42:13
specialized 21:12
specific 14:9 19:25 23:10 27:4 30:17 32:21,24 37:10,23 42:12 45:8 47:5 77:7 78:8 82:5 84:17 102:12
specifically 18:2 22:19 31:5 37:7 43:12,19 64:13 113:18 114:8
specification 11:25 12:2,7 24:14,18 25:2 29:5,19 29:21 31:15 31:25 32:9 32:11 33:16 33:17,19,24 34:12,15,20 34:24 35:5 35:11,12,15 36:3,4 37:4 40:4,7,10 41:1 42:20 43:8 44:24 45:23 50:11 51:6,7,10,15 52:2,11,22 54:6 58:3,23 60:14,16,24 61:1,8,11 62:3,14,23 64:10 65:1,3 68:25 70:5,7

71:13 72:15 72:25 77:6 77:11 80:21 81:20 82:7 82:13,21,24 83:6,17,25 84:7 85:5 86:14 87:17 88:21 90:12 91:1,2 92:7 93:1,6 94:22 95:9,10 96:6 96:10 97:15 98:15,18 99:8,19 100:6,12,16 100:23 105:16,22 107:16 117:8
specifics 115:16
speeding 88:8
spelled 89:16
spot 30:17
Square 3:14
SSH 48:2
stance 28:12
stand 50:21 64:8
standard 16:13,15 108:13,17 109:20 110:12,16,18 111:13,18 112:18,21,23 114:1 116:8 119:14
standards 16:8,12,20 110:2,4,25 112:3,3,5,7 112:19 113:16 117:18
stands 17:18
start 28:1
started 16:5
starts 68:9
state 7:22 8:21 12:5 34:14 60:6 71:3
stated 111:21
statement 12:21 29:11 29:24,25 34:11,19,22 35:7,13 36:1 39:22 40:8 41:6 63:4 66:3 68:13 103:5 116:11
statements 109:13
States 1:2 7:8
stay 109:13 117:14
stayed 111:8 111:10 114:4 117:17
staying 30:24
stenotype 121:10
stick 118:12
stock 47:15
Strawn 4:5,13 7:25 8:2
streamline 12:12
Street 3:6,15 4:6,14 5:6
strictly 28:9 29:12 31:22 31:24
Striegel 1:23 2:13 6:3,10 7:4 8:13,22 8:24 9:2,13 10:12 11:19 67:13 108:7 116:5 118:10 120:3,23 121:6
struggling 106:20
subject 55:20 57:5 82:4
subset 21:18 21:21,23 22:7,19,23 23:6,13 24:6 24:7,11,17 24:17 25:9 25:10,13,22 25:22 26:22 41:12 42:25 43:1,2 76:21 105:25 107:4
subsets 22:5 23:2 26:4
Suite 3:6 4:6 4:14 5:6
summarizing 33:19
Sun 15:16 40:19 47:13 48:20 118:11
supplicant 111:7 115:9
support 6:11 10:20 39:23 93:24
suppose 16:14
sure 8:22 9:5 10:11 12:19 30:19,20,23 32:2,3,13,20 33:1 38:18 38:19 45:7 50:15 54:14 60:19 66:25 69:17 73:24 74:1 83:14 83:15 98:5 99:4 101:14 101:17 105:3 106:8 118:7 119:5
survey 32:17 71:22
switch 19:10 20:11 22:13 44:4 48:3 57:14 104:3
switched 57:12
switches 15:8 46:10
switching 17:4
sworn 8:15 121:8
synched 119:19
synchroniza... 93:14,25 95:14 97:6
system 75:9 76:17,21 103:1,19 107:2,7
systems 1:10 4:3 7:6 8:1 59:7 95:15

T

T 6:7 120:1 121:1,1
tag 21:1
tagging 21:2,9
tags 21:7
take 21:2 66:25 75:7,7 75:19 76:14 89:8 100:11 101:2 107:22 119:8
taken 7:5 67:8 108:2 121:10
talk 12:13 15:1 18:7,8,9,15 42:25 43:3 43:11 53:13 62:8 63:22 112:23 114:14
talked 25:20 26:9 30:10 34:4 44:25 45:2 69:7 74:13 75:24 79:2 84:1 87:25 92:5 95:8 111:14 112:13 117:2
talking 10:7 16:19 23:9 33:21 38:1 42:24 48:18 75:15 80:2 93:22 117:23 118:11
talks 48:12 92:10 95:11 102:13 105:23
tandem 77:11
Task 16:24
tasks 80:23
teach 20:2
teaches 39:12
techniques 18:12
technology 53:4,10,13 53:21

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 421 of 1144
INFOEXPRESS, INC. - EX2572

telephone 57:14
telephony 54:13,15,16 54:20,23,23 54:25 55:2 57:11,15
tell 18:25 101:20 106:15 113:8
telling 116:5
Telnet 48:1
Ten 67:1
term 13:9,18 15:25 21:16 21:17,20 24:22 26:22 37:5 44:13 49:13,21,23 50:12,17 51:1,18,18 60:10 61:3 62:22 64:6 64:13 79:5 86:10 90:13 90:22 92:6 93:2 94:10 94:21 95:24 97:9,25 98:13 104:1 107:20
termed 40:11
terms 16:2 17:13,16,17 18:21 20:9 21:7 22:20 24:16 27:2 29:21 31:11 31:15 32:4 32:25 35:18 37:22,24 39:17,18 40:13 44:16 44:19 45:23 46:8,16 48:19 50:7,8 50:9,23 51:6 51:11,24 53:16 56:17 61:4,7 62:5 64:2 69:1 71:22 75:14 75:15 77:7 77:24 78:5,6 78:16 82:15 91:1 92:12 96:3 105:13 110:8,9 112:20 114:5 116:24
testified 8:16
testimony 67:15 76:8 96:17 106:25 120:5,7 121:7,9
testing 109:15
Texas 4:7,15
text 25:3,8 42:23
thank 11:18 55:3 72:8 109:7 117:21
Thanks 86:23
thereto 53:6 53:15
thing 9:18 21:22 28:25 39:12
things 12:12 16:20 18:16 19:11 21:11 21:13 22:17 27:7 35:16 40:23 46:15 48:2 57:12 62:5 66:1 73:5,11,21 74:4,17 83:7 83:18 90:2 90:24 97:19 97:20 99:15 99:19 104:22 115:5 117:7 117:11
think 10:16 12:5 14:24 17:23 21:16 26:9 30:7 34:1,13 37:12 38:25 39:1 43:18 47:14 50:22 51:5,21 52:5 54:22 56:3,6 56:16 57:24 60:23 61:24 61:24 65:21 66:15,16 67:3 70:18 81:18 86:6 88:15 90:4 90:13 95:7 96:2 97:1,12 98:2 99:5,11 99:12 100:2 100:10 101:15 103:11 104:5 104:18 107:1 107:13 110:22 113:13 114:20 115:25 116:10 117:12 118:4 119:17
thinking 21:24 31:11 84:9 84:10
third-party 95:14
thought 77:21
threats 111:12
three 14:25 18:15 22:15 23:16
Thursday 2:7
time 7:14,15 10:3 15:19 18:20 28:25 47:9,15,19 48:2,10,19 49:1,3 50:7 51:13,19 57:15 65:25 66:23 71:5 103:9 107:22 115:25 116:15 117:22
timeframe 57:8
timeline 15:14
times 66:5 99:12
timing 105:2 107:23
title 10:17,22 14:10
today 8:1 9:3 9:19 12:12 13:4 67:23 112:9 117:22
Today's 7:13
tools 55:22 93:15 97:6
top 24:5 93:14 97:5,6 114:12,25
totally 38:18 63:18 96:18 97:17
Townsend 5:12 7:18
traffic 28:5 46:12 69:6 87:24
transcript 120:5
transition 18:13
transitions 57:16
traverse 56:16
tremendously 55:3
true 47:8 101:11 105:9 120:6 121:9
trust 91:16 115:17
try 20:8 21:8 22:22 25:18 26:11,21,21 27:4,15 28:5 37:14,20 40:14 41:3 48:4,8 51:13 55:23 63:3 65:25 70:24 72:5 78:7 85:25 88:9 89:13 90:22 96:21 98:10 99:13 104:13 113:23
trying 16:8 19:24 20:1 22:1,4 26:23 27:9 28:14 30:18 38:3 40:20 55:8 55:21 60:18

61:17 62:15 63:17 70:8 70:12 71:22 75:25 84:18 86:17 91:4 92:18 101:19 111:9
turn 23:20 42:23 55:19 56:12 74:11 75:12,18 80:11 81:24 84:12,15,20 84:21 112:17
turnaround 119:15
two 13:17 14:25 18:15 20:16 22:15 23:16 46:20 93:24 110:23 119:16
type 27:14 37:20 38:10 39:1,9,14 40:14 45:18 45:19 56:7 57:17 63:24 70:5,9,12,21 70:25 71:14 74:7 76:12 76:18,19 82:2 84:22 92:16 107:8
types 23:19 26:13 27:5 38:7 40:22 40:25 49:1 52:13 54:6 56:15 58:4 58:22 84:18 90:23 91:3 92:7 94:22 104:20 105:14 114:24 115:3 116:21
typical 59:3 70:19 107:6
typically 16:22 17:2 45:14 107:5 112:15 115:14 116:23
typo 69:15

U

U.S 6:14
undergradu... 20:2
underlying 9:17 110:9
understand 9:22 10:4 12:5 17:14 20:19 22:2,4 25:12 34:2 36:16 42:7 42:22 44:22 44:25 49:13 50:12 51:4 52:1,20,22 53:2,18,20 54:16 59:24 60:19,25 61:15 62:14 62:23 64:11 65:2 72:5 75:2,5 76:3,5 76:9 77:3,4 79:11,21 80:17,20 81:14,19 82:9,11 83:8 83:19 84:25 85:3,21 86:10,19 90:23 92:22 93:2,6,8,19 94:10,13 95:22 97:8 98:4,15 100:12 101:1 101:3,4,6 102:1,4,23 103:13 106:16 113:4 116:4,21
understandi... 11:24 27:23 28:24 37:1 37:16 38:12 38:20 40:13 41:23 50:10 51:17 52:24 59:25 61:4,8 70:11 75:11 82:14 88:22 90:1,12 92:1 92:6 98:25 102:9 103:23 107:10,15,18 107:19 110:6 110:15
understood 18:25 27:18 35:18 38:14 38:22 46:19 69:25 70:4 70:15 83:14
undertaken 70:20
unique 52:6
uniquely 52:19
United 1:2 7:7
unmarked 11:14
upper 40:25
usage 18:19 78:3
use 16:22 18:13,18 19:19 20:5,7 21:6,12 22:3 22:22 23:2 23:15 24:11 24:22 25:23 26:11 27:3 28:3,8 29:1 42:11 45:7 46:8 47:25 48:7 55:23 63:20 90:22 110:24 113:10 114:14,17
user 38:2
user's 30:15
users 40:23
users' 28:20 30:2 32:7 34:6
uses 20:9 43:22
usually 112:15 114:21
utilizing 56:13

V

v 1:9,15 7:6,7
vantage 27:8
variations 116:15
variety 17:10 18:12,19,22 20:6,13,23 21:5,10 27:2 28:2 44:1 74:16 113:19 115:3
various 16:21 16:25 17:3,4 18:21 39:7 39:15,19,19 47:20 64:14 84:19 94:16 109:1 111:14 112:3 115:6
vary 21:3,6
verbiage 42:12
version 38:6 111:23
versions 108:12,17 109:1 110:18 113:10 114:18
versus 17:4,24 25:22 27:11 43:2,25,25 44:18 56:5 62:19 85:10
video 7:18 119:18
videoconfer... 2:14
videoconfer... 56:15
Videographer 5:13 7:3 8:10 67:6,10 107:25 108:4 118:2,22,25
videotaped 1:22 2:12 7:4
view 17:17 22:9 26:22 56:4 57:1,3 58:24 75:8 91:5 92:14
viewed 23:13 56:25 71:14 94:2
viewing 94:4
virtual 16:9

17:18,19 19:16 95:13
virtue 23:10
VLAN 15:1 16:11,13,15 17:1,4,14,18 17:18 18:1 18:18,22 19:2,5,20 20:5,9,16 21:22 22:7 22:19,22,25 23:2,6,7,11 25:23,24,25 26:11,13,16 26:20 27:4 27:20,25 28:9,9 30:14 45:14,16,16 45:23,25 46:3,6,8,21 46:23,25 47:2,7,7,19 48:7,10
VLANs 14:20 15:3,6,11,22 16:1,4,7,18 17:8 18:7,9 18:14 20:7 21:4,6 22:3 22:12 23:9 24:8,20,23 24:25 25:11 25:14 26:2,5 26:7 27:5,17 27:19 28:3 29:1 30:7 45:2,5,13 46:12,17,20 48:13 112:10
voice 56:6,9
VOIP 56:14 57:17

W

wage 109:4
walked 62:2 63:25
want 9:18 30:20 41:15 43:18 44:2 54:22 55:11 57:21 61:20 83:13 92:8 101:17 102:6 104:24 107:23 119:4 119:18
wanted 30:23 57:2 59:1 67:14 73:24
wanting 65:14
wants 56:17 107:1
way 19:22 20:3 20:7,25 21:7 21:15 27:18 37:6 39:17 45:9 52:6 63:19 77:25 86:20 92:14 93:4 111:24 112:8 114:6
ways 18:17,24 20:6,23 21:5 22:11,16,23 25:18 28:3,7
we'll 12:13,17 16:18,20 17:5 66:1 88:9 108:7 109:13 116:2 118:15 119:4 119:8,11
we're 10:7,10 16:19 17:17 23:8 30:23 56:14 57:14 60:12 67:13 75:25 89:14 101:9 109:17 115:25
we've 18:20 22:2 93:9 95:7
weeks 119:16
went 99:20
West 3:14
WHEREOF 121:13
wide 17:10 20:13 21:4 21:10 113:19 115:3
William 4:9 7:24 115:24
window 23:10
Winston 4:5 4:13 7:25 8:2
wireless 27:14 44:7,8,14
wish 55:15 59:9
wished 47:16
witness 117:24 121:7 121:13
witness' 76:8 106:25
WLogan@wi... 4:10
Wood 102:21 103:11
word 60:20 63:20
words 101:5
work 14:19,22 15:12,14,16 15:21,25 30:10,11 40:18 47:9 48:20 115:18 118:11
worked 15:2 15:11 30:6
working 15:17 15:22 16:5 26:17,19 47:17 112:4 112:7,11,15
works 110:10 111:1
worries 88:10
worth 119:19
worthy 112:18
wouldn't 32:23 104:22
wrap 20:8
wrapping 116:2
writing 116:18 117:7
written 91:17
wrong 94:15
wrote 13:5 24:24 65:4 103:11

X

x 1:6,12,18 6:1 6:7

Y

yeah 66:16 105:3 107:24 109:17 119:8 119:11
years 109:2,21 109:25 110:3 110:12,16,25 111:4,18

Z

Zoom 2:13 7:16 88:7 89:6

0

1

1 2:7 6:9 7:13 10:25 11:2 11:20 36:20 36:21 87:18
1:17 67:7,8
1:29 67:9,11
10 85:23
100 91:13
104 91:20 93:12
1075 5:6
109 14:25
11 6:13
11:53 2:8 7:14
110 40:1 87:19
117 109:12,12 109:19
12 6:14
120 87:19
123 108:8
125 112:23
136 114:14
144 108:25 109:5
15 33:4,10
1500 3:15
16 33:10
160 39:24
161 3:6
1700 5:6
18 23:21
19 49:8,9 78:8
19102-2186 3:16
1st 121:14

2

2 6:14 12:9,14 23:24
2:25 108:1,2
2:36 108:3,5
2:49 119:1,21
20 68:9
2001 108:13 110:13,19 114:5
2002 15:15 16:5 26:17 26:18 27:1 30:11 47:10
2003 12:23 14:15 116:6
2004 108:13
2010 108:13
2018 14:18
2020 108:13 110:19 111:20,23 114:6 116:8
2024 2:7 7:13 120:20 121:15
2027 113:6,11 114:1
2029 121:23
2121 4:14
214 4:16
215 3:17
22 68:3,18
24 12:23 89:19 90:6
2400 4:6
253-6982 5:8
29 41:22

3

30 41:22 88:6 118:13
30309 5:7
305A 43:24
305B 43:25
305C 43:25
312 3:8
33 88:3,12
35 13:7,14,15
36 13:15,15
38th 3:15
3A 43:11,23,24 47:5 73:14
3B 43:12 47:5 73:14
3GPP 17:6

4

4:23-cv-002... 1:9 7:11
4:23-cv-004... 1:15 7:12
40 12:4,20 13:2,23
404 5:8
42 28:16 29:11 31:1,24 33:4 34:4
4200 3:6
444 113:5
45 39:21
453-6492 4:16
46 41:6
48 24:16 25:4
484 12:12 25:4 25:8 113:5

5

5 24:16 41:21
50 24:16 25:4 49:4,12 78:9
51 59:15 63:5 66:4 109:12
52 68:1,9
53 66:20 68:11 68:13 108:8
54 71:2
55 72:14
57 73:3
59 79:25

6

60 79:14
60601 3:7
61 81:5
645 89:2
651-2600 4:8
68 109:6

7

7,523,484 6:14
713 4:8
72 88:14
73 88:2,5,6,13 88:24 89:14
74 91:6
75201 4:15
77002-2925 4:7
79 102:21,21 103:24 104:14 105:9

8

8 6:4
800 4:6
802.1X 44:18 108:12 109:2 110:4,7 111:1,9 114:18 116:14,24
876-7100 3:8

9

9 121:23
900 4:14
972-7184 3:17

EXHIBIT T

ATTORNEY DOCKET NO. 09142.0002U1

10/21/03 19569 U.S. PTO

22387 U.S.PTO 60/513080 102103

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a **PROVISIONAL APPLICATION FOR PATENT** under 37 C.F.R. § 1.53(c).

	Docket Number	09142.0002U1	Type a Plus Sign (+) inside this box → → →	+

INVENTOR(s)/APPLICANT(s)

LAST NAME	FIRST NAME	MIDDLE INITIAL	RESIDENCE (City and Either State or Foreign Country)
Lum	Stacey		Los Altos, California
Lee	Alice		Saratoga, California

TITLE OF INVENTION (280 characters max)

GATEKEEPER INVENTION FOR CONTROLLING ACCESS TO A CORPORATE NETWORK USING 802.1x

CORRESPONDENCE ADDRESS

Jennifer Pearson Medlin, Esq.

23859
PATENT TRADEMARK OFFICE

STATE	Georgia	ZIP CODE	30309	COUNTRY	USA

ENCLOSED APPLICATION PARTS (*Check All That Apply*)

- ☐ Provisional Application Title Page — *Number of pages* [ ]
- ☒ Specification, including claims and figures — *Number of pages* [**12**]
- ☒ Appendix — *Number of pages* [**7**]
- ☒ Credit Card Payment Authorization Form PTO-2038 for $80.00 for filing fee
- ☒ Other (Specify): Return Postcard

192479

ATTORNEY DOCKET NO. 09142.0002U1

METHOD PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT (*Check One*)			
☒	A Credit Card Payment Authorization Form PTO-2038 is enclosed to cover the filing fees.	**FILING FEE AMOUNT**	**$80.00**
☐	The Commissioner is hereby authorized to charge filing fees and credit Deposit Account Number:		
☒	The Commissioner is hereby authorized to charge any additional fees which may be required in connection with the following or credit any overpayment to Deposit Account No. 14-0269.		

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

[**X**] No.

[ ] Yes. The name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,

SIGNATURE _____ **Date** **10/21/03**

TYPED or PRINTED NAME: Jennifer Pearson Medlin **REGISTRATION NO. 41,385**
(*If Appropriate*)

NEEDLE & ROSENBERG, P.C.
Suite 1000
999 Peachtree Street
Atlanta, GA 30309
678-420-9300

EXPRESS MAIL NO. EL992020357US

CERTIFICATE OF EXPRESS MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail Invoice No. EL992020357US in an envelope addressed to: MAIL STOP PROVISIONAL PATENT APPLICATION, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, on the date indicated below.

Michael Laird — 10/21/03 (Date)

192479

ATTORNEY DOCKET NO. 09142.0002U1

GATEKEEPER INVENTION FOR CONTROLLING ACCESS TO A CORPORATE NETWORK USING 802.1x

The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access.

Definitions

GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria.

PC – A notebook, desktop PC, PDA, or similar computing device.

ND –Network device such as a network printer, which is normally incapable of running an agent.

EP – End point which can be a PC or ND.

AP – A switch or wireless access point (WAP) which is used to connect EPs to the corporate network. An EP connects to a switch with an Ethernet cable to one of the switch's ports. An EP typically connects to a WAP through a wireless network card, commonly through protocols like 802.11a or 802.11b.

ACL – Access Control List, which is a set of filtering rules that specify what traffic is permitted through a port. In the following description, the ACL is the one applied to a router port or a switch port.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 429 of 1144
INFOEXPRESS, INC. - EX2572

Existing System 1a: CyberGatekeeper Remote

In a typical system, policies are created by a policy manager, which may be connected to the corporate network. The policies are transferred to a GK that sits between the network access server (NAS) used by the EP and the corporate network. This implies that the GK has two NICs, one for the NAS side and one for the corporate network side. Each policy indicates various combinations of applications, configurations, and user identity that are permitted or prohibited for an EP accessing the corporate network. The NAS may be a remote access VPN, dialup server, or any other type of remote access device which is provided to permit EPs to access the corporate network. See Figure 1.

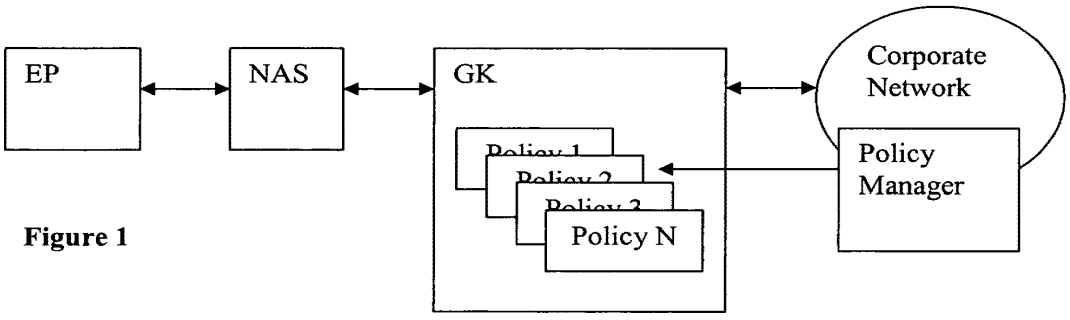


Figure 1

When the EP tries to access the corporate network, a software agent running on the EP automatically conducts an audit session with the GK. The agent tells the GK information about the EP including applications, configurations, and user logins, which the GK compares against the policies from the policy manager.

By default, the GK is designed to prevent access to the corporate network if there are no rules granting access to the corporate network. If the EP's audit information complies with the policies, the GK lets the EP access the corporate network by setting a filter rule(s) that allows traffic from the EP to communicate with the corporate network.

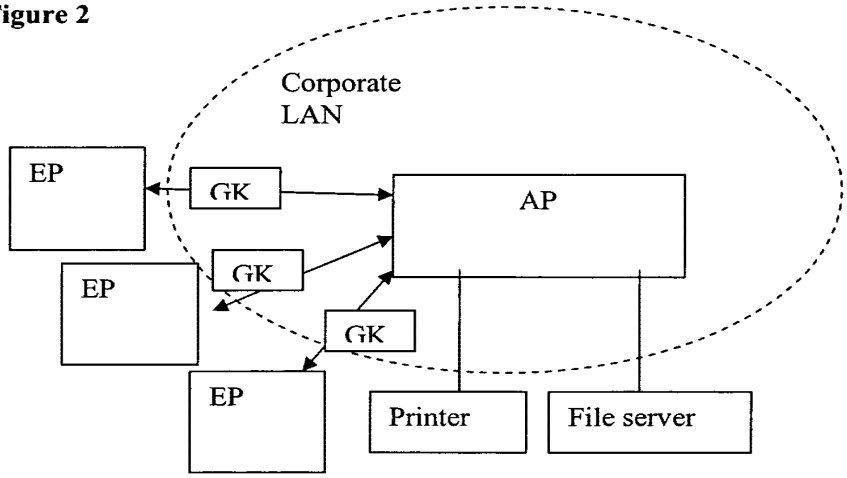
The GK continues to audit the EP regardless of whether the EP passed or failed the audit. This allows GK to allow or deny access if the EP configuration or applications change.

A disadvantage of this type of system is that network traffic between the EP and corporate network must pass through the GK to enforce access. If the network traffic between the EP and corporate network does not pass through GK, the filter rules would have no effect and would not be able to enforce access to the corporate network.

This is a problem when using a similar scheme to enforce access to the corporate network through an AP. Because the AP is part of the corporate network, much of the communications exchanged with an attached EP are to other EPs attached to the same AP. In such communications, the traffic remains inside the AP so the only external point where network traffic can be filtered for an EP is at each port of the AP.

Figure 2 shows how this would work. A large corporate network may use hundreds of APs, many of them with hundreds of ports, so this approach would be costly and impractical in the general case.

Figure 2



Another disadvantage to this system is that the EP must be capable of running an agent. Most NDs cannot run third party agents, and PCs whose operating systems are not supported cannot run the agents either.

Existing System 1b: VMPS

In a Cisco system, the proprietary VMPS protocol is used to program a switch to allow access by the EP to the corporate network upon authentication of the user identity. In this system, the AP uses the VMPS protocol require the user to enter a name and password which are authenticated by an authentication server.

A problem with this system is that it does not check whether or not the applications and configuration on the EP comply with corporate security policies. This means that users

whose EPs have security vulnerabilities or EPs that have been breached (i.e., may have a virus or trojan running on them) can access the corporate network.

Existing System 1c: 802.1x

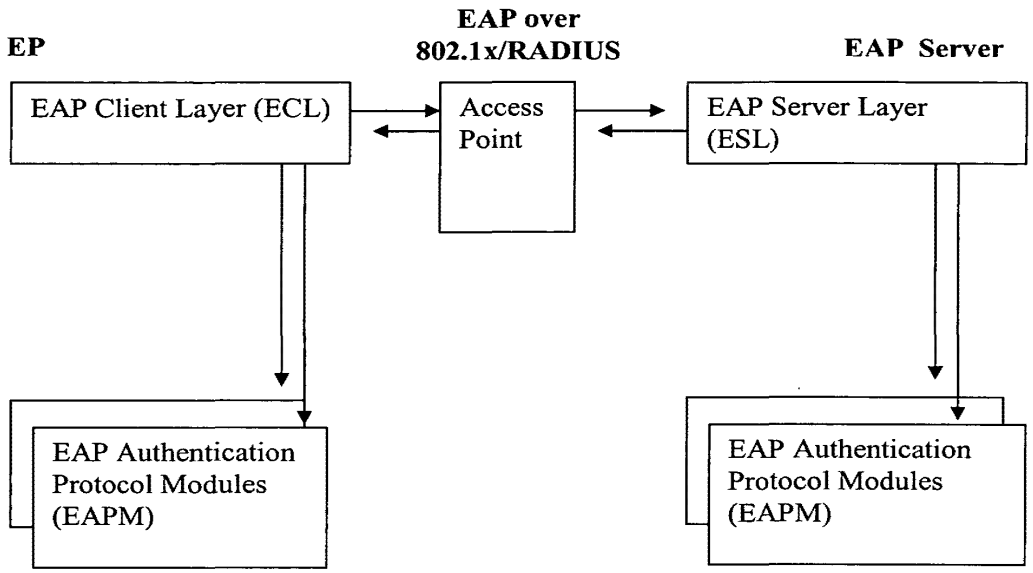
In a system using the 802.1x protocol, an authentication server enforces access by responding to 802.1x authentication requests. These requests originate from PCs that have 802.1x compliant client software that are forwarded through an 802.1x compliant AP. This system prevents users from accessing a network until they provide the proper authentication credentials, such as user name and password or a digital certificate.

In this type of system, the PC sends the authentication credentials, which are converted to 802.1x compliant EAP packets that are sent to the 802.1x compliant AP. The 802.1x compliant AP forwards the 802.1x EAP packets to an authentication server which verifies the credentials. Alternatively, the PC can send some or all of the authentication credentials automatically without user intervention.

The system optionally encrypts communications by using an EAP encryption protocol. This protocol runs first, then subsequent EAP authentication requests are embedded inside the EAP encryption protocol to ensure privacy. In network terminology, this technique is called "tunneling", whereby one protocol (the EAP authentication protocol) is embedded into another protocol (the EAP encryption protocol). After the authentication protocol has finished running, the encryption protocol also supplies a private key for encrypted communications for general traffic between the AP and EP.

A problem with this system is that it does not check whether or not the applications and configuration on the EP comply with an organization's security policies. This means that users whose EPs have security vulnerabilities or EPs that have been compromised (i.e. have been successfully attacked) can access the company network and potentially damage the network or other systems. Figure 3 shows the key components for this system.

Figure 3



CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 433 of 1144
INFOEXPRESS, INC. - EX2572

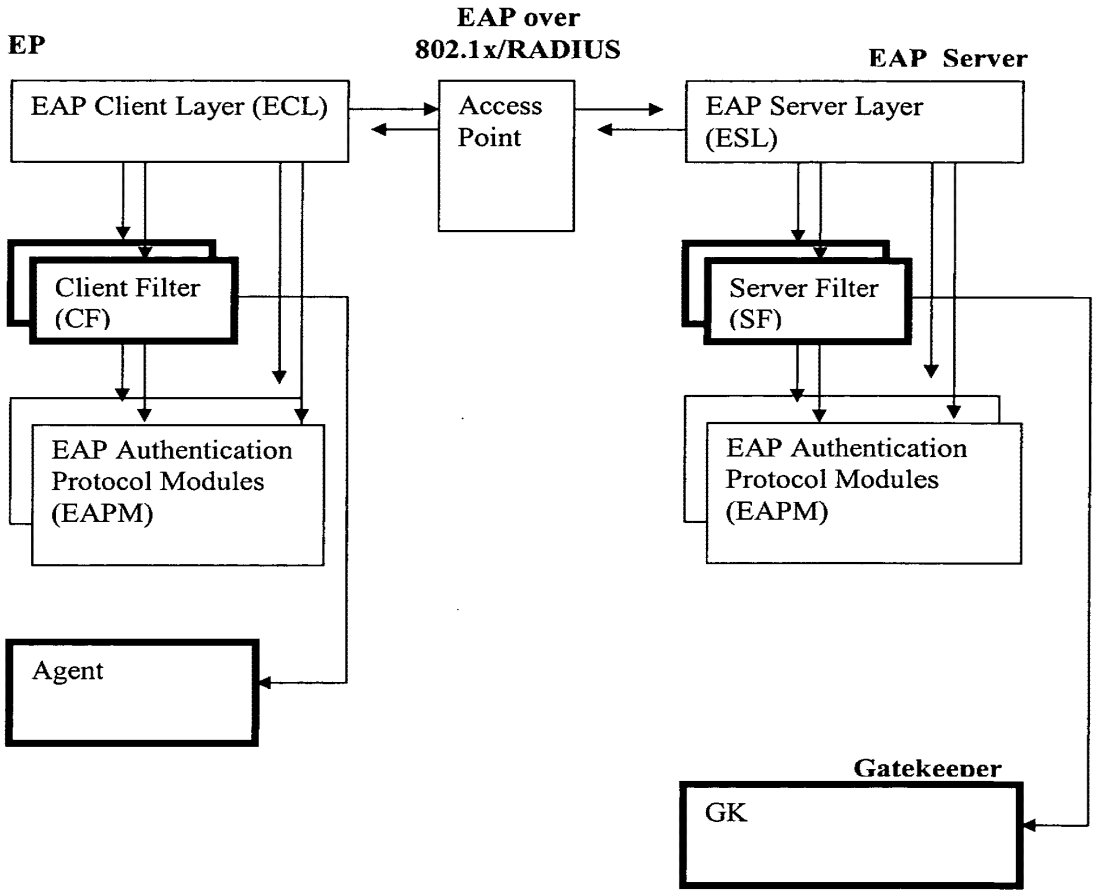
Invention

According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol.

In the invention, the auditing protocol takes place between the EP agent software and the GK. A client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP which relays them to the EAP server. The EAP server then calls a server filter which sends the responses to the GK for evaluation. The GK sends requests for more information on the reverse path and this continues until the audit is completed. If the audit is successful, the server sends a message to the AP which enables the EP's port allowing access for the PC. If the audit fails, the port on the AP is left disabled.

According to an exemplary embodiment, client filters (CF) and server filters (SF) are added along with an agent and GK to perform audits, as highlighted in Figure 4. There may be one or more instances of the CF and SF, which correspond to the separate EAP Authentication Modules (EAPM) that are supported. Note that the agent and GK are logical components. The functionality of the agent and GK can be embedded into the CF and SF, respectively, or in the case of the GK, may reside on a separate server.

Figure 4



The CF and SF APIs have APIs which correspond to the EAPM APIs. Therefore, the ECL or ESL can call the CF and SF instances corresponding to a particular authentication method as shown in Figures 5a and 5b. To the ECL and ESL, each instance of the CF and SF appears to be an EAPM which incorporates the functionality of the original EAPM prior to completion of the success response by the server EAPM.

Figure 5a: Client in Authentication State

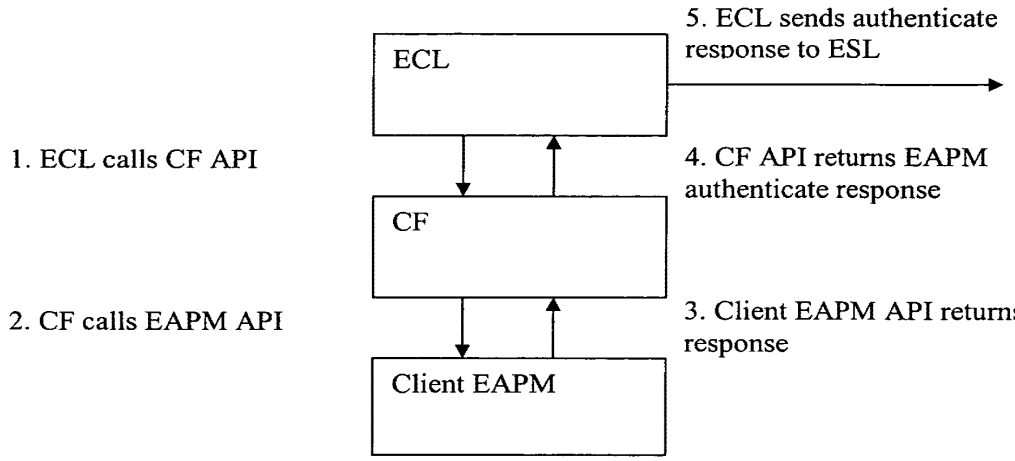
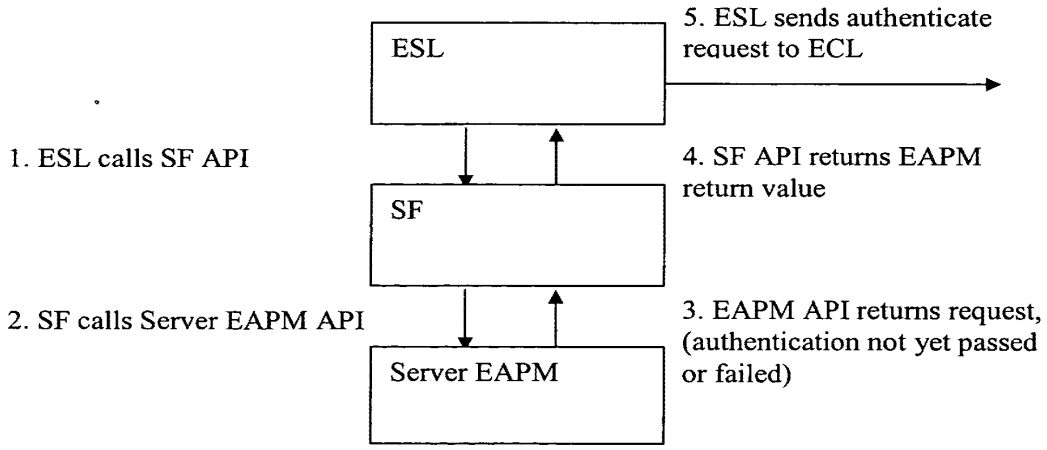


Figure 5b: Server in Authentication State



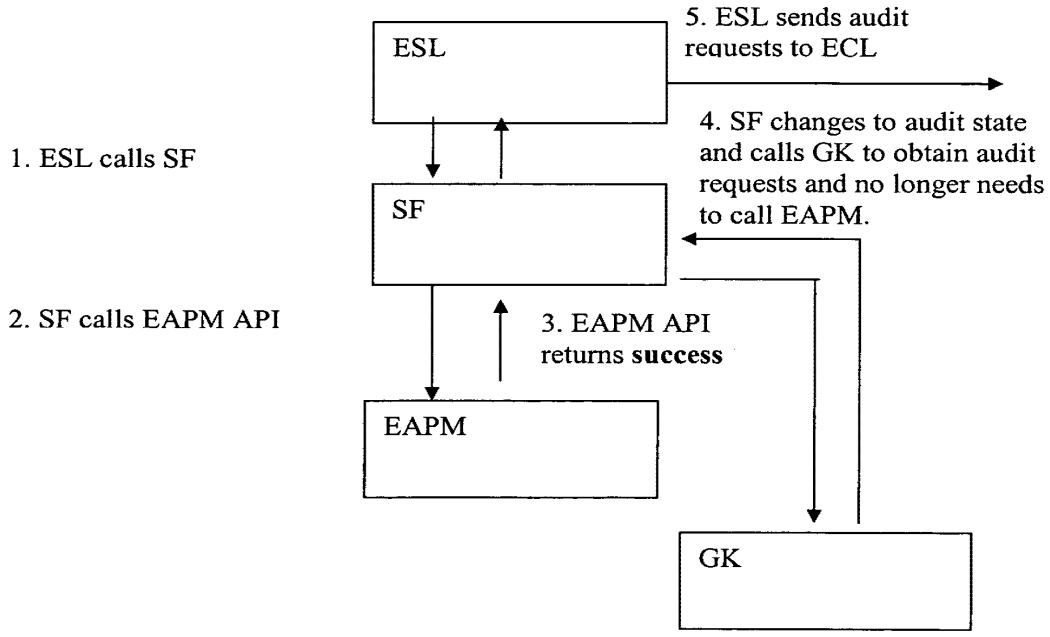
To use the invention, the ECL and ESL are configured to use the instance of the CF and SF corresponding to the desired authentication method. This authentication method corresponds to an authentication method supported by one of the EAPMs.

The ECL calls the corresponding CF to perform authentication, which at first calls the appropriate EAPM to obtain the proper authentication response. The authentication response is returned by the CF to the ESL, which sends the response to the server's ESL, SF, and EAPM. This process continues until the authentication either succeeds or fails, at which time the server's authentication EAPM returns a success or failure response to the SF.

If the SF receives a success response from the server EAPM as shown in Figure 6, the SF changes to the audit state and calls GK to obtain audit requests to send back to the client. In this state, the SF returns specially formatted audit requests to the ESL which are passed to the ECL, and eventually to the CF which sends back audit responses to the SF requests.

On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns information about the local system, which is converted to audit responses that are sent to the server.

Figure 6: Server Changing to Audit State



During the audit state, the SF and CF exchange audit requests and responses about the EP as shown in Figures 7a and 7b. The ECL and ESL continue to communicate with the CF and SF, but instead of calling the EAPM, the CF and SF call the agent and GK respectively, to perform this exchange. The audit session continues until the necessary audit information has been passed to the SF.

Figure 7a: Server in Audit State

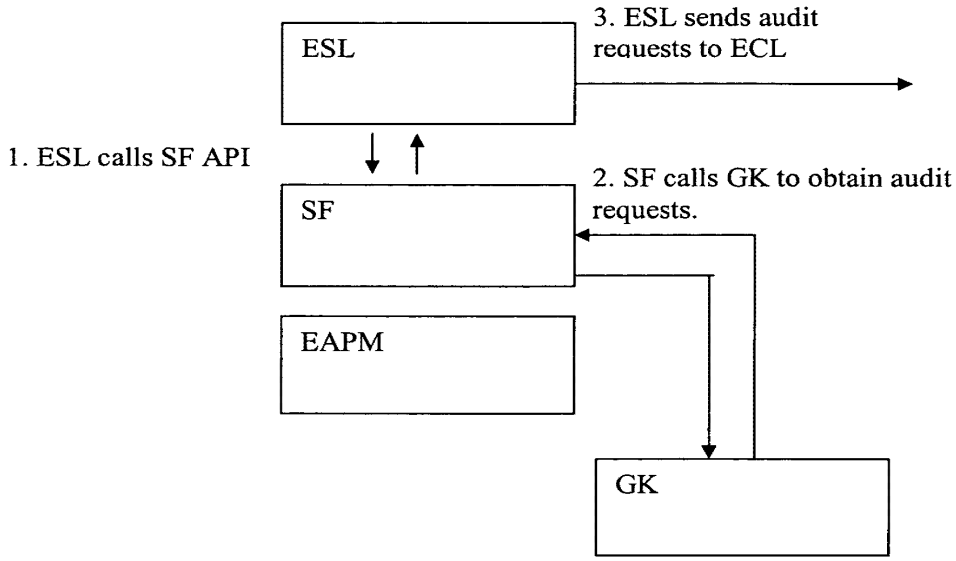
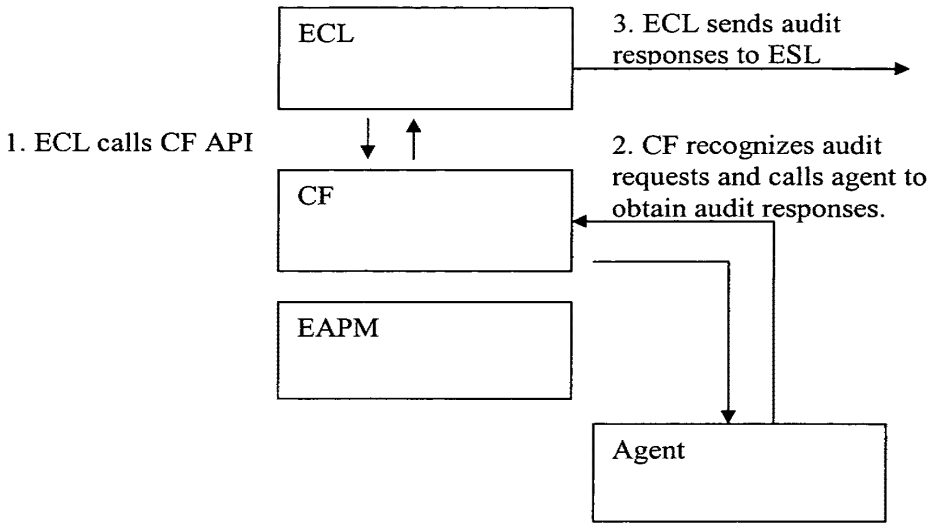


Figure 7b: Client Responding to Audit Requests



If the audit indicates the client EP is in compliance, the SF returns a success response. If the VLAN for the EP is specified in the policy, then the VLAN that should be used for this EP is passed back as well.

If the GK determines that the EP has failed the audit, GK returns a failure response to SF which causes one of the following: (1) the SF returns a failure to ECL, and the corresponding port on the AP is left disabled, or (2) the SF returns a success response to the ECL but specifies that the EP should be set to a restricted VLAN where the EP has limited network access. In either case, the EP is isolated from the company network until it successfully passes an audit with the GK.

After the audit has been performed, "keep alives" and updates regarding changes to previous audit information are exchanged. Changes are reevaluated and if inconsistent with the current state, access to the network is modified appropriately by changing the VLAN used for the EP or by terminating access by the EP by communicating with the AP.

Advantages of this invention are that:

1. The invention works with any AP that supports 802.1x. Additional protocols or interfaces are not needed to be compatible with this invention.

2. An EP attached to a port on the AP can be restricted from accessing the corporate network if it does not meet audit criteria. There is no need to physically insert a GK between the EP and the AP
3. The invention is highly scalable because a single GK can control many different ports and APs (i) from a different network, (ii) without a direct connection to the AP, and (iii) without requiring normal network traffic to traverse the GK.
4. If the routers used by the protected VLANs support ACLs, full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL.
5. The invention adds the ability to audit EPs that support an API where the audit filters can be inserted, without the need to change the existing authentication and encryption methods.

Details of exemplary enforcement modes of the invention are given in the attached Appendix.

APPENDIX

ATTORNEY DOCKET NO. 09142.0002U1

14

infoExpress Secure the last mile

CyberGatekeeper Enforcement Modes

http://www.infoexpress.com

(c) 2003 InfoExpress, Inc.

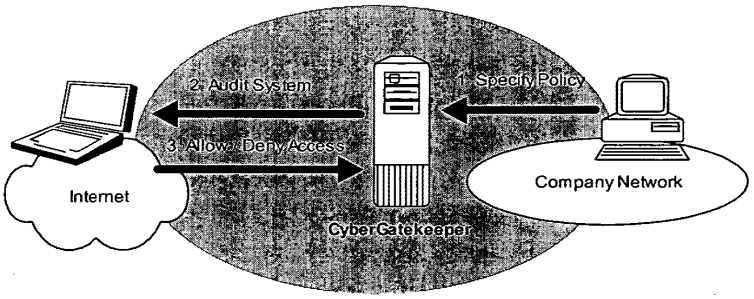
ATTORNEY DOCKET NO. 09142.0002U1

15

infoExpress **Secure the last mile**

Inline Mode Simplified

- DDefine acceptable configurations and applications
- AAudit remote system for compliance
- EEnforce access based on results of audit



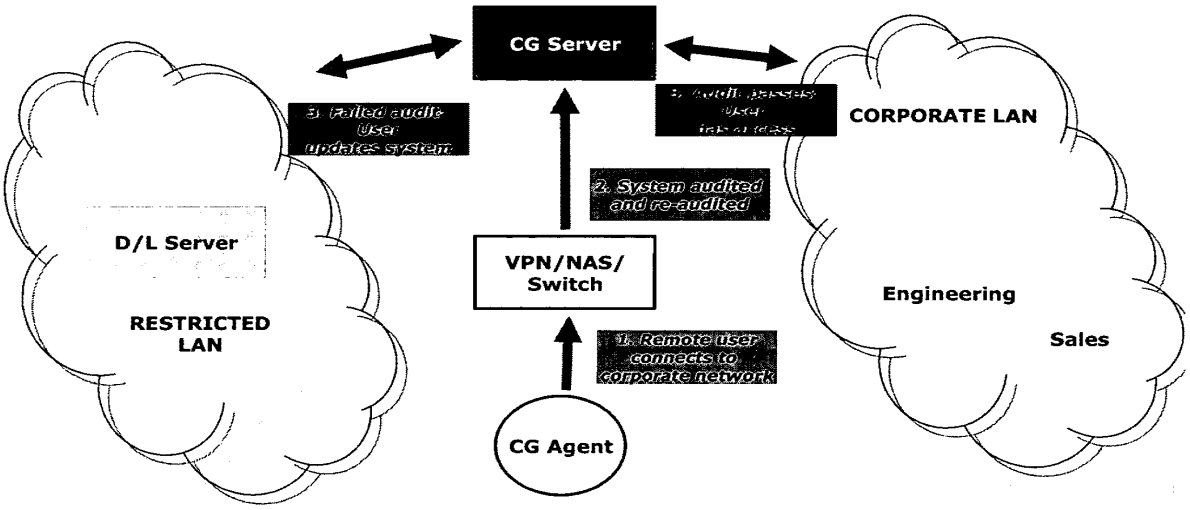
(c) 2003 InfoExpress, Inc. 2

InfoExpress Confidential Authors: Stacey Lum and Alice Lee

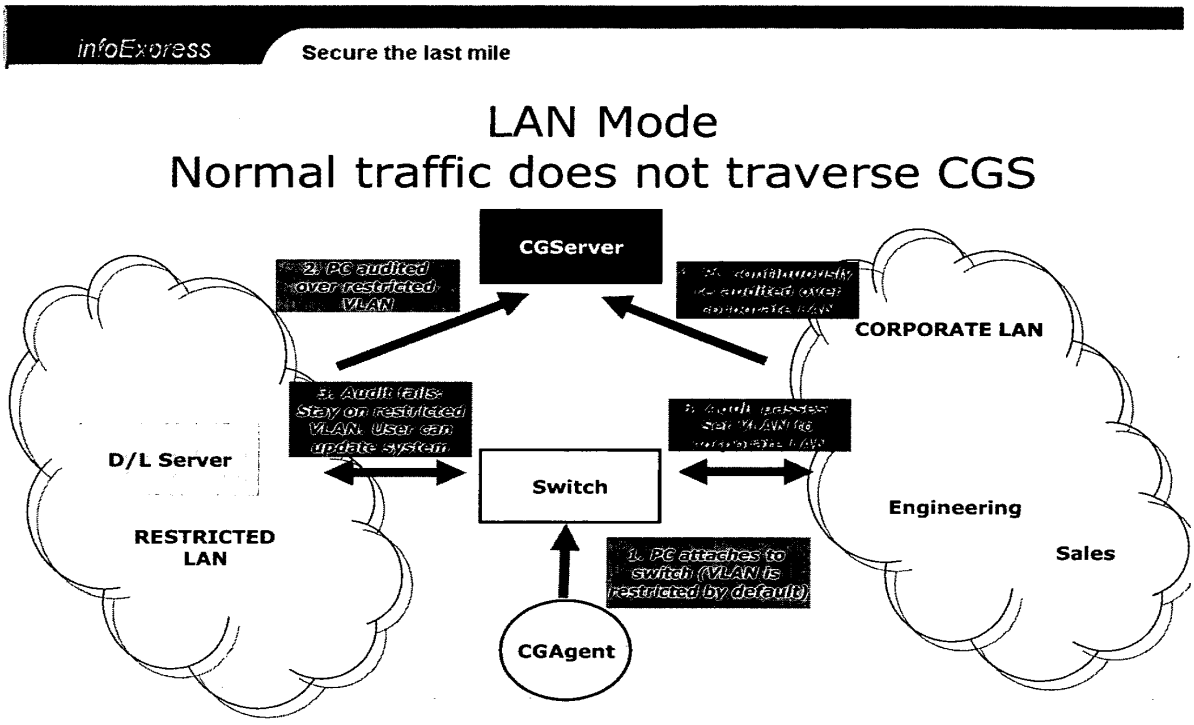
192377

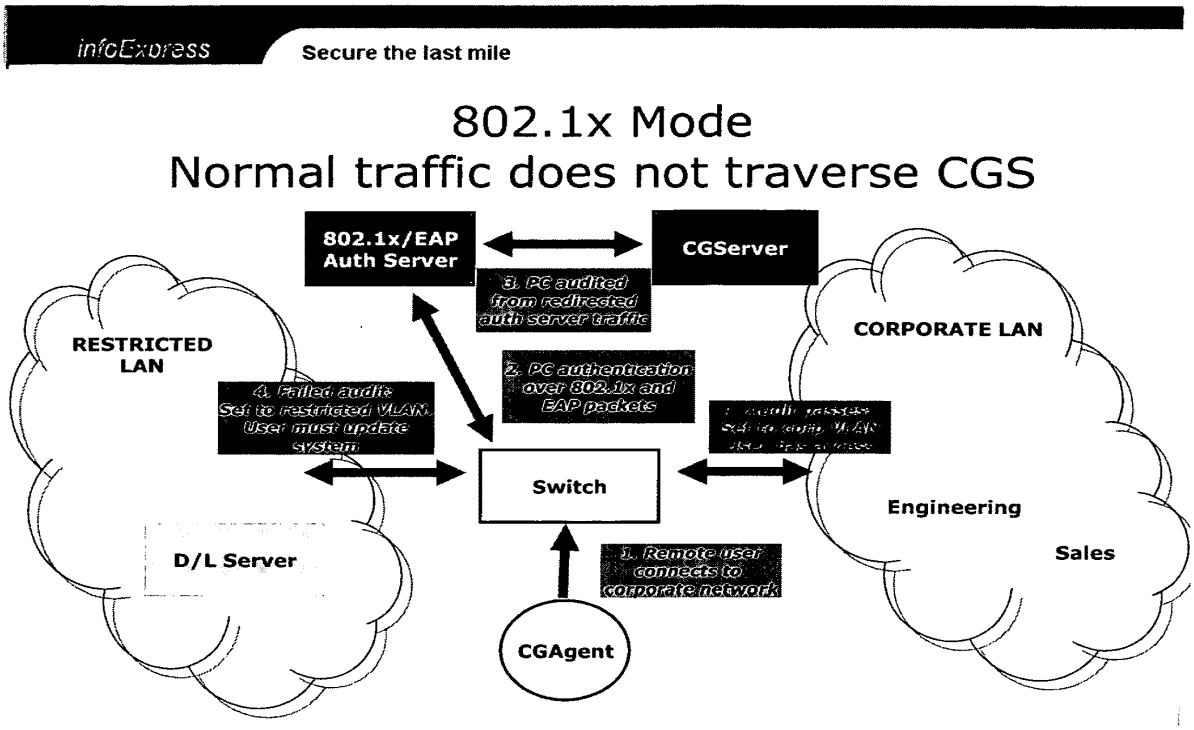
infoExpress Secure the last mile

Inline Mode
Audit and normal traffic traverses CGS

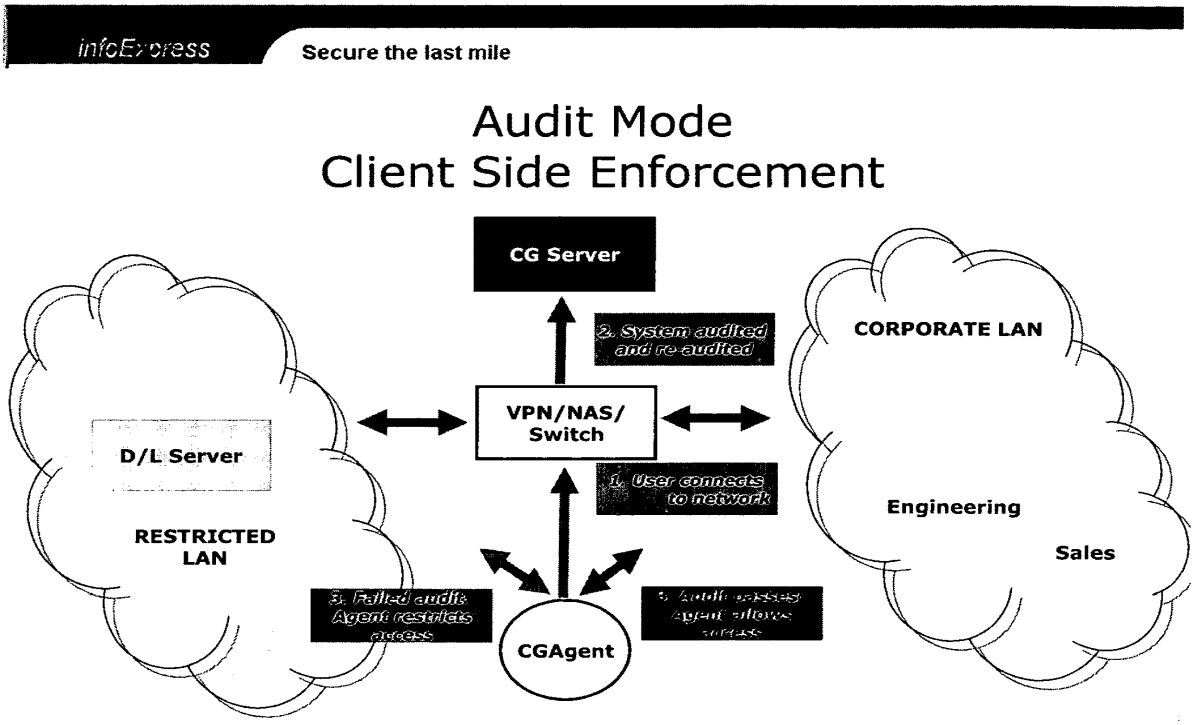


(c) 2003 InfoExpress, Inc.


infoExpress
Secure the last mile
LAN Mode
Normal traffic does not traverse CGS
CGServer
2. PC audited over restricted VLAN
CORPORATE LAN
3. Audit fails- Stay on restricted VLAN. User can update system
D/L Server
Switch
Engineering
Sales
RESTRICTED LAN
1. PC attaches to switch (VLAN is restricted by default)
CGAgent
(c) 2003 InfoExpress, Inc.
4



(c) 2003 InfoExpress, Inc.


infoExpress
Secure the last mile
Audit Mode
Client Side Enforcement
CG Server
2. System audited and re-audited
CORPORATE LAN
VPN/NAS/ Switch
D/L Server
1. User connects to network
Engineering
RESTRICTED LAN
Sales
3. Failed audit Agent restricts access
CGAgent
(c) 2003 InfoExpress, Inc.
6

PATENT APPLICATION SERIAL NO. _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

10/24/2003 MMEKONEN 00000112 60513080
01 FC:2005 80.00 OP

PTO-1556
(5/87)

*U.S. Government Printing Office: 2002 — 489-267/69033

EXHIBIT U

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

BILLJCO, LLC	)	
	)	CASE NO: 2:21-cv-00181-JRG
v.	)	(Lead Case)
	)	
CISCO SYSTEMS, INC.	)	
	)	
	)	

BILLJCO, LLC	)	
	)	
v.	)	CASE NO: 2:21-cv-00183-JRG
	)	(Member Case)
HEWLETT PACKARD ENTERPRISE	)	
COMPANY, ARUBA NETWORKS, LLC	)	
	)	
	)	

BILLJCO, LLC'S REPLY CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

I. Introduction 1

II. The Disputed Claim Terms Should Be Afforded Their Plain And Ordinary Meaning As Would Be Understood By A POSITA In View Of The Intrinsic Evidence 2

A. "a Bluetooth communication interface" 2

B. "application" 5

C. "application context identifier data" 7

D. "an application in use at the sending data processing system" 8

E. "identity information for describing an" an originator identity" 9

III. Conclusion 10

TABLE OF AUTHORITIES

Cases

ACQIS LLC v. Samsung Electronics Co., Ltd.,
Case No. 2:17-cv-145, 2018 WL 647734 (E.D. Tex. Jan. 31, 2018).....4

ACQIS LLC v. Mitac Computing Tech. Corp.,
20-cv-962 (W.D. Tex. Nov. 17, 2021 4

Baxalta Inc. v. Genentech, Inc.,
972 F.3d 1341 (Fed. Cir. 2020).....5

Fundamental Innovation Sys. Int'l LLC v. Samsung Elecs. Co.,
Case No. 2:17-cv-145-JRG-RSP, 2018 WL 647734 (E.D. Tex. Jan. 31, 2018).....4

Hill-Rom Servs., Inc. v. Stryker Corp.,
755 F.3d 1367 (Fed. Cir. 2014).....10

Interactive Gift Exp., Inc. v. Compuserve Inc.
256 F.3d 1323 (Fed. Cir. 2001).....6

Liebel-Flarsheim Co. v. Medrad, Inc.,
358 F.3d 898 (Fed. Cir. 2004).....6

O2 Micro Int'l. Ltd. v. Beyond Innovation Tech. Co., Ltd
521 F.3d 1351 (Fed. Cir. 2008).....7

Phillips v. AWH Corp.,
415 F.3d 1303 (Fed. Cir. 2005) (en banc)..... passim

Summit 6, LLC v. Samsung Elecs. Ltd.,
802 F.3d 1283 (Fed. Cir. 2015).....5

Thorner v. Sony Computer Entm't Am. LLC,
669 F.3d 1362 (Fed. Cir. 2012).....

Uniloc USA, Inc. v. Apple, Inc.,
Case No. 19-cv-1692, 2021 WL 432183 (N.D. Cal. Jan. 15, 2021).....3

VCase Form. v. Benetton Grp. & Rollerblade, Inc
334 F.3d 1314 (Fed. Cir. 2003) 4

Wisconsin Alumni Research Foundation v. Apple Inc.,
905 F.3d 1341 (Fed. Cir. 2018).....1

All emphasis supplied unless otherwise indicated

I. Introduction

Despite Defendants false implications otherwise, BillJCo's claim construction position has always been that the plain and ordinary meaning should control. Presumptively, patent terms are given their plain and ordinary meaning, i.e., the "meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005) (en banc).

The plain and ordinary meaning of the disputed claim terms to a POSITA in view of the intrinsic evidence as discussed in BillJCo's Opening Claim Construction brief are fully aligned with the claims and patent specifications. There is no clear evidence of any intent by the applicant to vary from these plain and ordinary meanings. Yet, Defendants hope to import limitations from the specifications into the claims under the guise that “lexicography” necessitates narrow, convoluted constructions. The intrinsic evidence shows Defendants' arguments as nothing but an improper attempt to import limitations from isolated embodiments in the specifications to the exclusion of others.

II. The Disputed Claim Terms Should Be Afforded Their Plain And Ordinary Meaning As Would Be Understood By A POSITA In View Of The Intrinsic Evidence

A. "a Bluetooth communication interface"

Defendants' claim construction for "Bluetooth," which is part of the disputed phrase "Bluetooth communication interface," is that the use "Bluetooth" requires incorporation of the entirety of promulgated industry standards that existed as of the priority date for the asserted patent. This argument lacks any support in the intrinsic evidence, which does not mention any industry standard. Moreover, the ordinary meaning of "Bluetooth communication interface" to a POSITA in view of the intrinsic evidence is contrary to Defendants' arguments. *Wisconsin Alumni Research Foundation v. Apple Inc.*, 905 F.3d 1341, 1348 (Fed. Cir. 2018) ("the 'ordinary

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 454 of 1144
INFOEXPRESS, INC. - EX2572

meaning' of a claim term is its meaning to the ordinary artisan after reading the entire patent").

Beginning with the intrinsic evidence, Defendants fail to give any attention to the claim language itself, upon which any claim construction must remain centered. See *Phillips*, 415 F.3d at 1312. The claims demonstrate that "Bluetooth" was not intended to refer to any industry standard. First, the claims **do not** recite any standard or "protocol." Second, the claims **do** recite limitations that demonstrate "Bluetooth" was intended to refer to a wave spectrum range:

> periodically beaconing outbound a broadcast unidirectional wireless data record communicated through **the Bluetooth communications interface** to serve as a physical location reference contributing to physical location determination processing of one or more user carried mobile data processing systems **in a Bluetooth wave spectrum range** vicinity of the beaconing data processing system …. Dkt. 65, Ex. H, '994 Patent, Col. 448:35-42; see also Id. Col. 449:38-47; Col. 450:32-39.

The use in the claim of "Bluetooth communications interface" with "Bluetooth wave spectrum range" demonstrates Bluetooth references a wave spectrum range. See *Phillips*, 415 F.3d at 1314 ("the context in which a term is used in the asserted claim can be very instructive.").

Further intrinsic evidence, namely, the specification also uses "Bluetooth" to reference "a class of Radio Frequency (RF) wave spectrum." Indeed, this is the only teaching of "Bluetooth."

> Locating functionality may incorporate triangulated locating of the MS, for example using **a class of Radio Frequency (RF) wave spectrum** (cellular, WiFi (some WiFi embodiments referred to as WiMax)**, bluetooth**, etc), and may use measurements from different wave spectrums for a single location determination (depends on communications interface(s) available). A MS may have its whereabouts determined using a plurality of **wave spectrum classes** available to it (cellular, WiFi, **bluetooth, etc).** Dkt. 65, Ex. H, '994 Pat., Col. 6:55-63.

> Presence of field 2490d indicates to send processing feeding from queue 24 to target the MS ID over the specified comm. interface (e.g. when MS has a plurality of comm. interfaces (e.g. cellular, WiFi, **Bluetooth, etc; i.e. MS supports multiple classes of wave spectrum**)). Dkt. 65, Ex. H, '994 Patent, Col. 121:11-14.

"[T]he specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term'" *Phillips*, 415 F.3d 1315 (quotation omitted). Applying general English to the specification portions above demonstrates

that "Bluetooth" references a class of wave spectrum range. The specification recites "a class of Radio Frequency (RF) wave spectrum," and then uses parentheses to explain these classes. Thus, the specification explains the plain and ordinary meaning of "Bluetooth communication interface" is a means for transmitting data in the Bluetooth wave spectrum range.

Lacking any support in the intrinsic evidence, Defendants resort to arguments related to different claim terms in different patents from different cases. These cases are inapposite because they expressly claim a standard or protocol. For example, Defendants reference *Uniloc USA, Inc. v. Apple, Inc.*, Case No. 19-cv-1692, 2021 WL 432183, at *8 (N.D. Cal. Jan. 15, 2021) claiming that the court there held that the claim terms "Bluetooth messaging" and "Bluetooth protocols" should be limited to functionality described in the Bluetooth Core Specification "as it existed at the time of the claimed invention." Dkt. 32 at 7. The court in *Uniloc* found that "Bluetooth messaging" and "Bluetooth protocols" mean "Bluetooth [messaging/protocols] as defined in the Bluetooth specification versions 1.1 or earlier (including versions 1.0A and 1.0B), **and that remain in later versions of the Bluetooth specification**." *Uniloc*, 2021 WL 432183, at *8 (emphasis supplied). As such, the *Uniloc* court rejected the argument that the claim terms were limited to the Bluetooth protocol at the time of the claimed invention, and instead found that it included features from earlier specifications that were also found in later versions. All specifications for Bluetooth include wireless transmissions in the 2.4 Ghz to 2.4835 Ghz wave spectrum. Ex. H, Sharony Decl. ¶ 51. More importantly, in *Uniloc*, the independent claim specified that "the beacon is arranged to broadcast a series of inquiry messages each in the form of a plurality of predetermined data fields arranged according to a **first communication protocol**." *Uniloc*, Case No. 19-cv-1692, 2021 WL 432183, at *3. This dependent claims them specify this protocol is Bluetooth. *Id.* at *8. Thus, in *Uniloc*, the claims at issue expressly recited

a "communication protocol." That is not the case here, however, because the claims here do not recite a "protocol," standard, specification, or the like, and neither do the specifications.

Similarly, Defendants cite *ACQIS LLC v. Samsung Electronics Co., Ltd.*, Case No. 2:20-cv-00295-JRG (E.D. Tex. Sept. 26, 2021) in support of their proposed construction. However, like in *Uniloc*, the recited claim limitation in *ACQIS* was "Universal Serial Bus (USB) **protocol**." Dkt. 67-2 at 32-33 (emphasis supplied).[1] That is not the case here. The intrinsic evidence, namely the claims and specification, make no mention of a "protocol."

Defendants further cite *Fundamental Innovation Sys. Int'l LLC v. Samsung Elecs. Co.*, Case No. 2:17-cv-145, 2018 WL 647734, at *11 (E.D. Tex. Jan. 31, 2018). There, the claims and specification required a particular connector, namely, USB connector, and for this reason, the claims were limited to USB connectors that existed at the time of the claimed invention. *Id*. As discussed, however, the inventor of the Patents-in-Suit here used "Bluetooth" not to reference a standard, but instead, to reference a class of wave range spectrum, along with other wave spectra, e.g., cellular (0.8 GHz to 2.4 GHz); WiFi(2.4 GHz or 5 GHz); and WiMAX (2 GHz to 11 GHz).[2] Dkt. 65, Ex. H, '994 Pat., Col. 6:55-63.

The similarities in Defendants cited cases that the claims recited a standard or protocol actually bolster BillJCo's case. BillJCo's claims do not recite a standard or protocol. As such, requiring compliance with such would be improper.

Defendants cite *VCase Form. v. Benetton Grp. & Rollerblade, Inc.*, 401 F.3d 1307, 1311-

[1] This same patent was also the subject matter of litigation in *ACQIS LLC v. Mitac Computing Tech. Corp.*, 20-cv-962 (W.D. Tex. Nov. 17, 2021), wherein the court found that USB Serial Bus (USB) protocol was to be afforded its plain an ordinary meaning. Kuo Decl. Ex. M.

[2] See e.g., https://www.techwalla.com/articles/what-type-of-wavelengths-do-cellphones-use (cellular); https://www.scientificamerican.com/article/how-does-wi-fi-work/ (WiFi); https://computer.howstuffworks.com/wimax.htm (WiMAX).

12 (Fed. Cir. 2005) for the proposition that references on face of patent are intrinsic evidence for claim construction. Defendants then cite U.S. Patents 5,923,702 and 5,717,688; neither of which include any discussion regarding "Bluetooth." Thus, these are irrelevant.

B. "application"

Defendants contort the word "application," which is ubiquitous in computer science and has been part of the everyday lexicon of smartphone users for years, and define it according to an isolated embodiment from the specification. *See Summit 6, LLC v. Samsung Elecs. Ltd.*, 802 F.3d 1283, 1291 (Fed. Cir. 2015) (No construction required because term was “comprised of commonly used terms,” “used in common parlance,” and was a “straightforward term.”).

Defendants offer the nonsensical argument that BillJCo’s plain and ordinary meaning of "application" (a computer software program for performing a function) lacks explanation. Dkt. 67 at 10. The explanation is this **is** the plain and ordinary meaning.

Defendants actually admit to lifting its limiting construction – "[a]n entity of processing which can be started, terminated, and have processing results. Applications (i.e. executables) can be started as a contextual launch, custom launch through an API or command line, or other launch method of an executable for processing" – *verbatim* from the specification. Dkt. 67 at 10. Its only justification for this is “lexicology.” Dkt. 67 at 11. But Defendants ignore the “exacting” lexicography standard which “requir[es] the patentee to 'clearly express an intent' to redefine a term." *Baxalta Inc. v. Genentech, Inc.*, 972 F.3d 1341, 1349 (Fed. Cir. 2020).

Nothing Defendants point to rises to this “exacting” standard. Rather, all Defendants can muster is an isolated embodiment related to an "atomic command." *See e.g.*, Ex. 1: Kuo Decl. Ex. I, '011 Patent, Col. 269:41-59. The claims do not mention atomic commands, and Defendants fail to explain why this specific process would apply to all uses of “application.” Indeed, this

piece-meal selection of the specification falls far short of the "exacting" evidence necessary to vary from the plain and ordinary meaning. *Liebel-Flarsheim*, 358 F.3d at 913.

Ignoring its "exacting" burden to show "clearly express[ed] intent" to redefine a term, Defendants argue that *BillJCo* fails to point to anywhere in the specification to support the plain and ordinary meaning. Dkt. 67 at 12. In doing so, Defendants improperly attempt to put the onus on BillJCo to prove it used "application" according to its plain and ordinary meaning. That is not the law. "The words of a claim are generally given their ordinary and customary meaning." *Phillips*, 415 F.3d at 1312-13. It is up to Defendants to present evidence of a clear intent to impart a special meaning. *Thorner*, 669 F.3d at 1365.

Moreover, if the applicant had intended to limit "application," it would stand to reason that discussion similar to that relied on by Defendants would be found in more than just in one of many embodiments. *See Interactive Gift Exp., Inc. v. Compuserve Inc.*, 256 F.3d 1323, 1334–35 (Fed. Cir. 2001) (Court not importing limitation where: "it is unclear whether this isolated statement in the specification is intended to be a general statement or to be limited to a particular embodiment. However, there is nothing in the rest of the specification supporting the position that a point of sale location is defined as having at least two blank material objects.").

Notwithstanding Defendants' burden, BillJCo identified the word "application" being used according to its plain and ordinary meaning throughout the specification. Ex. 1: Kuo Decl. Ex. I, '011 Patent, Col. 1:36-40, Col. 4:62-65; Ex. J, '804 Patent, Col. Col. 1:20-24, 4:36-39. See also, Dkt. 52-1 at 6-11 ("The present disclosure relates generally to location based services for mobile data processing systems, and more particularly to location based exchanges of data between distributed mobile data processing systems for locational applications"; "It is an advantage herein for enabling useful distributed applications without the necessity of having a

service, and without the necessity of users and/or systems registering with a service.").

Defendants' proposed construction actually adds confusion by defining "application" with the technical term "executable."[3] As illustrated in its brief, Defendants' construction would also likely lead to a dispute about what "executable" means (Dkt. 67 at 11), and would essentially leave its meaning to the jury, which would be improper. *O2 Micro Int'l. Ltd. v. Beyond Innovation Tech. Co., Ltd.*, 521 F.3d 1351, 1360 (Fed. Cir. 2008) ("[B]y failing to provide a construction of this term, the district court effectively submitted a legal question to the jury.").

C. "application context identifier data"

Defendants falsely argues that BillJCo mischaracterized their construction. The claim phrase is "application context identifier data." Defendants' construction is "data identifying a context in which the application was presented to a user via a user interface." This construction takes the individual words from "application context identifier data" and rearranges them as "data identifying a context in which the application…." BillJCo mischaracterized nothing, and instead, just highlighted a fault in Defendants' proposed construction.

Next, Defendants added the unrecited limitation "*the application was presented to a user via a user interface*" as part of its proposed claim construction. Dkt. 67 at 12. It is undisputed that the claim does not include this extra limitation. And unlike above, this limitation is not even found in the specification. Indeed, Defendants are left to argue only that their construction reflects the *purpose* of the claim term as used in the specification and claims.

[3] "Executable" is discussed in the specification. See e.g., Dkt. 65, Ex. I, '011 Patent, Col. 158:35-41 ("…executables, with or without parameters, including Dynamic Link Library (DLL) interfaces (e.g. function), post-compile linked interfaces (e.g. function), scripts, batch files, command files, or any other executable"); Id., Col. 228:54-59 ("A paths field 5300f identifies … data processing system file name paths to executables (e.g. .exe, .dll, etc) for spawning associated with the Application for the AppTerm referenced with the prefix of field 5300a").

Defendants devote substantial argument to explaining why its proposed construction is consistent with the teachings in the specification. Dkt. 67 at 14-15. This, however, is immaterial to whether the plain and ordinary meaning for "application context identifier data" should be altered, or mandate that Defendants' limiting language be appended to the claim. Indeed, Defendants do not argue, because they cannot, that the plain and ordinary meaning of "application context identifier data" is inconsistent with the purpose of the invention.

In response to BillJCo's argument that the context information need not be presented to the user, Defendants incorrectly state the claim requires the "application context identifier data identif[ies] location based content for presenting" (Dkt. 67 at 14) by improperly cropping the relevant claim limitation. The claim actually states the "application context identifier data **identifying location based content for presenting by a location based application of the receiving user carried mobile data processing system to a user interface**…." Dkt. 65, Ex. I, '011 Patent, Col. 448:33-36. As claimed, it is location based content that is presented to the user interface, and the application context identifier data identifies this location based content. The claim does not require that the application context identifier data itself is presented to the user.

Defendants offers attorney argument to dispute what a POSITA would understand from Fig. 65B-5. However, Defendants offer no expert opinion in support.

D. "an application in use at the sending data processing system"

Defendants interject confusion into the claim construction issue as to whether an application is “in use” or “asleep.” Dkt. 67 at 17. But that is not the issue as "an application in use at the sending data processing system" should be given its plain and ordinary meaning.

Defendants incorrectly argue BillJCo's construction would effectively submit a legal question to the jury. Dkt. 67 at 18. In essence, Defendants argue "in use" needs to be defined as

"running." Defendants, however, fail to explain why "in use" would not be understandable, or why "running" is any more understandable. Here, "the ordinary meaning of claim language as understood by a person of skill in the art may be readily apparent even to lay judges, and claim construction in such cases involves little more than the application of the widely accepted meaning of commonly understood words." *Phillips*, 415 F.3d at 1314.[4]

It is further notable that in concurrent litigation involving the patents in suit, the Defendant there initially proffered the same construction as Defendants do here. After being presented with BillJCo's argument, the other Defendant withdrew its proposal and agreed that the plain and ordinary meaning is appropriate. Ex. 1: Kuo Decl. Ex. K.

Defendants' cherry-picking of Dr. Sharony's testimony (Dkt. 76 at 18) is also meaningless. A review of the relevant transcript demonstrates a POSITA's clear distinction between "in use" and "running" on the grounds that "…you can have applications that wakes up from time to time like the Gmail… to see if there is an email and then goes back to sleep. So it's not active." Ex. 1: Kuo Decl., Ex. L, 154:17-25.

Accordingly, there is no reason to alter that plain and ordinary meaning of "in use" to substitute it for "running." Defendants' proposed construction should be rejected.

E. "identity information for describing an originator identity"

As Defendants concede, the dispute over the claim phrase "identify information for describing an originator identity" centers on Defendants attempt to require that the identifier "uniquely identifies the originator device." It is undeniable that the word "uniquely" or anything of the sort is not recited in the subject claim phrase.

[4] Defendants falsely assert BillJCo attempts to delete "in use" from the claim through an attempted distinction between "used," "accessed," and "in use." This is also meritless for the same reasons as above.

Defendants reference portions of the specification discussing unique identifier for mobile systems claim that "an identifier that identifies which specific device sent the data, i.e., a unique identification." Dkt. 67 at 20. But this belies the claim language which recite "beaconing outbound a broadcast unidirectional wireless data record." Dkt. 65 Ex. H, '994 Patent, claim 1. Since the transmission is one-way (or "unidirectional") there is no requirement to know which "specific" device sent the data. BillJCo's expert and the specification confirm other instances where identification of a "specific" device is not required. Dkt. 65 at 18.

Defendants reference some embodiments from the specification in hopes of adding the "uniquely" limitation into the claim. But "[e]ven when the specification describes only a single embodiment, the claims of the patent will not be read restrictively unless the patentee has demonstrated a clear intention to limit the claim scope using words or expressions of manifest exclusion or restriction." *Hill-Rom Servs., Inc. v. Stryker Corp.*, 755 F.3d 1367, 1372 (Fed. Cir. 2014). In this case, the specification is not limited to unique IDs.

> For indirect location functionality disclosed herein, affirmifier and pacifier WDRs do not need to have a correct originating MS ID field 1100a. The MS ID may be null, or anything to distinguish WDRs for MS locations. However, to accomplish other LBX features and functionality, MS Identifiers (MS IDs) of nearby MSs (or unique correlations thereof) maintained in queue 22 are to be known for processing by an MS. **MS ID field 1100a may contain a group identifier of MSs in some embodiments for distinguishing between types of MSs (e.g. to be treated the same, or targeted with communications, as a group)**, as long as the MS containing queue 22 can distinguish its own originated WDRs 1100. A defaulted value may also be set for a "do not care" setting (e.g. null). Dkt. 65, Ex. J, '804 Patent, Col. 59:19-32 (emphasis supplied).

As is clearly discussed, The MSs may have a unique identifier, a nonunique identifier, e.g., a group identifier, or no identifier, e.g., null.

III. Conclusion

For the reasons discussed above, Plaintiff BillJCo respectfully requests that this Court find that the disputed claims terms be afforded their plain ordinary meanings.

Dated: January 27, 2022

Respectfully submitted,

/s/ Brian R. Michalek

Brian R. Michalek (*pro hac vice* granted)
Casey Grabenstein (*pro hac vice* granted)
Brian Landry (*pro hac vice* granted)
Joseph M. Kuo (*pro hac vice* granted)
Erin Westbrook (*pro hac vice* granted)
brian.michalek@saul.com
casey.grabenstein@saul.com
brian.landry@saul.com
joseph.kuo@saul.com
erin.westbrook@saul.com
Saul Ewing Arnstein & Lehr LLP
161 N. Clark St., Suite 4200
Chicago, IL 60601
Telephone: 312-876-7100
Facsimile: 312-876-0288

Of Counsel:

Claire Abernathy Henry
Texas State Bar No. 24053063
E-mail: claire@wsfirm.com
Andrea L. Fair
Texas State Bar No. 24078488
E-mail: andrea@wsfirm.com
WARD, SMITH & HILL, PLLC
1507 Bill Owens Parkway
Longview, Texas 75604
(903) 757-6400 (telephone)
(903) 757-2323 (facsimile)
Attorneys for Plaintiff BillJCo, LLC

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing document has been served via e-mail on **January 27, 2022** to all counsel of record who are deemed to have consented to electronic service via the Court's CM/ECF system.

/s/Brian R. Michalek

EXHIBIT V

Brian R. Michalek (SBN 302007)
Casey T. Grabenstein (*pro hac vice*)
Joseph M. Kuo (*pro hac vice*)
SAUL EWING LLP
161 N. Clark St., Suite 4200
Chicago, IL 60601
Telephone: (312) 876-7100
Facsimile: (312) 876-0288
brian.michalek@saul.com
casey.grabenstein@saul.com
joseph.kuo@saul.com

Andrew Schwerin (*pro hac vice*)
SAUL EWING LLP
Centre Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102 2186
Telephone: (215) 972-7184
Facsimile: (215) 972-7184
andrew.schwerin@saul.com

Michael E. Flynn-O'Brien (SBN 291301)
BUNSOW DE MORY LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: (650) 351-7245
Facsimile: (415) 426-4744
mflynnobrien@bdiplaw.com

Attorneys for Plaintiff InfoExpress Inc.

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

INFOEXPRESS INC. Plaintiff, v. **CISCO SYSTEMS, INC.,** Defendant.	Case No. 4:23-cv-02698-YGR **INFOEXPRESS INC.'S DISCLOSURE OF ASSERTED CLAIMS AND INFRINGEMENT CONTENTIONS PER PATENT L.R. 3-1 and 3-2**

I. DISCLOSURE OF ASSERTED CLAIMS AND INFRINGEMENT CONTENTIONS (PATENT L.R. 3-1)

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 467 of 1144
INFOEXPRESS, INC. - EX2572

Pursuant to Patent Local Rule 3-1, Plaintiff InfoExpress Inc. ("InfoExpress") hereby provides the following disclosures to Defendant Cisco Systems, Inc. ("Cisco" or "Defendant") of its asserted claims and infringement contentions, based on the information reasonably available to it at this time.

A. Asserted Claims (Patent L.R. 3-1(a))

InfoExpress currently asserts that Cisco infringes claims of U.S. Patent Nos. 7,523,484 ("the '484 Patent"); 8,051,460 ("the '460 Patent"); 8,677,450 ("the '450 Patent"); 8,578,444 ("the '444 Patent"); 8,347,350 ("the '350 Patent"); and 8,117,645 ("the '645 Patent") (collectively, "the Asserted Patents") as shown in the table below. The claims identified in this section are the "Asserted Claims."

Patent	Claims	Applicable statutory subsections of 35 U.S.C. §271
'484 Patent	1–5, 11–13, 15–20, 23–25, 27-28, 33–35, 38–39, 41-43, 48–50, 53, 57-59, 61-63, 65-66, 68, 71 and 82	35 U.S.C. §271(a) and (b)
'460 Patent	1–6, 10–12, 16–22, and 27	35 U.S.C. §271(a) and (b)
'450 Patent	1–4, 7–9, 11, 14, 16, 22–23, and 25–28	35 U.S.C. §271(a) and (b)
'444 Patent	1–7, 10–14, 17, and 22	35 U.S.C. §271(a) and (b)
'350 Patent	1–2, 4–10, 13, and 18-19	35 U.S.C. §271(a) and (b)
'645 Patent	1–2 and 5–6	35 U.S.C. §271(a) and (b)

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 468 of 1144
INFOEXPRESS, INC. - EX2572

B. Accused Technology (Patent L.R. 3-1(b))

InfoExpress currently asserts that the Cisco products and methods for its Identity Services Engine ("ISE") infringe the Asserted Claims of the Asserted Patents. Cisco's ISE includes infringing hardware and software including:

1. Cisco's ISE software versions:

- Versions 1.0.4, 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3.

2. Cisco's ISE hardware (NAC appliances), including its:

- ISE-3315-K9, ISE-3355-K9, and ISE-3395-K9;
- SNS-3415-K9 and SNS-3495-K9;
- SNS -3515-K9 and SNS-3595-K9;
- SNS-3615-K9, SNS-3655-K9, and SNS-3695-K9;
- SNS-3715-K9, SNS-3755-K9, and SNS-3795-K9; and
- ISE Virtual Machine (S/M/L)-K9.

(Collectively, "Accused Technology").

Information concerning the Accused Technology are disclosed in Cisco's Administrator Guides for ISE versions 2.0 through 3.3 (which have been produced as INFOEX-CSCO_0001603 to 0014308) and in its Release Notes for ISE versions 1.04 through 3.3 (which have been produced as INFOEX-CSCO_0014606 to 0015185).

C. Infringement Claim Charts (Patent L.R. 3-1(c))

Attached are Charts A-F showing infringement of the Asserted Patents, and identifying where each limitation of each Asserted Claim is found in the Cisco Accused Technology.

The contentions set forth in the attached charts are not intended to include all evidence supporting InfoExpress's infringement theories, but rather are intended to provide illustrative instances and preliminary theories of infringement for purposes of discovery, based upon InfoExpress's review to date of publicly available information regarding Cisco's Accused Technology. InfoExpress reserves the right to cite and rely on additional evidence of infringement, as may be discovered from information produced by Cisco, or by third parties, and

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 469 of 1144
INFOEXPRESS, INC. - EX2572

to provide additional instances and theories of infringement based upon such review and discovery. Similarly, references below to instances or portions of technology involved in the infringement of claims of the Asserted Patents should not be construed as limiting or otherwise determining the scope of any claim of the Asserted Patents, or as precluding other instances or portions of such technology or software as being infringing.

D. Indirect Infringement (Patent L.R. 3-1(d))

Based on the information presently known to InfoExpress, and without the benefit of relevant discovery or the Court's claim construction, InfoExpress provides the following contentions pursuant to Patent Local Rule 3-1(d):

1. 35 U.S.C. § 271(b)

In addition to Cisco's direct infringement, InfoExpress also asserts that Cisco induces infringement of the Asserted Claims disclosed in Section I.A, pursuant to 35 U.S.C. § 271(b). The details regarding InfoExpress's allegations of induced infringement are set forth in InfoExpress's Complaint (Dkt. 1), the Joint Case Management Conference statement (Dkt. 26), and the Amended Complaint (including Exhibits G-EE of the Amended Complaint) (Dkt. 38), and which InfoExpress hereby incorporates by reference. Further, this is set forth in Attached Charts A-F and herein below.

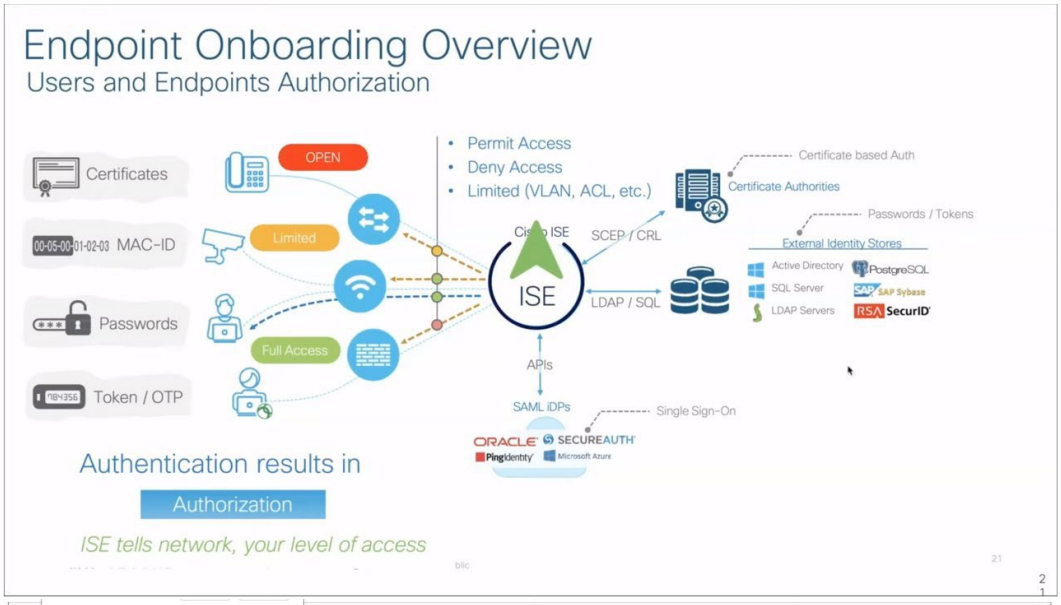
Cisco induces infringement under 35 U.S.C. §271(b) by taking active steps and providing instruction, guidance, and encouragement to cause underlying direct infringement of the Asserted Claims, with both knowledge of the Asserted Patents and with the specific intent to cause, instruct, direct and/or require third parties, including their customers, subscribers, users and developers, to use Cisco's ISE in a manner that directly infringes the Asserted Claims. This includes, but are not limited to:

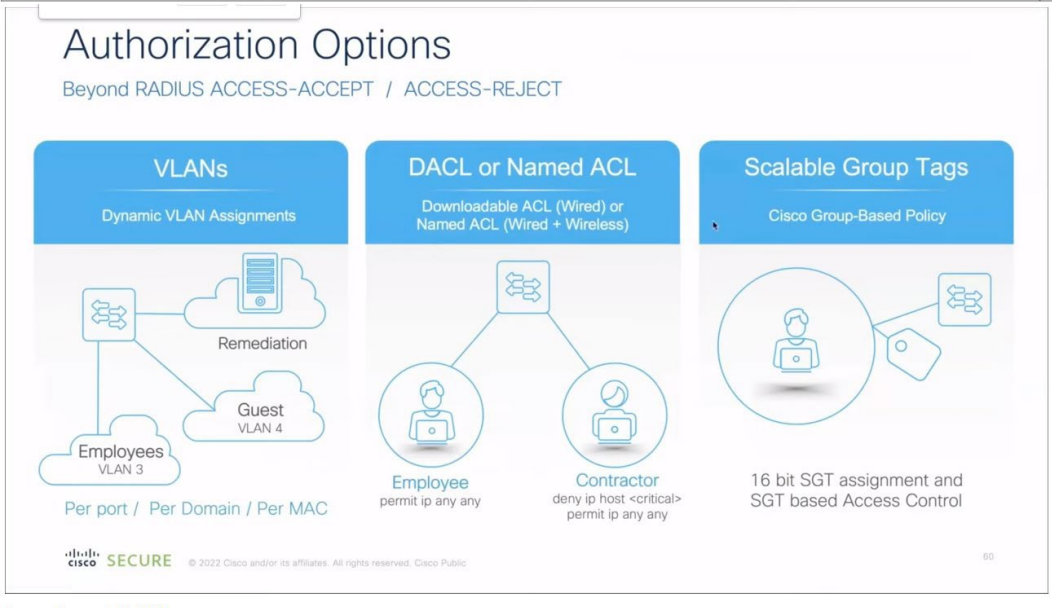
- Instructing third parties such as its customers to install and run ISE software and hardware products, through its literature including its ISE Admin Guide. The ISE Admin

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 470 of 1144
INFOEXPRESS, INC. - EX2572

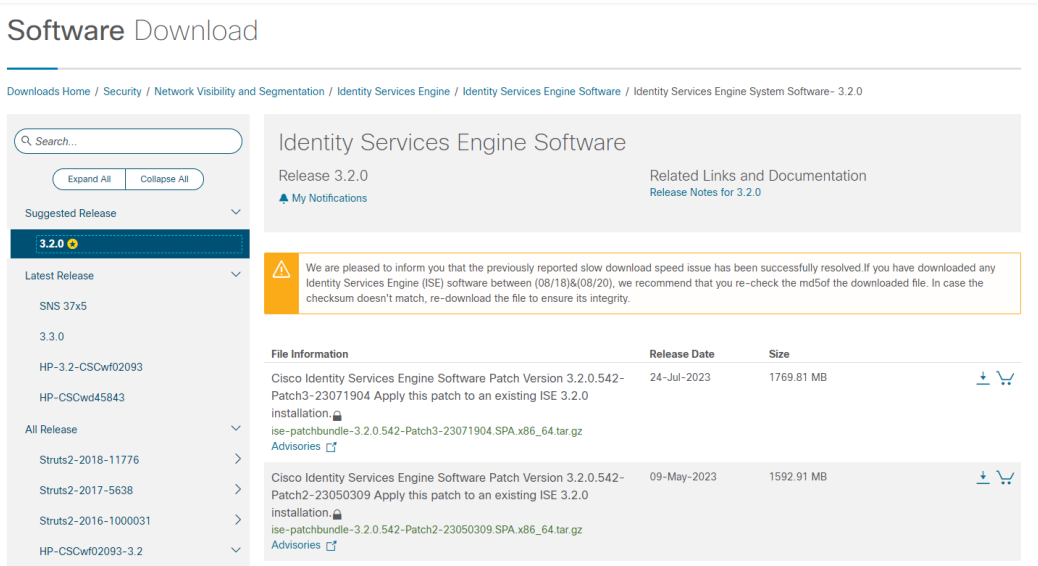
Guide, as shown in the claim charts, contains comprehensive instructions for installing ISE and running it in an infringing manner.

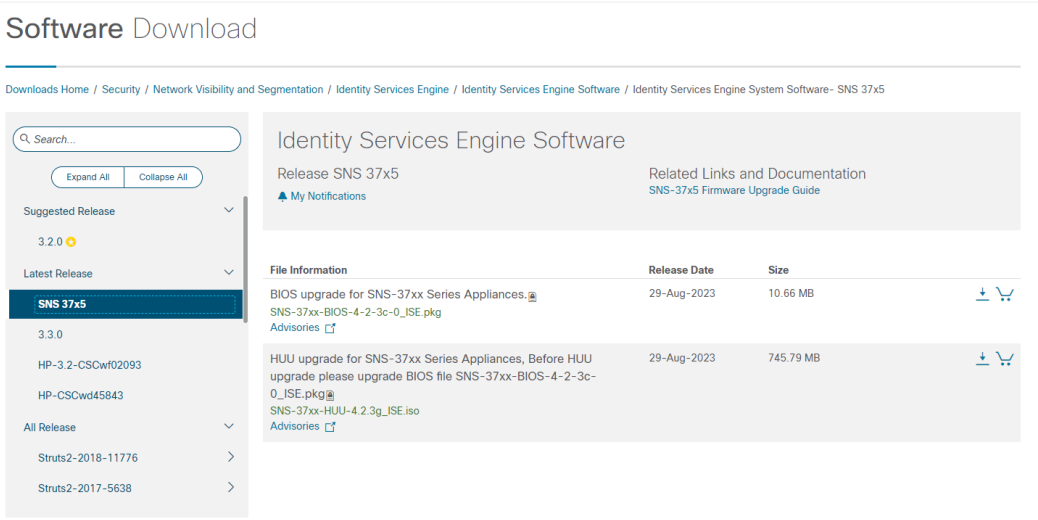
- Encouraging third parties such as its customers to install and run ISE software and hardware products, through webinars, training videos and demonstrations, for example, Cisco, Secure Access with ISE, https://www.youtube.com/watch?v=rjv_1MNUbpM&list=PLvBZXH_IO6nCu9p49Tl1LE4kY6mpyz1eN&index=27, which (as specifically shown in the still images below, taken at 11:44 and 1:02:18), instructs third-party users to use ISE in an infringing manner:





- Encouraging third parties such as its customers to install and run ISE software in an infringing manner, by providing software updates to its ISE through at least its website at https://software.cisco.com/download/home/283801620/type/283802505/release/3.2.0 (last visited September 19, 2023). Here, third parties are permitted to download certain portions of updated ISE (such as software patches). Third parties are also permitted to download updates for their NAC appliances, including their SNS 37x5 models. Users who have these software updates can run ISE software and/or their hardware NAC appliances in an infringing manner.





- Providing product support for ISE to third parties (such as its customers) through its Cisco Support (see, e.g., ***Cisco's Technical Assistance Center*** ("TAC")), whereby users can obtain technical support for their ISE products. Users are instructed to run ISE in an

infringing manner, to generation information in the form of logs of their ISE sessions, and then to upload that information to Cisco personnel for troubleshooting, as shown here:

Collect Support Bundle on Cisco ISE

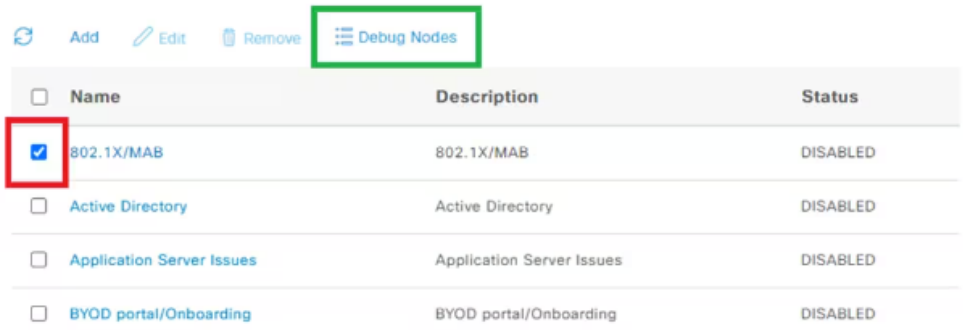
Step 1. Enable Debugs for ISE Components

Various issues on ISE require different sets of logs to troubleshoot. A full list of needed debugs must be provided by the TAC engineer. However, ISE 3.x has preconfigured categories of debugs which you can use to collect initial logos to speed up case resolution.

The list of debugs requested by the TAC engineer must always take priority over this list.

In order to find these preconfigured debugs navigate to **Operations > Troubleshoot > Debug Wizard > Debug Profile Configuration**.

Choose the feature for which debugs must be enabled with the choice of the proper check box at the beginning of each row, for example, 802.1x (red), and navigate to node selection (green):



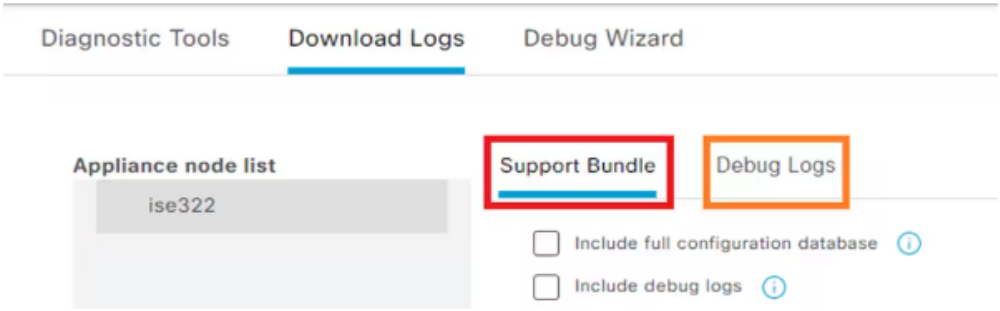
Then choose nodes for which these debugs must be enabled with the choice of the proper checkbox at the beginning of each row (red) and save changes (green):

Debug Nodes

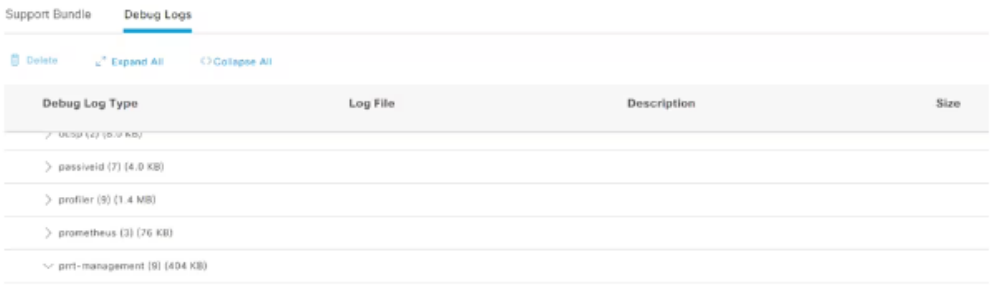
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 473 of 1144
INFOEXPRESS, INC. - EX2572

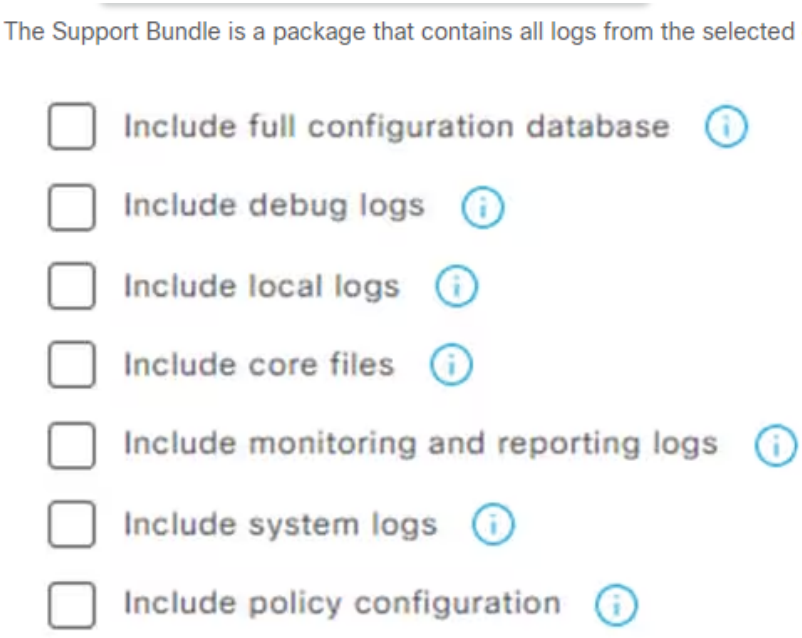
Step 4. Collect Support Bundle

Navigate to **Operations > Troubleshooting > Download Logs** and choose the ISE node (the one, where debugs were enabled). On the tab of each node, there are two options: Collect Support Bundle (red) or download specific log file - Debug Logs (orange).



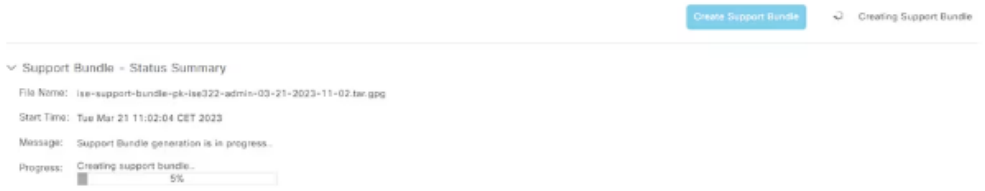
For the Debug Logs, a full list of all available log files is displayed. After you click the name of the file, it is downloaded.





- full configuration database attaches full ISE configuration to the Support Bundle
- debug logs are most used since they contain all the debugs from all ISE components
- local logs contain log that shows Radius authentications for this node in the deployment
- core files can cause the Support Bundle to grow, but it is required during crash troubleshooting
- monitoring and reporting logs contain operational data
- system logs contain system-specific logs (for troubleshooting services provided by OS)
- policy configuration - xml version of configured policies on ISE

When everything is set, click the **Create Support Bundle** button and wait.



When the process to create the Support Bundle is completed, it is available for download. After you click the **Download** button, the Support Bundle is saved on the local disk of the PC and can be uploaded to TAC in order to troubleshoot.

If the Web interface is not available, you can collect the Support Bundle from CLI. In order to do this, log in with the use of SSH or console access and use the command:

```
backup-logs name repository ftp {encryption-key plain key | public-key}
```

name - the name of your Support Bundle

ftp - the name of the repository configured on ISE

key - is the key used for encrypting/decrypting the Support Bundle

The official tool to upload the Support Bundle is https://mycase.cloudapps.cisco.com/case.

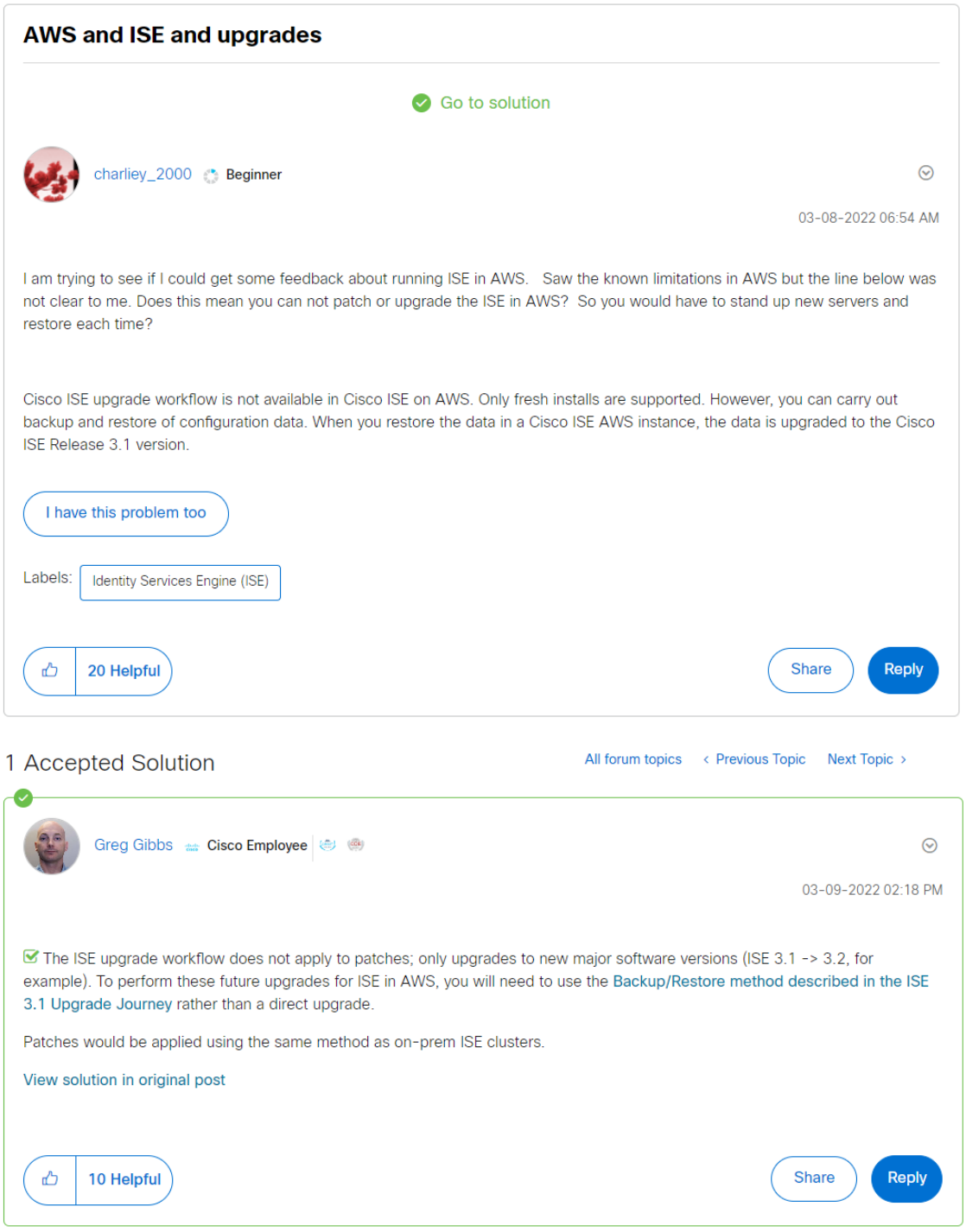
Do not zip or change the extension of the Support Bundle file. It must be uploaded in the same exact state as it was downloaded from ISE.

Revision History

Revision	Publish Date	Comments
2.0	03-May-2023	The content and the images were updated.
1.0	05-Mar-2019	Initial Release

Cisco, *Collect Support Bundle on the Identity Services Engine* https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/214153-collect-support-bundle-on-cisco-identity.html#toc-hId-1103642895 (last visited September 19, 2023).

- Hosting an online community for NAC and ISE support, hosted at https://community.cisco.com/t5/network-access-control/bd-p/discussions-network-access-control, whereby users can pose technical questions about ISE, and others (including Cisco personnel) can answer them, such as in the example below. This technical support encourages Cisco's customers to use ISE in an infringing manner:



AWS and ISE and upgrades

Go to solution

charliey_2000 Beginner

03-08-2022 06:54 AM

I am trying to see if I could get some feedback about running ISE in AWS. Saw the known limitations in AWS but the line below was not clear to me. Does this mean you can not patch or upgrade the ISE in AWS? So you would have to stand up new servers and restore each time?

Cisco ISE upgrade workflow is not available in Cisco ISE on AWS. Only fresh installs are supported. However, you can carry out backup and restore of configuration data. When you restore the data in a Cisco ISE AWS instance, the data is upgraded to the Cisco ISE Release 3.1 version.

I have this problem too

Labels: Identity Services Engine (ISE)

20 Helpful Share Reply

1 Accepted Solution

All forum topics ‹ Previous Topic Next Topic ›

Greg Gibbs Cisco Employee

03-09-2022 02:18 PM

The ISE upgrade workflow does not apply to patches; only upgrades to new major software versions (ISE 3.1 -> 3.2, for example). To perform these future upgrades for ISE in AWS, you will need to use the Backup/Restore method described in the ISE 3.1 Upgrade Journey rather than a direct upgrade.

Patches would be applied using the same method as on-prem ISE clusters.

View solution in original post

10 Helpful Share Reply

E. Literal Infringement and Doctrine of Equivalents (Patent L.R. 3-1(e))

Based on its current investigation, InfoExpress contends that each limitation of each Asserted Claim is literally present in the Accused Technology. InfoExpress reserves the right to apply the doctrine of equivalents to any limitation in the Asserted Claims that Cisco contends is not literally infringed after discovery from Cisco, or as appropriate in response to the Court's legal determination of issues, including without limitation the construction of the Asserted Claims, and as may be determined by any InfoExpress experts in connection with their expert reports.

F. Priority Date (Patent L.R. 3-1(f))

InfoExpress contends that each of the Asserted Claims are entitled to claim priority to U.S. Provisional Patent Application No. 60/503,582, filed on September 24, 2003.

G. InfoExpress's Practice of the Claimed Inventions (Patent L.R. 3-1(g))

InfoExpress contends that its current network access control product called CGX practices one or more of the Asserted Claims.

H. Timing of the point of first infringement, the start of claimed damages, and the end of claimed damages (Patent L.R. 3-1(h))

Patent No.	Patent Issue Date	First Infringement Date	Start of Damages Term	End of Damages Term
[redacted]				
7,523,484	April 21, 2009	April–May 2011	May 31, 2017	February 17, 2027
8,051,460	November 1, 2011	November 1, 2011	May 31, 2017	September 24, 2024
8,677,450	March 18, 2014	March 18, 2014	May 31, 2017	September 24, 2024
8,578,444	November 5, 2013	November 5, 2013	May 31, 2017	September 24, 2024
8,347,350	January 1, 2013	January 1, 2013	May 31, 2017	September 24, 2024
8,117,645	February 14, 2012	February 14, 2012	May 31, 2017	September 24, 2024

I. Willful Infringement (Patent L.R. 3-1(i))

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 478 of 1144
INFOEXPRESS, INC. - EX2572

InfoExpress contends that Cisco willfully infringes the Asserted Patents. The details regarding InfoExpress's allegations of willful infringement are set forth in InfoExpress's Complaint (Dkt. 1), the Joint Case Management Conference statement (Dkt. 26), and the Amended Complaint (including Exhibits G-EE of the Amended Complaint) (Dkt. 38), and which InfoExpress hereby incorporates by reference. Discovery is also ongoing, and InfoExpress reserves the right to supplement this response upon identification of new information.

II. ACCOMPANYING DOCUMENT PRODUCTION (Patent L.R. 3-2)

Pursuant to Patent Local Rule 3-2, InfoExpress is producing concurrently with this disclosure the following documents:

A. Patent L.R. 3-2(a).

There are no documents of which InfoExpress is presently aware.

B. Patent L.R. 3-2(b).

There are no non-privileged documents of which InfoExpress is presently aware. InfoExpress reserves the right to produce and/or rely upon privileged documents evidencing the conception, reduction to practice, design, and development of the inventions claimed in the Patents-in-Suit at the appropriate time and with appropriate safeguards.

C. Patent L.R. 3-2(c).

See INFOEX-CSCO_0000001 to INFOEX-CSCO_0001567.

D. Patent L.R. 3-2(d).

See INFOEX-CSCO_0001568 to INFOEX-CSCO_0001602.

E. Patent L.R. 3-2(e).

See INFOEX-CSCO_0015186 to INFOEX-CSCO_0017110.

F. Patent L.R. 3-2(f).

There are no documents of which InfoExpress is presently aware.

G. Patent L.R. 3-2(g).

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 479 of 1144
INFOEXPRESS, INC. - EX2572

There are no documents of which InfoExpress is presently aware.

H. Patent L.R. 3-2(h).

There are no documents of which InfoExpress is presently aware.

I. Patent L.R. 3-2(i).

See INFOEX-CSCO_0017111 to INFOEX-CSCO_0018446; *and also* INFOEX-CSCO_0016304 to INFOEX-CSCO_0017037.

J. Patent L.R. 3-2(j).

There are no documents of which InfoExpress is presently aware.

InfoExpress and its counsel are continuing their investigation into the facts of this case and discovery is in its early stages. Accordingly, InfoExpress reserves the right to supplement its production of documents responsive to these categories as additional information and documents are obtained in discovery.

Dated: October 2, 2023

Respectfully submitted,

/s/ Brian R. Michalek, Esq.

Brian R. Michalek (SBN 302007) (*pro hac vice*)
brian.michalek@saul.com
Casey T. Grabenstein (*pro hac vice*)
casey.grabenstein@saul.com
Joseph M. Kuo (*pro hac vice*)
joseph.kuo@saul.com
SAUL EWING LLP
161 N. Clark St., Suite 4200
Chicago, IL 60601
Telephone: (312) 876-7100
Facsimile: (312) 876-0288

Andrew Schwerin (*pro hac vice*)
andrew.schwerin@saul.com
Centre Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102 2186
Telephone: (215) 972-7184
Facsimile: (215) 972-7184

Michael E. Flynn-O'Brien (SBN 291301)

Elizabeth Day (SBN 177125)
BUNSOW DE MORY LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: (650) 351-7245
Facsimile: (415) 426-4744
mflynnobrien@bdiplaw.com

Attorneys for Plaintiff InfoExpress Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing document has been served via email on October 2, 2023 to all counsel of record who are deemed to have consented to electronic services via the Court's CM/ECF system.

s/ Andrew Schwerin, Esq.
Andrew Schwerin

EXHIBIT F-1

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Claim 1

	Cisco's Identity Services Engine
[Claim 1-preamble] A network gatekeeper comprising:	Cisco infringes this claim by making, using, testing, offering for sale, and selling the Identity Services Engine ("ISE")[1] product and system and through performance of each of the claimed steps and/or providing instructions and data from its servers to third-parties to perform at least one of the claimed steps. Further, subsequent to Cisco's making, using, testing, offering for sale, and selling of the ISE, Cisco offers services to third-parties and customers with respect to the ISE. For example, these can include "Technical Services," "Advisory Services," and "Cisco Talos Incidence Response" services. (https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/ise-licensing-guide-og.html). For technical services, for example, Cisco encourages customers to purchase "Cisco Smart Net Total Care" for Cisco ISE physical appliances and Software Support (SWSS) contracts for Cisco ISE virtual machines. For advisory services, Cisco offers Expert Services to address "your business objectives with the technology we offer" (including ISE). *Id*. And for the Talos Incident Response, Cisco provides a full suite of proactive and emergency services to help third-parties prepare, respond, and recover from a cybersecurity breach. Cisco explains that third-parties can "order and transact Cisco Talos Incident Response when ordering Cisco ISE subscriptions." *Id*. Additionally, and as set forth in InfoExpress's 3-1 disclosures, Cisco's ISE also includes Cisco's ISE (NAC) appliance. Specifically, these are Cisco-provided tangible hardware and "virtual appliances" on which ISE can be deployed. A list of accused ISE (NAC) Appliances (also referred to as "hardware platforms") which ISE supports, are disclosed in InfoExpress's Disclosure of Asserted Claims and Infringement Contentions per Patent L.R. 3-1 and 3-2 at Section II.B.2. These ISE (NAC) Appliances are listed in Cisco's Identity Services Engine Administrator Guides, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-

[1] Certain portions of the evidence cited herein identify and relate to the Cisco Identity Services Engine, Release version 3.0. We understand that each version of the Accused Technology is operationally and functionally the same with respect to and for the purposes of identifying infringement for each of the Asserted Claims.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	CSCO_0001603 to 0014308, and also their Release Notes for ISE Releases 1.04, 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014606 to 0015185. Cisco's ISE (NAC) appliances are directed to "[g]ranting and denying network access" and using "attributes related to users and their devices" in "determining authorized network access." https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/datasheet-c78-726524.html.[2] Cisco further explains that its NAC appliance (known in one example as "The Cisco Secure Network Server") "supports Cisco's powerful network access and control security applications." *Id.* Further, Cisco explains that the "Cisco Secure Network Server… is configured specifically to support the Cisco Identity Services Engine (ISE) security application." *Id.* To the extent the preamble is limiting, Cisco's ISE is "a security policy management platform that provides secure access to network resources" and thereby grants access to a protected network.

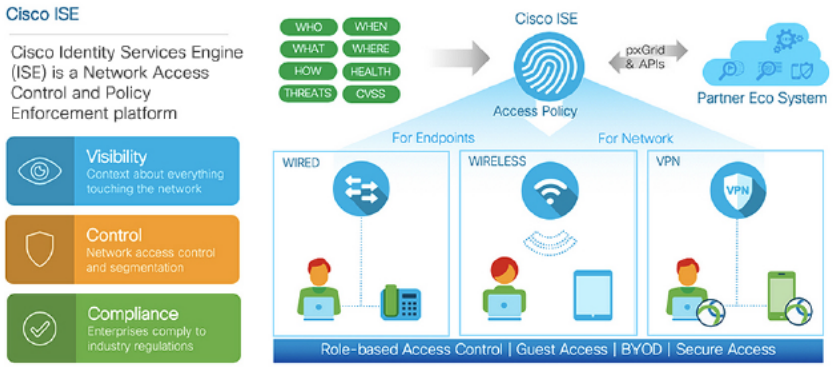
[2] Certain portions of the evidence cited herein identify and relate to the "Cisco Secure Network Server Data Sheet" for Cisco SNS-3715, SNS-3755, and SNS-3795 Secure Network Server. We understand that each other version of the Accused Technology relating to the Cisco ISE (NAC) appliances including ISE-3315-K9, ISE-3355-K9, and ISE-3395-K9; SNS-3415-K9 and SNS-3495-K9; SNS -3515-K9 and SNS-3595-K9; SNS-3615-K9, SNS-3655-K9, and SNS-3695-K9; and ISE Virtual Machine (S/M/L)-K9 are operationally and functionally the same with respect to and for the purposes of identifying infringement for each of the Asserted Claims.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	Introduction to Cisco Identity Services Engine Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, wireless controllers, Virtual Private Network (VPN) gateways, 5GaaS networks, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation. Cisco ISE is available on secure network server appliances with different performance characterizations, and also as software that can be run on a virtual machines (VMs). Note that you can add more appliances to a deployment for better performance. Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also enables the configuration and management of distinct personas and services, thereby giving you the ability to create and apply services, where needed, in a network, but operate the Cisco ISE deployment as a complete and coordinated system. For detailed Cisco ISE ordering and licensing information, see the *Cisco Identity Services Engine Ordering Guide*. For information on monitoring and troubleshooting the system, see the "Monitoring and Troubleshooting Cisco ISE" section in the *Cisco Identity Services Engine Administrator Guide*. Release Notes for Cisco Identity Services Engine, Release 3.0 ("ISE 3.0 Release Notes") at 1, *available at* https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/release_notes/b_ise_30_rn.html (last accessed June 26, 2023). Cisco further describes ISE as a "Network Access Control and Policy Enforcement platform" which thereby grants access to a protected network.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Cisco ISE Overview



Cisco Identity Services Engine (ISE) is an identity-based network access control and policy enforcement system. It functions as a common policy engine that enables endpoint access control and network device administration for enterprises.

You can leverage Cisco ISE to ensure compliance, enhance infrastructure security, and streamline service operations.

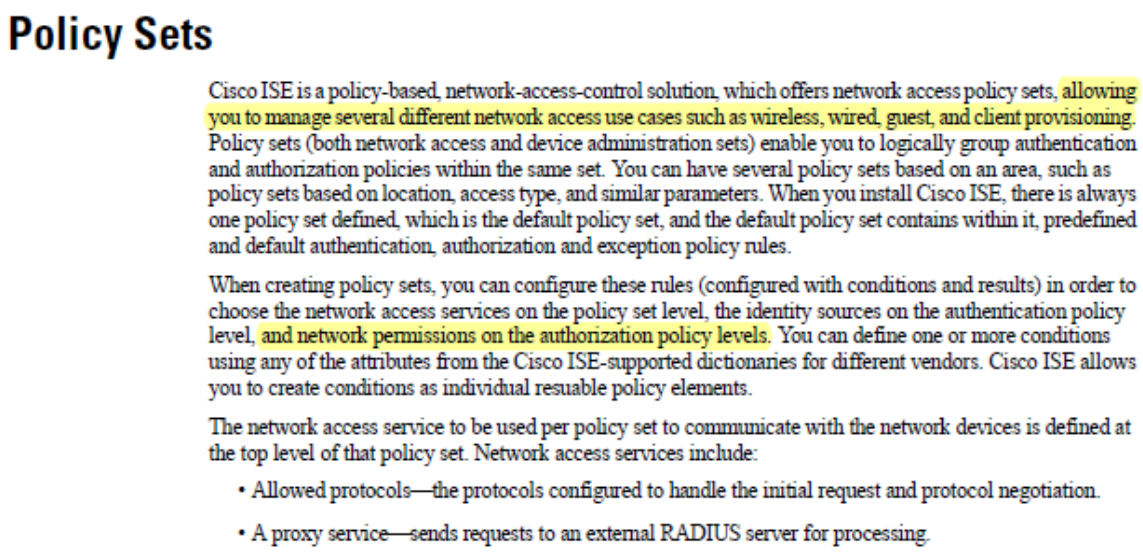
A Cisco ISE administrator can gather real-time contextual data for a network, including users and user groups (who?), device type (what?), access time (when?), access location (where?), access type (wired, wireless, or VPN) (how?), and network threats and vulnerabilities.

Source: Cisco, Identity Services Engine Administrator Guide, Release 3.0 ("ISE 3.0 Admin Guide"), at 1, *available at* https://www.cisco.com/c/en/us/td/docs/security/ise/30/admin_guide /b_ISE_admin_3_0.pdf (last visited May 31, 2023).

Cisco further describes its ISE as permitting different "network permissions on the authorization policy levels[,]" which is thereby a "method of granting access to a protected network."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

<table>
<tr><td></td><td>



Policy Sets

Cisco ISE is a policy-based, network-access-control solution, which offers network access policy sets, allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type, and similar parameters. When you install Cisco ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules.

When creating policy sets, you can configure these rules (configured with conditions and results) in order to choose the network access services on the policy set level, the identity sources on the authentication policy level, and network permissions on the authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE-supported dictionaries for different vendors. Cisco ISE allows you to create conditions as individual resuable policy elements.

The network access service to be used per policy set to communicate with the network devices is defined at the top level of that policy set. Network access services include:

- Allowed protocols—the protocols configured to handle the initial request and protocol negotiation.
- A proxy service—sends requests to an external RADIUS server for processing.

Id. at 856; *see also id.* at 546 ("A user role is a set of permissions that determine what tasks a user can perform and what services they can access on the Cisco ISE network. . . . .Cisco ISE allows you to restrict network access based on user attributes for both network access users and administrators.")</td></tr>
<tr><td>**[1-a]** at least one security policy including requirements that must be satisfied before an access device</td><td>Cisco's ISE comprises "at least one security policy including requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network[.]"

Cisco describes how ISE uses policy sets, through which a user "can configure the[] rules (configured with conditions and results) in order to choose ***the network access*** services on the policy set level[.]" ISE 3.0 Admin Guide at 856. Cisco further describes configuring "rules (configured with conditions and results)" for policy sets—and therefore that ISE comprises "requirements." Furthermore, Cisco describes how ISE describes how one</td></tr>
</table>

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

is granted access to a less-restricted subset of a protected network;	can create policy sets to configure rules for "network permissions on the authorization policy levels." Therefore, ISE comprises "requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network." *Id.* **Policy Sets** Cisco ISE is a policy-based, network-access-control solution, which offers network access policy sets, allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type, and similar parameters. When you install Cisco ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules. When creating policy sets, you can configure these rules (configured with conditions and results) in order to choose the network access services on the policy set level, the identity sources on the authentication policy level, and network permissions on the authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE-supported dictionaries for different vendors. Cisco ISE allows you to create conditions as individual resuable policy elements. The network access service to be used per policy set to communicate with the network devices is defined at the top level of that policy set. Network access services include: • Allowed protocols—the protocols configured to handle the initial request and protocol negotiation. • A proxy service—sends requests to an external RADIUS server for processing. *See also id.* at 2 (ISE uses "policy sets that define authorization, ***access***, and authentication [to] enable[] secure network segmentation").

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

- **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods.
- **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation.
- **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services.

See also ISE 3.0 Admin Guide at 1056-57 (default posture policies); 582 (in Easy Connect Mode, "Cisco ISE issues a CoA to the [network access device ("NAD")] (based on the ***appropriate policy managed in the policy service node***)"and then "the user is provided access by the NAD to the network ***based on that policy***"), 858-59 (Authentication Policies).

Similarly, Cisco explains that (at least with respect to mobile device management (MDM) server integration with ISE), "ISE is the enforcement point . . . [that] then applies the appropriate ***access control policies*** to switches, access routers, wireless access points, and other network access points." Because ISE "applies the appropriate access control policies," to devices that are accessing a "Cisco ISE-enabled network" (and parts thereof, such as the "Corporate Resources" depicted in the figure), it comprises "requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

In the following illustration, Cisco ISE is the enforcement point and the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution.

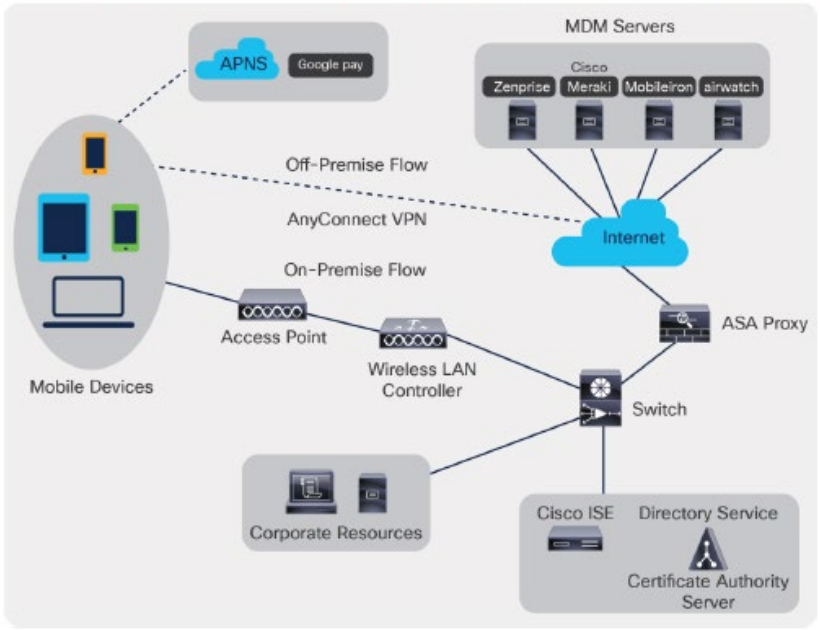


Figure 5.
Cisco ISE and MDM servers

You can configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. It then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network.

Cisco, Randomized and Changing MAC Deployment Guide (2022) ("Randomized and Changing MAC Deployment Guide") at 43, https://www.cisco.com/c/en/us/products/collateral/wireless/randomized-changing-mac-dg.pdf (last visited June 27, 2023).

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

[1-b] a policy auditor configured to audit the access device using the at least one security policy, in response to a request to access the less-restricted subset of the protected network, the request being sent from the access device to the gatekeeper via a communication device; and	Cisco's ISE comprises "a policy auditor configured to audit the access device using the at least one security policy, in response to a request to access the less-restricted subset of the protected network, the request being sent from the access device to the gatekeeper via a communication device[.]" Cisco describes how ISE, generally, "enables [the user] to validate and maintain security capabilities on any client machine that accesses the protected network." ISE 3.0 Admin Guide at 1057; *see also id.* at 2 ("You can also tie identity data to various network elements to ***create policies*** that govern network access and usage."). Because ISE can "validate . . . security capabilities," it can therefore "audit" such a "client machine that accesses the protected network" (that is, the "access device"). *See id.* It therefore contains a "policy auditor" for doing so. ISE's policy auditor is the system(s) and/or apparatus that executes these audits. By way of one example, ISE's auditor perform these audits by formulating and sending requests for certain information to the access devices. ISE can execute these requests by, for example, agents that reside on the access devices: **Client Posture Assessment** To ensure that the imposed network security measures remain relevant and effective, Cisco ISE enables you to validate and maintain security capabilities on any client machine that accesses the protected network. By employing posture policies that are designed to ensure that up-to-date security settings or applications are available on client machines, the Cisco ISE administrator can ensure that any client machine that accesses the network meets, and continues to meet, the defined security standards for enterprise network access. Posture compliance reports provide Cisco ISE with a snapshot of the compliance level of the client machine at the time of user login, as well as any time a periodic reassessment occurs. Posture assessment and compliance occurs using one of the following agent types available in Cisco ISE: • AnyConnect ISE Agent: A persistent agent that can be installed on Windows or Mac OS X client to perform posture compliance functions. • Cisco Temporal Agent: A temporary executable file that is run on the client to check the compliance status. The agent is removed from the client machine after the login session is terminated. By default, the agent resides in the Cisco ISE ISO image, and is uploaded to Cisco ISE during installation. ISE 3.0 Admin Guide at 1057.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Posture Types

The following posture agents monitor and enforce Cisco ISE posture policies:

- **AnyConnect**: Deploys the AnyConnect agent to monitor and enforce Cisco ISE posture policies that require interaction with the client. The AnyConnect agent stays on the client. For more information about using AnyConnect in Cisco ISE, see Cisco AnyConnect Secure Mobility, on page 1099.
- **AnyConnect Stealth**: Runs posture as a service, with no user interface. The agent stays on the client.

When you choose the AnyConnect Stealth posture type in the posture requirement, some of the conditions, remediations, or attributes in a condition are disabled (grayed out). For example, when you enable AnyConnect Stealth requirement, the Manual Remediation Type is disabled (grayed out) because this action requires client-side interaction.

When you map the posture profile to the AnyConnect configuration, and then map the AnyConnect configuration to the Client Provisioning window for AnyConnect Stealth mode deployment:

- AnyConnect can read the posture profile and set it to the intended mode.
- AnyConnect can send information related to the selected mode to Cisco ISE during the initial posture request.
- Cisco ISE can match the right policy, based on the mode and other factors, such as identity group, OS, and compliance module.

. . . .

- **Temporal Agent**: When a client attempts to access the trusted network, Cisco ISE opens the Client Provisioning portal. The portal instructs the user to download and install the agent, and run the agent. The temporal agent checks the compliance status, and sends the status to Cisco ISE. Cisco ISE acts based on the results. The temporal agent removes itself from the client after compliance processing completes. The temporal agent does not support custom remediation. The default remediation supports only message text.

ISE 3.0 Admin Guide at 1010-11; *see also id.* at 1102-03 (Continuous Endpoint Attribute Monitoring mode, whereby for initial posture assessment, the AnyConnect Agent "reports a complete list of running and installed applications" on the access device, after which it "scans the applications [on the access device] every X minute and sends the differences from the last scan to the server").

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Another way by which Cisco's ISE can execute these audit requests is by "agentless posture[, which] ***provides posture information from clients***, and completely removes itself when finished, until invoked by Cisco ISE again." ISE 3.0 Admin Guide at 1012. Cisco further describes how in agentless posture mode, "Posture evaluation runs on the client, and sends the status to Cisco ISE." *Id.* at 1013. *See also and also* Cisco Community, *How To: Agentless Posture Configuration, Validation & Troubleshooting* (Oct. 15, 2020), *available at* https://community.cisco.com/t5/security-knowledge-base/how-to-agentless-posture-configuration-validation-amp/ta-p/4152763 (last visited May 31, 2023).

Agentless Posture

Agentless posture provides posture information from clients, and completely removes itself when finished, until invoked by Cisco ISE again. No action is required from the end user.

Requirements

- The client must be reachable by its IP address, and that IP address must be available in RADIUS accounting. IPv6 is not supported.
- Windows and Mac clients are currently supported.
  - For Windows clients, port 5985 to access Powershell on the client must be open. Powershell must be version 5.1 or later. The client must have cURL version 7.34 or later.
  - For macOS clients, port 22 to access SSH must be open to access the client. The client must have cURL version 7.34 or later.

. . . .

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Agentless Posture Process Flow

1. The client connects to the network.
2. Cisco ISE detects if agentless posture is enabled in the authorization profile used by client.
3. If so, Cisco ISE sends an agentless posture job request to the Cisco ISE Messaging queue.
4. Cisco ISE gets the job from the messaging queue, and starts the agentless posture flow.
5. Cisco ISE connects to the client via power shell or SSH.
6. Cisco ISE pushes the certificate, if it's not already in the client's trust certificate authority store.
7. Cisco ISE runs the client provisioning policy.
8. Cisco ISE pushes the agentless plug-in to the client and launches the plug-in.
9. Posture evaluation runs on the client, and sends the status to Cisco ISE.
10. Cisco ISE removes the agentless plug-in from the client. Logs of the posture flow remain on the client for 24 hours, or until the client deletes them.

ISE 3.0 Admin Guide at 1012-13.

By way of but one example—Easy Connect Enforcement Mode—Cisco describes how "[t]he user logs in to the domain and a ***security audit event*** is sent to Cisco ISE[,]" and then "ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the ***security audit event***." ISE 3.0 Admin Guide at 580-82. Because ISE performs a "security audit event" on the client (the claimed "access device"), it contains a "a policy auditor configured to audit the access device using the at least one security policy[.]"

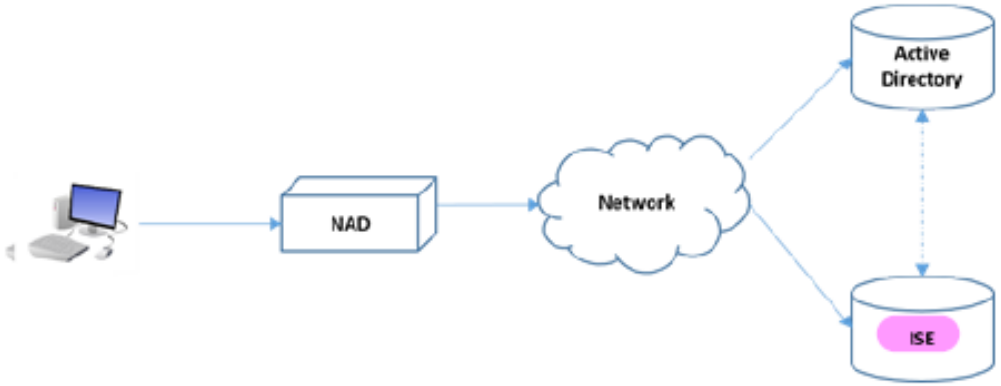
U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Easy Connect Enforcement Mode Process Flow

The Easy Connect Enforcement mode process is as follows:

1. The user connects to the NAD from a wired endpoint (such as a PC for example).
2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD.
3. The user logs in to the domain and a security audit event is sent to Cisco ISE.
4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event.
5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy.

Figure 20: Easy Connect Enforcement Mode Basic Flow



ISE 3.0 Admin Guide at 581.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Finally, Cisco's ISE comprises "the [audit] request being sent from the access device to the gatekeeper via a communication device[.]"

In Cisco's Randomized Changing MAC, it describes generally (in the text and also the schematic) how mobile devices (the claimed "access devices") connect to the network through "switches, access routers, wireless access points, and other network access points" (that is, the "communication devices"). Randomized Changing MAC at 43.

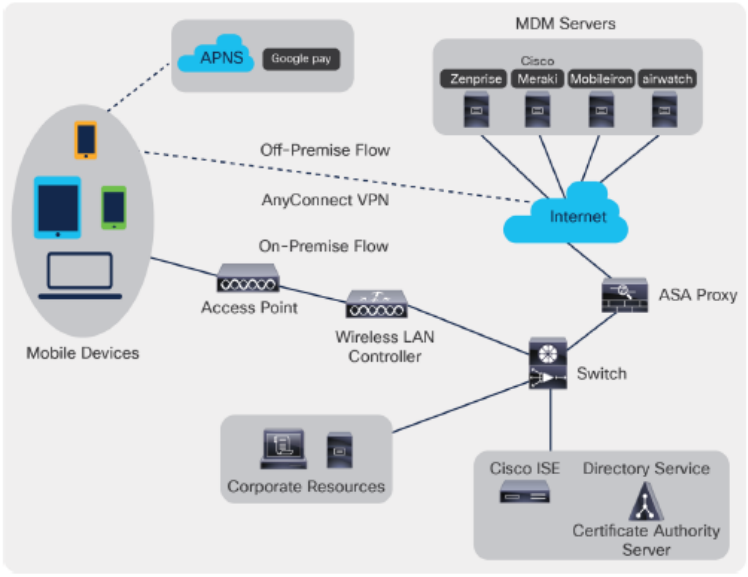


Figure 5.
Cisco ISE and MDM servers

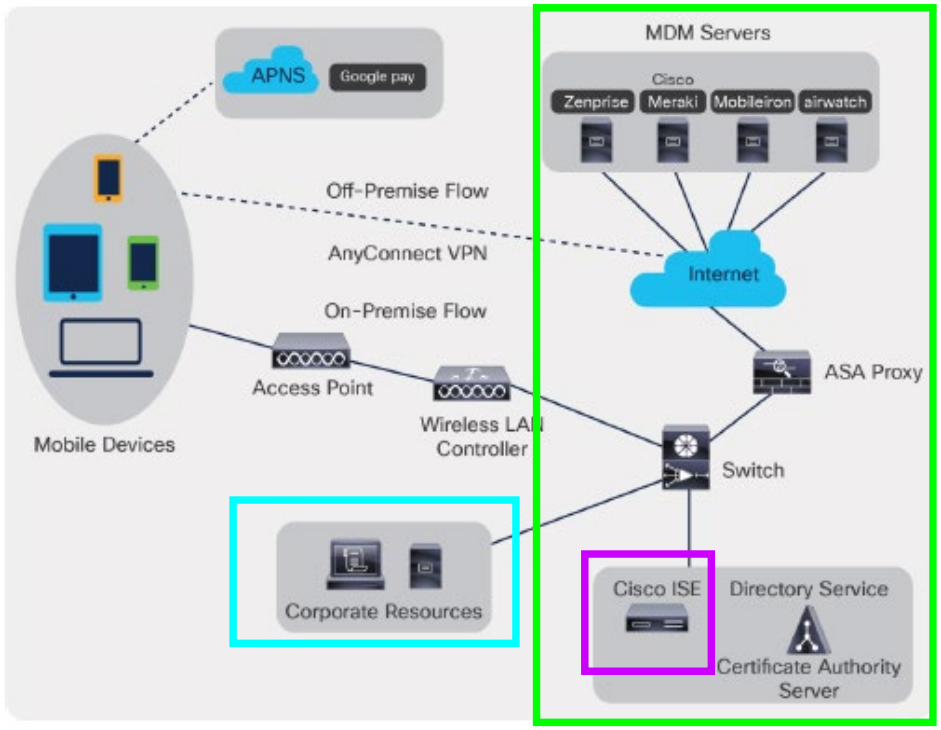
You can configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. It then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

[1-c] an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit results in a determination that the access device meets the requirements of the at least one security policy, the restricted subset of the protected network	Cisco's ISE comprises "an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit results in a determination that the access device meets the requirements of the at least one security policy, the restricted subset of the protected network including the gatekeeper." As shown, if ISE determines that a Mobile Device (that is, the claimed "access device") "meets the requirements of the at least one security policy" it reconfigures the switch or access point (the claimed "communication device") to allow the Mobile Devices access to the Corporate Resources (the claimed "less-restricted subset of the protected network"). Thus, ISE "reconfigure[s] the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit results in a determination that the access device meets the requirements of the at least one security policy[.]" The ISE contains "an access control" that is configured for doing so. Finally, as show in the schematic, the network resources apart from the Corporate Resources (the claimed "restricted subset of the protected network" includes ISE (which further contains the claimed "gatekeeper").

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

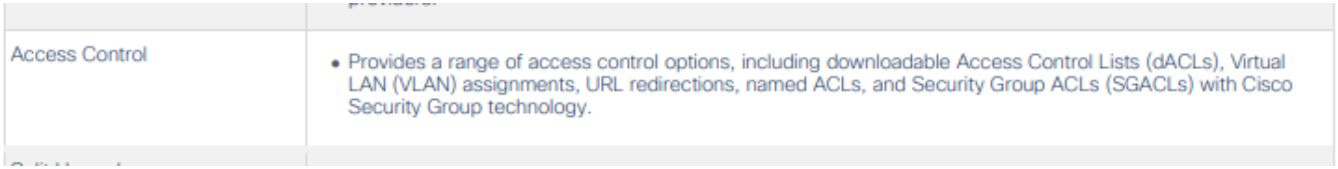
including the gatekeeper.



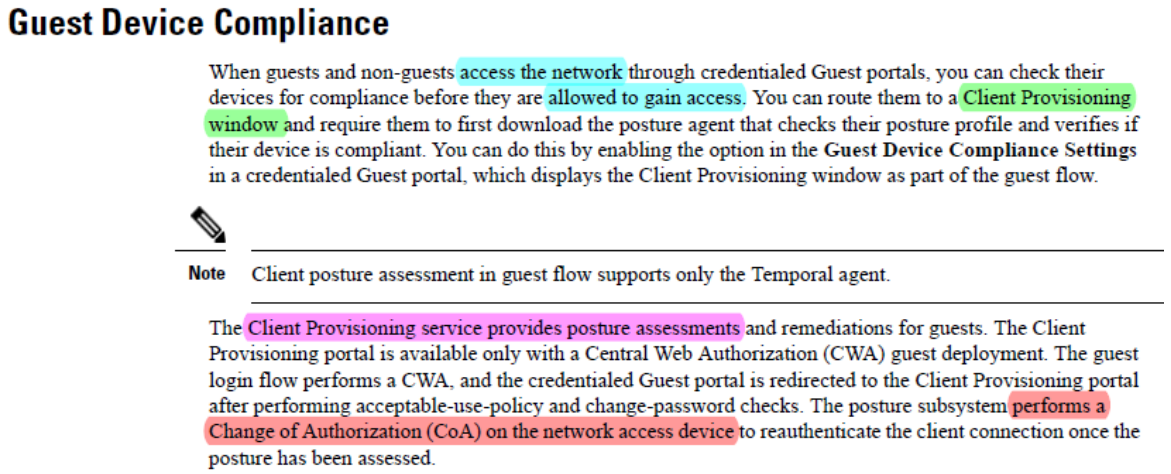
You can configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. It then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network.

Cisco also describes in its ISE Data Sheet "a range of access control options" for this step, "including downloadable Access Control Lists (dACLs), Virtual LAN (VLAN) assignments, URL redirections, named ACLs, and Security Group ACLs (SGACLs) with Cisco Security Group technology[.]" By using any or all of these

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	methods, ISE "reconfigur[es] the communication port for communicating data between the access device and the less-restricted subset of the protected network"—for example, network resources.  Cisco Identity Services Engine Data Sheet (2023) ("ISE Data Sheet") at 5, available at https://www.cisco.com/c/en/us/products/security/identity-services-engine/ise-ds.pdf (last visited September 22, 2023). By way of an example—guest device compliance—Cisco states that "the posture agent [] checks their posture profile and verifies if their device is compliant[,]" and further that "the Client Provisioning service provides posture assessments"—that is, ISE "determine[es] that the access device meets the requirements of the at least one security policy." ISE 3.0 Admin Guide at 401. Upon such "determination," ISE grants the access device access to network resources, and thereby ISE "reconfigures the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network" *See id.* Finally, as show above with respect to MDM servers integrated with ISE, "the restricted subset of the protected network include[es] the gatekeeper[.]" *Id.*

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)



Guest Device Compliance

When guests and non-guests access the network through credentialed Guest portals, you can check their devices for compliance before they are allowed to gain access. You can route them to a Client Provisioning window and require them to first download the posture agent that checks their posture profile and verifies if their device is compliant. You can do this by enabling the option in the **Guest Device Compliance Settings** in a credentialed Guest portal, which displays the Client Provisioning window as part of the guest flow.

Note Client posture assessment in guest flow supports only the Temporal agent.

The Client Provisioning service provides posture assessments and remediations for guests. The Client Provisioning portal is available only with a Central Web Authorization (CWA) guest deployment. The guest login flow performs a CWA, and the credentialed Guest portal is redirected to the Client Provisioning portal after performing acceptable-use-policy and change-password checks. The posture subsystem performs a Change of Authorization (CoA) on the network access device to reauthenticate the client connection once the posture has been assessed.

ISE 3.0 Admin Guide at 401-02.

Another example relates to ISE operating with respect to access points (including both Cisco and third-party, i.e. non-Cisco) access points). ISE "validates endpoint compliance [and] . . . authorizes the "endpoint"—that is, it "determine[es] that the access device meets the requirements of the at least one security policy[.]" ISE 3.0 Admin Guide at 804. After such determination, it "sends the [Change of Authorization] ("CoA")]" and the "guest user receives the appropriate access based on the CoA." By such CoA commands, ISE thereby "reconfigure[s] the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network." Additionally, and as shown in the schematic, the ISE node (which contains the claimed "gatekeeper") is included in "the restricted subset of the protected network[.]"

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

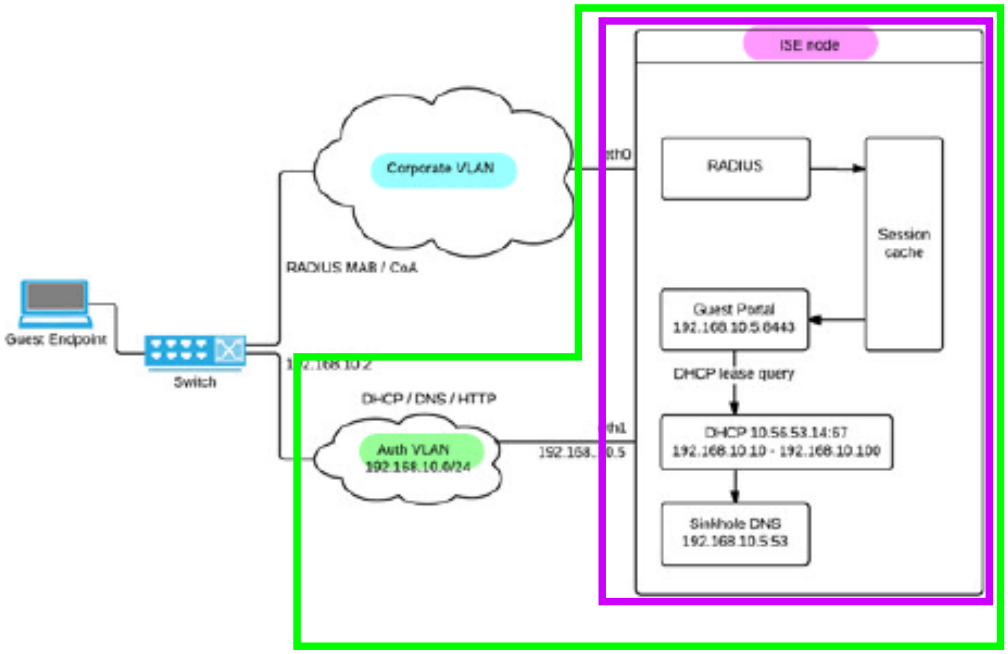
You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

Multiple VLANs may be connected to one network interface card by configuring a VLAN IP helper from the NAD configuration. For more information about configuring an IP helper, see the administration guide for the network device for instructions. For guest access flows that include VLANs with IP helpers, define a guest portal, and select that portal in an authorization profile that is bound to MAB authorization. For more information about guest portals, see the Cisco ISE Guest Services section in *Cisco ISE Admin Guide: Guest and BYOD* .

The following diagram displays a basic network setup when an Auth VLAN is defined (the Auth VLAN is connected directly to a Cisco ISE node).

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

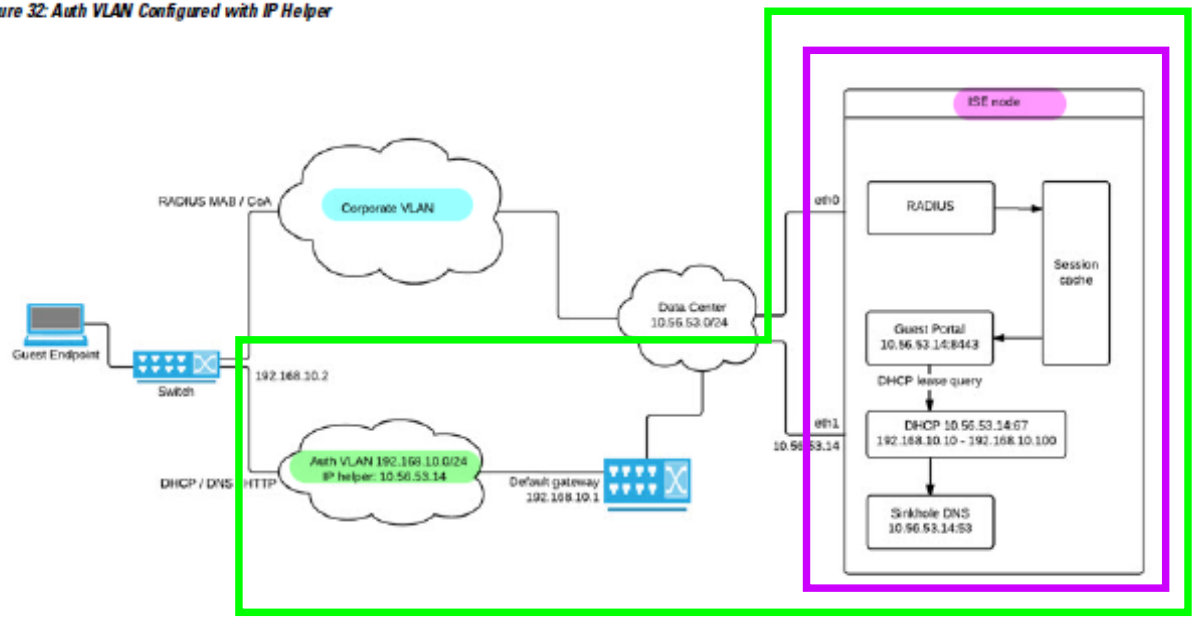
Figure 31: Auth VLAN Connected to Cisco ISE Node



The following diagram displays a network with Auth VLAN and an IP helper.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Figure 32: Auth VLAN Configured with IP Helper



ISE 3.0 Admin Guide at 804-06.

In one further example—ISE's Easy Connect Enforcement Mode—ISE collects certain data, after which it "issues a CoA to the [network access device, ("NAD")] (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy." ISE 3.0 Admin Guide at 580-81. By issuing a CoA to the NAD, to provide the user access to the network, ISE "reconfigure[s] the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network." Additionally, and as shown in the schematic, ISE (which contains the claimed "gatekeeper") is included in "the restricted subset of the protected network[.]"

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

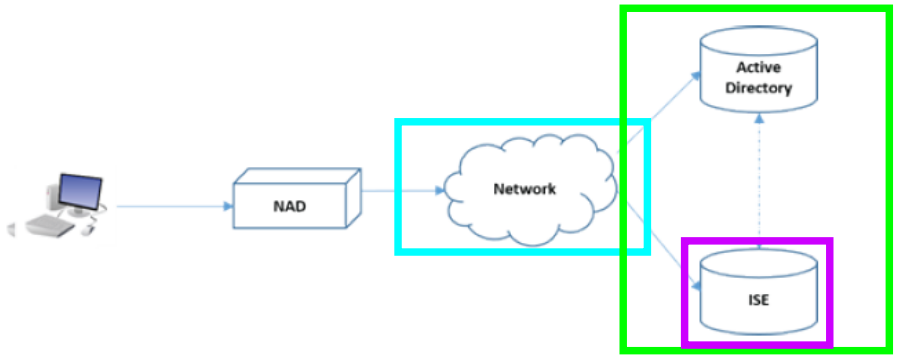
Accordingly, the ISE "reconfigure[s] the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network." Additionally, and as shown in the schematic, the ISE node (the claimed "gatekeeper") is included in "the restricted subset of the protected network[.]"

Easy Connect Enforcement Mode Process Flow

The Easy Connect Enforcement mode process is as follows:

1. The user connects to the NAD from a wired endpoint (such as a PC for example).
2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD.
3. The user logs in to the domain and a security audit event is sent to Cisco ISE.
4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event.
5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy.

Figure 20: Easy Connect Enforcement Mode Basic Flow



U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	In addition to making, using, offering for sale, and selling the ISE, Cisco also induces third-parties to infringe this claim as set forth in InfoExpress's 3-1 disclosures under 35 USC 271(b). For this claim, the underlying direct infringement is caused by the third-parties including Cisco's customers, subscribers, users and developers. And Cisco's acts of induced infringement including the following: as set forth herein, the Release Notes, Admin Guide, Randomized and Changing MAC Deployment Guide and Data Sheets for the ISE are all provided by Cisco to third-parties which provide deliberate and specific instruction and guidance for third-parties to use the ISE in a manner infringed by this claim. In addition, Cisco's Identity Services Engine Administrator Guide ("ISE AG) explains also provide such specific guidance of infringement to third-parties explaining that "[a]dministrators can use the admin portal to: Manage deployments, help desk operations, and network devices, and node monitoring and troubleshooting; Manage Cisco ISE services, policies, administrator accounts, and system configuration and operations." https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/admin_guide/b_ise_admin_3_3/b_ISE_admin_33_overview.html For example, the Admin Guide explains that its audience can be third party administrators ("Cisco ISE administrators can perform various administrative tasks based on the administrative group to which they belong. These administrators are critical. Grant administrative access only to users who are authorized to administer Cisco ISE in your network" ISE 3.0 Admin Guide at 13); developers ("On Facebook, create a Facebook application: a) Log on to http://developers.facebook.com and sign up as a developer," ISE 3.0 Admin Guide at. 397), and it instructs these third-parties on configuring the ISE, for example, with respect to the claimed authentication, compliance, and access point reconfiguration. With respect to this claim, the Admin Guide instructs third-parties how to "Create a Certificate Authentication Profile for TLS-Based Authentication." ISE 3.0 Admin Guide at 269-270. In particular, Cisco instructs these third-parties how to "use certificates for authenticating endpoints that connect to your network" and "defin[ing] a certificate authentication profile in Cisco ISE…" *Id*. In another example, the Cisco's Admin guide instructs third-parties how to apply and/or configure security policies. For example, Cisco explains that the third-parties can "globally configure the Admin portal for posture

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	services." ISE 3.0 Admin Guide at 1015. There, Cisco's Admin guide instructs third-parties how to "download updates automatically to the Cisco ISE through the web from Cisco. *Id*. Further, Cisco explains the various steps for how to "create a posture requirement." Id.. at. 1015-17; *see also id.* at 1066 (Cisco instructing third-parties on "Create[ing] Client Posture Requirements"); *id* at 1067 ("Posture Reassessment Configuration Settings"); *id*. at 1023 ("You can use the Posture Update window to download updates dynamically from the web."); *id.* at 1072 ("Creat[ing] a Posture Condition", "Creat[ing] Posture Remediation."); *id.* at 1073 ("Create Posture Policy"). The ISE AG provides third-parties with an "Administration Portal" which provides third-parties "Policy windows include[ing] tools for managing network security in the areas of authentication, authorization, profiling, posture, and client provisioning." https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/admin_guide/b_ise_admin_3_3/b_ISE_admin_33_basic_setup.html#reference_D93EF6652C8D4EB8B56EC6B857DA6F9A. Further, the ISE AG permits third-parties to create "Posture conditions" by following the following field path at the Administration Portal: "Policy -> Policy Elements -> Conditions -> Posture windows." Id. In another example, Cisco's Admin guide instructs third-parties with respect to "Quarantine [for] a Vulnerable Endpoint." ISE 3.0 Admin Guide at 1127. Specifically, Cisco explains that "You can choose to quarantine the endpoint, provide limited access (redirect to a different portal), or reject the request" and then provides three steps for doing so. *Id*. Similarly, the ISE AG explains to third-parties how they can configure the ISE to "perform the following operations to monitor and control network access through ANC: Quarantine: … Setting to the Quarantine state essentially moves an endpoint from its default VLAN to a specified Quarantine VLAN. You must define the Quarantine VLAN previously that is supported on the same NAS as the endpoint." https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/admin_guide/b_ise_admin_3_3/b_ISE_admin_33_maintain_monitor.html.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

2. The network gatekeeper of claim 1, wherein the network gatekeeper is communicatively coupled with a router configured to limit access to only the restricted subset using an access control list.	Cisco discloses that ISE comprises "[t]he network gatekeeper of claim 1, wherein the network gatekeeper is communicatively coupled with a router configured to limit access to only the restricted subset using an access control list." Cisco makes, uses, sells, and offers for sale a variety of ISE-validated products which customers oftentimes require with its ISE solutions including wireless access points, switches, LAN controllers, routers, servers, and remote access devices. A list of "access points" that are compatible with its ISE—including switches, routers, and remote access devices (i.e. firewalls)—is listed in Cisco's Identity Services Engine Network Component Compatibility documents, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014309 to INFOEX-CSCO_0014605. These Cisco documents describe "Cisco Identity Services Engine (ISE) validated compatibility with switches, wireless LAN controllers, and other policy enforcement devices as well as operating systems with which Cisco ISE interoperates." INFOEX-CSCO_0014586 at 14586. They further state, with respect to "Validated Network Access Devices," that "Cisco ISE supports interoperability with any Cisco or non-Cisco RADIUS client network access device (NAD) that implements common RADIUS behavior (similar to Cisco IOS 12.x) for standards-based authentication." INFOEX-CSCO_0014586 at 14587. These Cisco documents identify the claimed "access points" including both Cisco-made and third-party access points. Cisco also describes ISE-compatible third-party devices in its ISE 3.0 Admin Guide at 806-07, including those made by Aruba, Motorola, HP, Ruckus, Alcatel, Brocade, and Juniper. See also ISE 3.0 Admin Guide at 430 ("The [Wireless LAN Controller ("WLC")] can now log the guest in via the Cisco ISE RADIUS server. When this is complete, the WLC redirects the guest device's browser to the original URL destination. The Wireless LAN Controller (WLC) and the network access devices (NAD) requirements to support the original URL redirect for guest portals are WLC 5760 and Cisco Catalyst 3850, 3650, 2000, 3000, and 4000 Series Access Switches running releases IOS-XE 3.6.0.E and 15.2(2)E."); 874 (Cisco AI Endpoint Analytics receives endpoint attribute data from multiple sources, such as Cisco Catalyst 9000 Series devices[.]"); 697 ("The following devices support sending [Manufacturer Usage Descriptor ("MUD")] data to Cisco ISE: Cisco Catalyst 3850 Series Switches running Cisco IOS XE Version 16.9.1 & 16.9.2[,] Cisco Catalyst Digital Building Series Switches running Cisco IOS Version 15.2(6)E2[, and] Cisco Industrial Ethernet 4000 Series Switches running Cisco IOS Version 15.2(6)E2[.]"); 788 ("Cisco TrustSec-enabled devices use the TrustSec attributes to communicate with

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	Cisco ISE. Cisco TrustSec-enabled devices, such as the Cisco Nexus 7000 Series Switches, Cisco Catalyst 6000 Series Switches, Cisco Catalyst 4000 Series Switches, and Cisco Catalyst 3000 Series Switches are authenticated using the Cisco TrustSec attributes that you define while adding Cisco TrustSec devices."). Cisco further discloses that ISE uses Access Control Lists, or ACLs. ISE 3.0 Admin Guide at 867-68; ISE Data Sheet at 5 ("[ISE] [P]rovides a range of access control options, including ***downloadable Access Control Lists (dACLs)***, Virtual LAN (VLAN) assignments, URL redirections, ***named ACLs***, and ***Security Group ACLs (SGACLs)*** with Cisco Security Group technology." In particular, static ACLs "reside on and are directly configured from the switch." **Downloadable ACLs** Access control lists (ACLs) are lists of access control entries (ACEs), which may be applied by a Policy Enforcement Point (for example, a switch) to a resource. Each ACE identifies the permissions allowed per user for that object, such as read, write, execute and more. For example, an ACL may be configured for use the Sales area of the network, with an ACE allowing Write permissions for the Sales group and a separate ACE allowing Read permissions for all other employees of the organization. With RADIUS protocol, ACLs grant authorization by filtering source and destination IP addresses, transport protocols, and additional parameters. Static ACLs reside on and are directly configured from the switch and can be applied in your

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

authorization policies from the ISE GUI: downloadable ACLs (DACLs) can be configured, managed and applied in your authorization policies from the ISE GUI.

To implement DACLs in your network authorization policy in ISE:

1. Configure a new or existing DACL from **Policy** > **Policy Elements** > **Results** > **Downloadable ACLs**. For more information see Configure Permissions for Downloadable ACLs, on page 868.
2. Configure a new or existing authorization profile from **Policy** > **Policy Elements** > **Results** > **Authorization Profiles**, using any of the DACLs you already configured.
3. Implement the authorization profiles you have configured when creating and configuring new and existing policy sets from **Policy** > **Policy Sets**.

Finally, Cisco describes how routers work with ACLs: "ACLs are applied at the interface of the router." Cisco, Configure and Filter IP Access Lists, https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.pdf (last accessed September 26, 2023). Therefore, Cisco teaches that ISE comprises a "router configured to limit access to only the restricted subset using an access control list."

Apply ACLs

You can define ACLs and still not apply them. But, the ACLs have no effect until they are applied to the interface of the router. It is a good practice to apply the ACL on the interface closest to the source of the traffic. As shown in this example, when you try to block traffic from source to destination, you can apply an inbound ACL to E0 on router A instead of an outbound list to E1 on router C. An access-list has a **deny ip any any** implicitly at the end of any access-list. If traffic is related to a DHCP request and if it is not explicitly permitted, the traffic is dropped because when you look at DHCP request in IP, the source address is s=0.0.0.0 (Ethernet1/0), d=255.255.255.255, len 604, rcvd 2 UDP src=68, dst=67. Notice that the source IP address is 0.0.0.0 and destination address is 255.255.255.255. Source port is 68 and destination 67. Therefore, you must permit this kind of traffic in your access-list or else the traffic is dropped due to implicit deny at the end of the statement.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

<table>
<tr>
<td>3. The network gatekeeper of claim 1, wherein the network gatekeeper is further configured to update the access device using an update module.</td>
<td>Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the network gatekeeper is further configured to update the access device using an update module."

Cisco describes "Posture Remediation Options," and also "Custom Posture Remediation Actions," which include "a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) remediation types." ISE 3.0 Admin Guide at 1059, 1061.

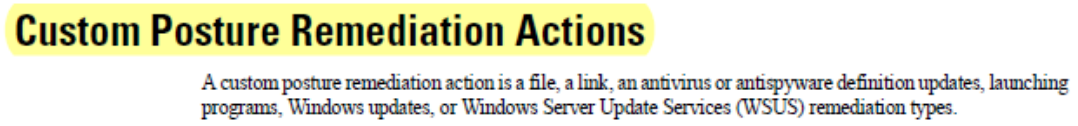
Posture Remediation Options

The following table provides a list of posture remediation options that are supported by the Cisco ISE Posture Agents for Windows and Macintosh, and the Web Agent for Windows.

Table 162: Posture Remediation Options

<table>
<tr><th>ISE Posture Agent for Windows</th><th>ISE Posture Agent for Macintosh OS X</th></tr>
<tr><td>Message Text (Local Check)</td><td>Message Text (Local Check)</td></tr>
<tr><td>URL Link (Link Distribution)</td><td>URL Link (Link Distribution)</td></tr>
<tr><td>File Distribution</td><td>—</td></tr>
<tr><td>Launch Program</td><td>—</td></tr>
<tr><td>Antivirus Definition Update</td><td>Antivirus Live Update</td></tr>
<tr><td>Antispyware Definition Update</td><td>Antispyware Live Update</td></tr>
<tr><td>Patch Management Remediation (AC 4.1 - and ISE 1.4)</td><td>—</td></tr>
<tr><td>Windows Update</td><td>—</td></tr>
<tr><td>WSUS</td><td>—</td></tr>
</table>
</td>
</tr>
</table>

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

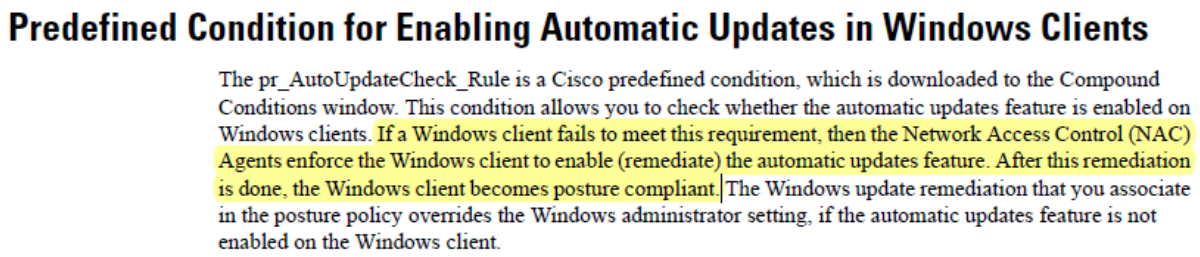


Custom Posture Remediation Actions

A custom posture remediation action is a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) remediation types.

By "remediat[ing]" an endpoint, Cisco ISE "update[s] the access device using an update module." *See also* ISE 3.0 Admin Guide at 1061-64 ("Add an Antispyware Remediation: You can create an antispyware remediation, which ***updates clients*** with up-to-date file definitions for compliance after remediation." and similar disclosures for Antivirus Remediation, File Remediation, Launch Program Remediation, Patch Management Remediation, and others).

See also ISE 3.0 Admin Guide at 1029 (automatic updates in Windows clients):



Predefined Condition for Enabling Automatic Updates in Windows Clients

The pr_AutoUpdateCheck_Rule is a Cisco predefined condition, which is downloaded to the Compound Conditions window. This condition allows you to check whether the automatic updates feature is enabled on Windows clients. If a Windows client fails to meet this requirement, then the Network Access Control (NAC) Agents enforce the Windows client to enable (remediate) the automatic updates feature. After this remediation is done, the Windows client becomes posture compliant. The Windows update remediation that you associate in the posture policy overrides the Windows administrator setting, if the automatic updates feature is not enabled on the Windows client.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	and at 1048-50 (Patch Management Condition Settings):

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Patch Management Condition Settings

The following table describes the fields in the **Patch Management Conditions** window. To view this window, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Patch Management Condition**.

Table 157: Patch Management Condition

Field Name	Usage Guidelines
Name	Enter the name of the patch management condition.
Description	Enter a description for the patch management condition.
Operating System	Choose an operating system to check the installation of a patch management software on the endpoint, or check the latest patch management definition file updates to which the condition is applied. You can select the Windows OS or macOS. You can also select more than one version of an operating system to create the patch management condition.
Vendor Name	Choose a vendor from the **Vendor Name** drop-down list. Based on your selection, the patch management products and their supported versions, check type, and minimum compliant module support details are displayed in the **Products for Selected Vendor** table. The list in the table changes according to the selected operating system.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Field Name	Usage Guidelines
Check Patches Installed	(Available only when you select the **Up To Date** check type) You can configure severity levels for missing patches, which are then deployed based on the severity. Choose one of the following options: • **Critical Only**: To check if critical software patches are installed on the endpoints in your deployment. • **Important and Critical**: To check if important and critical software patches are installed on the endpoints in your deployment. • **Moderate, Important, and Critical**: To check if moderate, important, and critical software patches are installed on the endpoints in your deployment. • **Low To Critical**: To check if low, moderate, important, and critical software patches are installed on the endpoints in your deployment. • **All**: To install the missing patches for all severity levels.

and also Randomized Changing MAC at 44 ("Cisco ISE performs the following functions with the external MDM server: . . . Handles device remediation: Endpoints are granted restricted access during remediation."); *and also* ISE Data Sheet at 4 ("Automated device-compliance checks for device-posture and ***remediation*** options using Cisco Secure Client (formerly Anyconnect agent), Temporal and Agentless options . . ." and 7 ("Supports automatic ***remediation*** of PC clients as well as periodic reassessments . . .")

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Automated device-compliance checks for device-posture and remediation options using Cisco Secure Client (formerly Anyconnect agent), Temporal and Agentless options with custom scripts support. Cisco Secure Client Temporal and Agentless are two different ways to gather posture from endpoints beyond a full agent. Agentless option is supported from ISE 3.0 onwards lo Cisco Secure client also provide advanced VPN services for desktop and laptop checks. ISE also integrates with market-leading Mobile Device Management/Enterprise Mobility Management (MDM/EMM) vendors. MDM integration helps ensure that a mobile device is both secure and policy compliant before it is given access to the network.

. . .

Endpoint posture service	• Performs posture assessments to endpoints connected to the network.
	• Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM.
	• Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media.
	• Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies.
	• Provides hardware inventory for full network visibility.
	• Requires the AnyConnect 4.x agent for posture assessment on these OS platforms:
	  ◦ Windows 10 and later
	  ◦ Mac OS X 10.13 and later
	  ◦ Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu)

ISE Data Sheet at 4, 7.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

4. The network gatekeeper of claim 1, wherein the network gatekeeper is further configured to obtain system data from the access device.	Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the network gatekeeper is further configured to obtain system data from the access device." Above, with respect to claim element **1-b**, Cisco describes various methods within ISE by which the gatekeeper can generally obtain data from the access device, including its AnyConnect Agent (which can "reports a complete list of running and installed applications" on the access device, ISE 3.0 Admin Guide at 1102-03); its AnyConnect Stealth Agent (which reports certain information back to ISE, *id.* at 1010-11), and its agentless posture mode ("provides posture information from clients" and "sends [posture evaluation] status to Cisco ISE," *id.* at 1012-13). With respect to system data, Cisco describes how ISE can obtain the "***hardware attributes of an endpoint***." ISE 3.0 Admin Guide at 174; *see also id.* at 174-5 (listing attributes), 176 ("Cisco ISE profiles the hardware attributes of a client's system, however, there may be a few hardware attributes Cisco ISE does not profile. . . . The hardware inventory data collection interval can be controlled . . . The default interval is 5 minutes.") Also with respect to system data, Cisco describes how ISE can obtain "***endpoint attribute data***" which further includes "Profiling attributes: the Multi-Factor Classification attributes--Hardware Manufacturer, Hardware Model, Operating System, and Endpoint Type[;] Trust Score attributes: Attributes related to Random MAC addresses, profiling changes, spoofing detection, and other behaviors that are monitored by Cisco AI Endpoint Analytics to calculate comprehensive Trust Scores for endpoints.[';] . . . Endpoint Trust Score [and] [Configuration Management Database ("CMDB")] attributes" *Id.* at 874-75; *see also* Randomized Changing MAC at 44 (listing six examples of device attributes). Cisco provides yet another example of "system data" (which the gatekeeper is configured to obtain) in the form of "simple posture conditions," including file conditions, registry conditions, application conditions, service conditions, and USB conditions on the client (the claimed "access device"). *Id.* at 1027.

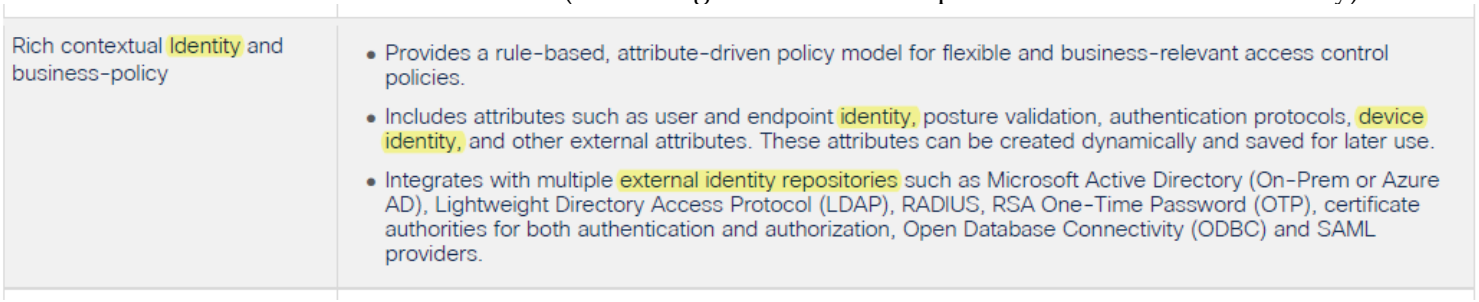
U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	Simple Posture Conditions You can use the **Posture Navigation** pane to manage the following simple conditions: • File Conditions: A condition that checks the existence of a file, the date of a file, and the versions of a file on the client. • Registry Conditions: A condition that checks for the existence of a registry key or the value of the registry key on the client. • Application Conditions: A condition that checks if an application or process is running or not running on the client. **Note** If a process is installed and running, user is compliant. However, the Application condition works in reverse logic; If an application is not installed and not running, the end user is complaint. If an application is installed and running, the end user is non-complaint. • Service Conditions: A condition that checks if a service is running or not running on the client. • Dictionary Conditions: A condition that checks a dictionary attribute with a value. • USB Conditions: A condition that checks for the presence of USB mass storage device.
5. The network gatekeeper of claim 4, wherein the network gatekeeper is further configured to use the system data to	Cisco's ISE comprises "[t]he network gatekeeper of claim 4, wherein the network gatekeeper is further configured to use the system data [of claim 4] to determine if the access device meets requirements of a security policy, and to issue commands responsive to this determination, the commands being configured to grant access to the less-restricted subset. As shown above with respect to claim element **1-c**, Cisco's ISE comprises "an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

determine if the access device meets requirements of a security policy, and to issue commands responsive to this determination, the commands being configured to grant access to the less-restricted subset.	results in a determination that the access device meets the requirements of the at least one security policy, the restricted subset of the protected network including the gatekeeper." Furthermore, with respect to claim 4 are disclosed three examples of "system data" that "the network gatekeeper is further configured to obtain . . . from the access device": hardware attributes, endpoint attribute data, and simple posture conditions. Cisco ISE's "gatekeeper is further configured to use the system data to determine if the access device meets requirements of a security policy, and to issue commands responsive to this determination, the commands being configured to grant access to the less-restricted subset." With respect to the "hardware attributes," Cisco further discloses that one can "check posture compliance" for them. ISE 3.0 Admin Guide at 1032, 1051. Furthermore, "Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network." *Id.* at 2. "By "check[ing] for compliance," ISE "determine[s] if the access device meets requirements of a security policy[.]" With respect to the "endpoint attribute data" , Cisco further discloses that "a Cisco ISE administrator can then create specific authorization rules using these values"—which meet the claimed "requirements of a security policy." *See* ISE 3.0 Admin Guide at 874. It follows that ISE "determine[s] if the access device meets requirements of a security policy[.]" With respect to the "simple posture conditions," Cisco further discloses that generally, "Cisco ISE allows you to check for compliance, also known as posture, of endpoints, ***before allowing them to connect to your network***. ISE 3.0 Admin Guide at 2. Thus by checking compliance i.e. posture, ISE "determine[s] if the access device meets requirements of a security policy[.]" Upon such a "determination" that "the access device meets requirements of a security policy" ISE "issue[s] commands . . . being configured to grant access to the less-restricted subset." Examples of these "commands" are listed with respect to claim 1-c, including Change of Authorization ("CoA") commands.

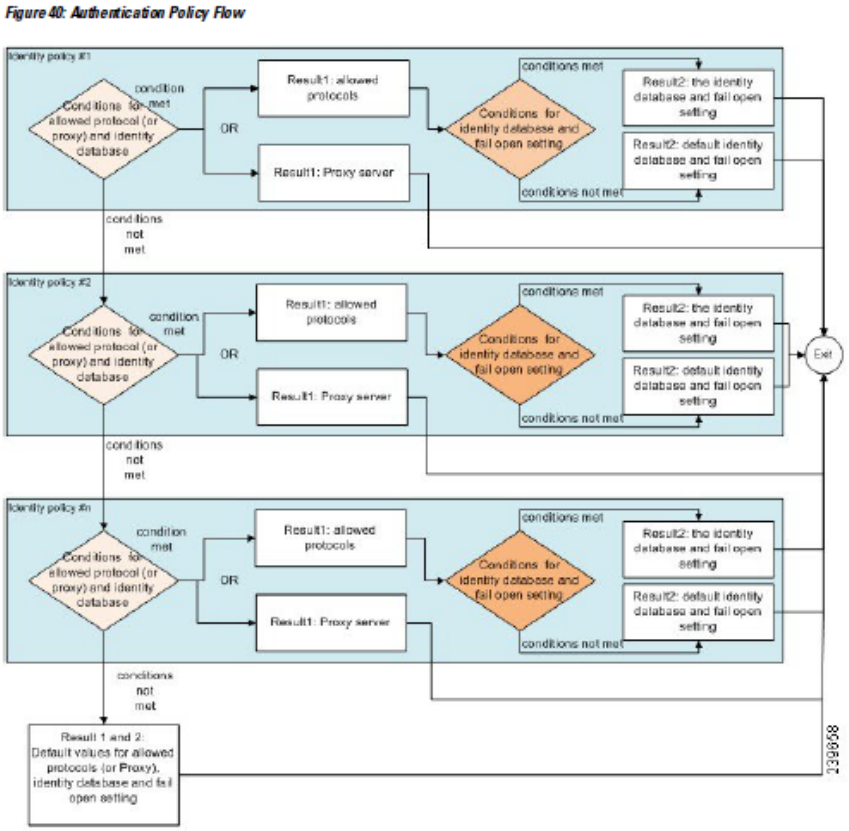
U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

11. The network gatekeeper of claim 1, wherein the at least one security policy is responsive to an identity of the access device.	Cisco's ISE comprises "network gatekeeper of claim 1, wherein the at least one security policy is responsive to an identity of the access device." Cisco describes how ISE generally "can gather real-time contextual data for a network, including ***users and user groups (who?)***"—and thus discloses that it can gather data relating "to an identity of the access device." ISE 3.0 Admin Guide at 2. It follows that ISE comprises "at least one security policy [that] is responsive an identity of the access device." *See also* ISE Data Sheet at 5 (describing features with respect to user and device identity).  Rich contextual Identity and business-policy • Provides a rule-based, attribute-driven policy model for flexible and business-relevant access control policies. • Includes attributes such as user and endpoint identity, posture validation, authentication protocols, device identity, and other external attributes. These attributes can be created dynamically and saved for later use. • Integrates with multiple external identity repositories such as Microsoft Active Directory (On-Prem or Azure AD), Lightweight Directory Access Protocol (LDAP), RADIUS, RSA One-Time Password (OTP), certificate authorities for both authentication and authorization, Open Database Connectivity (ODBC) and SAML providers. Cisco goes on to describe how ISE can employ ***authentication policies*** for determining identity. ISE 3.0 Admin Guide at 858-59.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	Authentication Policies
	
	Each policy set can contain multiple authentication rules that together represent the authentication policy for that set. Priority of the authentication policies is determined based on the order to those policies as they appear within the policy set itself (from the Set view page in the Authentication Policy area).
	
	Cisco ISE dynamically chooses the network access service (either an allowed protocol a server sequence) based on the settings configured on the policy set level, and thereafter checks the identity sources and results from the authentication and authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE dictionary. Cisco ISE allows you to create conditions as individual policy elements that can be stored in the Library and then can be reused for other rule-based policies.
	
	The identity method, which is the result of the authentication policy, can be any one of the following:
	• Deny access—Access to the user is denied and no authentication is performed.
	• Identity database—A single identity database that can be any one of the following:
	  • Internal users
	  • Guest users
	  • Internal endpoints
	  • Active Directory
	  • Lightweight Directory Access Protocol (LDAP) database
	  • RADIUS token server (RSA or SafeWord server)
	  • Certificate authentication profile
	• Identity source sequences—A sequence of identity databases that is used for authentication.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)



ISE 3.0 Admin Guide at 858-59; *see also id.* at 860 (Configure Authentication Policies: Define an authentication policy per policy set by configuring and maintaining multiple authentication rules, as necessary.").

Cisco also explains that with its mobile device management (MDM) server integration with ISE, one can authenticate using a ***Device Unique ID/Global Unique ID (DUID/GUID***).

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

DUID/GUID data flow

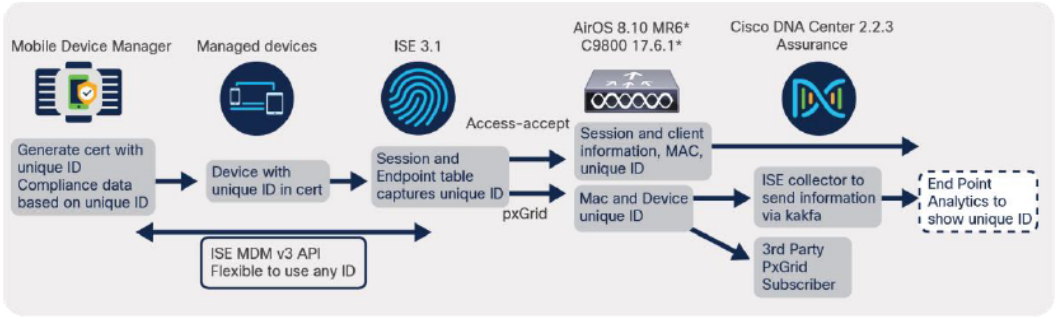


Figure 4.
DUID/GUID data flow

- This solution relies on the mobile device manager, also referred to as a device manager or unified endpoint manager (for example, Cisco Meraki, Airwatch, Intune, MobileIron, etc.), which manage devices in an enterprise infrastructure.
- ISE provides the provisioning of the device with the unique ID-based (DUID) certificates.
- The device presents this certificate during TLS-based authentication. ISE authorizes the devices and also reads the unique ID from the certificate.
- The DUID is used for compliance check with MDM servers and also a unique identifier of the device in the endpoint table.
- The randomized MAC address will not matter, as now the device will have a DUID using the ID in the certificate.

Randomized and Changing MAC Deployment Guide at 42.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Handle random and changing MAC addresses with an MDM server

To avoid issues caused by the use of the MAC address randomization method, configure Cisco ISE to identify endpoints that are connected to an MDM server by a unique device identifier instead of a MAC address. Mobile devices increasingly use random and changing MAC addresses for each SSID. This means that an endpoint presents different MAC addresses to the MDM server and to Cisco ISE. As a result, when the MDM server and Cisco ISE are integrated and an action is initiated for an endpoint, issues arise because the endpoint's identity is different in the two systems.

In Cisco ISE, you can now work around this problem by configuring Cisco ISE to use a unique device identifier instead of MAC addresses. When an endpoint enrolls with an MDM server, the MDM server sends a certificate with a GUID value to the endpoint. The endpoint uses this certificate for authentication with Cisco ISE. Cisco ISE receives the GUID for the endpoint from the certificate. All communications between Cisco ISE and the MDM server now use the GUID to identify the endpoint, helping ensure accuracy and consistency between the two systems.

Note that GUIDs are available only in certificate-based authentication methods. Basic authentication methods that use only a username and password will not be able to leverage the GUID-based solution.

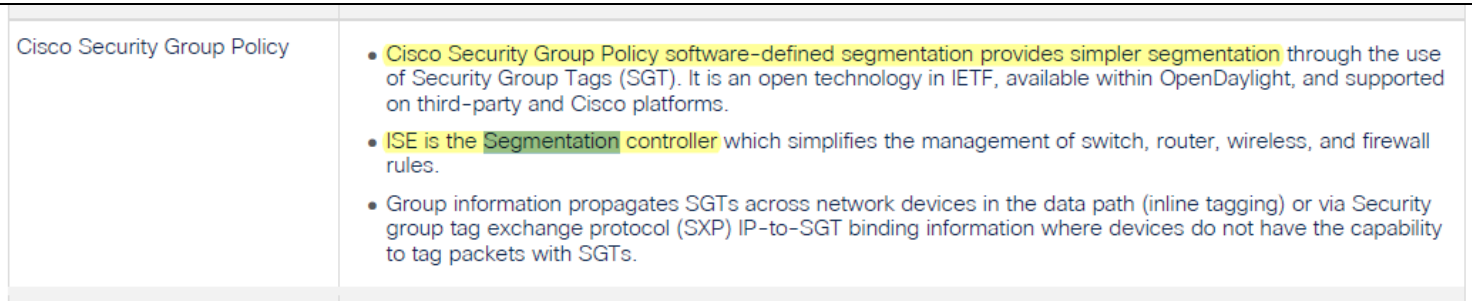
The Cisco ISE MDM APIs have been updated (Cisco ISE MDM APIs Version 3) to facilitate the gathering and management of GUID data. Currently, MobileIron supports Cisco ISE MDM APIs Version 3, and sends GUID information to Cisco ISE.

Randomized and Changing MAC Deployment Guide at 48.

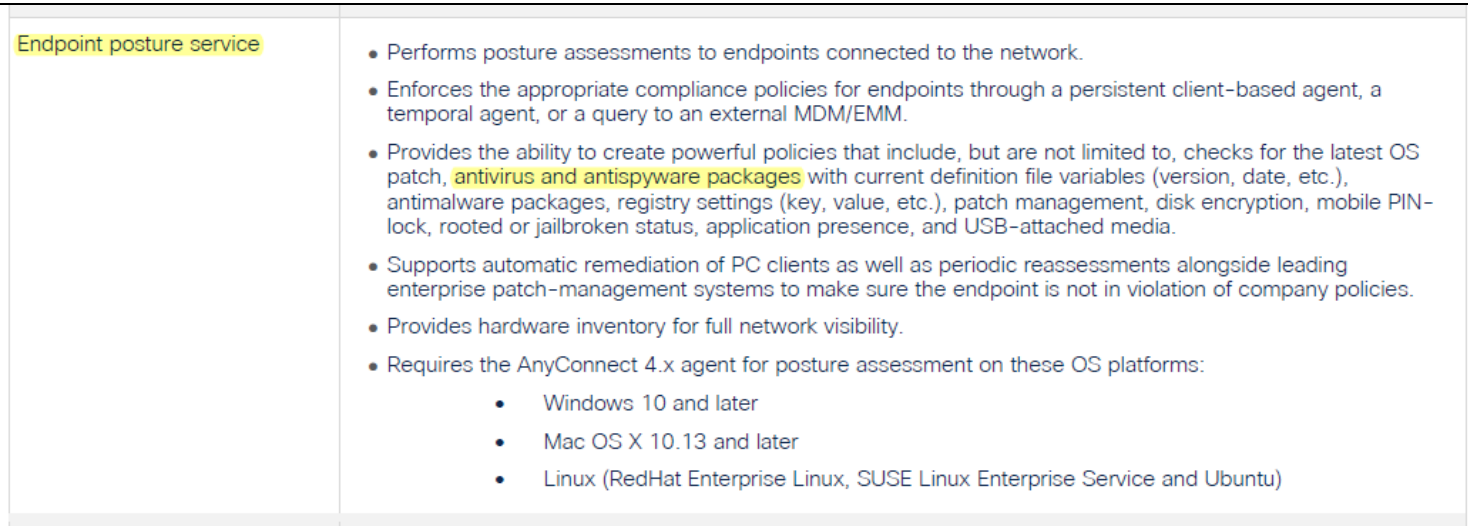
U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

12. The network gatekeeper of claim 1, wherein the at least one security policy is selected by the policy auditor responsive to a part of the less-restricted subset of the protected network to which access is requested.	Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the at least one security policy is selected by the policy auditor responsive to a part of the less-restricted subset of the protected network to which access is requested." Cisco describes how ISE includes a policy auditor which "uses contextual data about network devices and endpoints to facilitate ***network segmentation***. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables ***secure network segmentation***." ISE 3.0 Admin Guide at 2. Because ISE allows comprises "at least one security policy . . . responsive to a part of the less-restricted subset of the protected network"—the "segment" of it, in Cisco's terms, it discloses this claim element. • **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods. • **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation. • **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services. *See also* Cisco ISE Data Sheet at 6.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	
13. The network gatekeeper of claim 1, wherein the audit is responsive to antivirus software executing on the access device.	Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the audit is responsive to antivirus software executing on the access device." Cisco discloses that ISE can assess the posture of access devices (which Cisco terms "endpoints"), which includes assessing their "antivirus" and "antispyware" packages. ISE Data Sheet at 7. Thus, the "the audit is responsive to antivirus software executing on the access device."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	 *See also* ISE 3.0 Admin Guide at 1057-58 (posture assessment options include Antivirus Installation and Antivirus Version/ Antivirus Definition Date).
15. The network gatekeeper of claim 1, wherein the policy auditor is configured to request data from an agent on	Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the policy auditor is configured to request data from an agent on the access device." Cisco discloses "Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure ***that endpoints receive the appropriate posture agents*** for posturing services." ISE 3.0 Admin Guide at 2. Thus, ISE's "policy auditor is configured to request data from an agent on the access device"

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

the access device.

- **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods.
- **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation.
- **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services.

Cisco goes on to explain these posture agents in greater depth:

Posture Types

The following posture agents monitor and enforce Cisco ISE posture policies:

- **AnyConnect**: Deploys the AnyConnect agent to monitor and enforce Cisco ISE posture policies that require interaction with the client. The AnyConnect agent stays on the client. For more information about using AnyConnect in Cisco ISE, see Cisco AnyConnect Secure Mobility, on page 1099.
- **AnyConnect Stealth**: Runs posture as a service, with no user interface. The agent stays on the client.

  When you choose the AnyConnect Stealth posture type in the posture requirement, some of the conditions, remediations, or attributes in a condition are disabled (grayed out). For example, when you enable AnyConnect Stealth requirement, the Manual Remediation Type is disabled (grayed out) because this action requires client-side interaction.

  When you map the posture profile to the AnyConnect configuration, and then map the AnyConnect configuration to the Client Provisioning window for AnyConnect Stealth mode deployment:

  - AnyConnect can read the posture profile and set it to the intended mode.
  - AnyConnect can send information related to the selected mode to Cisco ISE during the initial posture request.
  - Cisco ISE can match the right policy, based on the mode and other factors, such as identity group, OS, and compliance module.

. . . .

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	• **Temporal Agent**: When a client attempts to access the trusted network, Cisco ISE opens the Client Provisioning portal. The portal instructs the user to download and install the agent, and run the agent. The temporal agent checks the compliance status, and sends the status to Cisco ISE. Cisco ISE acts based on the results. The temporal agent removes itself from the client after compliance processing completes. The temporal agent does not support custom remediation. The default remediation supports only message text. . . . . ISE 3.0 Admin Guide at 1010-13; *and also id.* at 1013-15 (agentless posture configuration and troubleshooting).
16. The network gatekeeper of claim 1, wherein the communication device includes a wireless access point.	Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a wireless access point." Cisco explains that with respect to mobile device management (MDM) server integration with ISE, "ISE is the enforcement point . . . [that] then applies the appropriate access control policies to switches, access routers, ***wireless access points***, and other network access points." Randomized and Changing MAC Deployment Guide at 43; *see also* ISE 3.0 Admin Guide at 830 (same); *and also* 363 (The device administrator is the user who logs into the network devices such as switches, ***wireless access points***, routers, and gateways, (normally through SSH), to perform the configuration and maintenance of the administered devices.") Thus the "communication device" includes a "wireless access point."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	You can configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. It then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network. Randomized and Changing MAC Deployment Guide at 43. A list of Cisco hardware products that are compatible with its ISE—including wireless access points—is listed in Cisco's Identity Services Engine Network Component Compatibility documents, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014309 to INFOEX-CSCO_0014605. These Cisco documents describe "Cisco Identity Services Engine (ISE) validated compatibility with switches, wireless LAN controllers, and other policy enforcement devices as well as operating systems with which Cisco ISE interoperates." INFOEX-CSCO_0014586 at 14586.
17. The network gatekeeper of claim 1, wherein the communication device includes a wireless access point configured to support an 802.1x standard.	Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a wireless access point configured to support an 802.1x standard." Above, with respect to claim element 16, Cisco describes various wireless access points. For example, Cisco describes in its Component Compatibility documents for ISE Releases 2.4, 2.6, 2.7, and 3.0 that its Aironet-series access points are "fully supported" to use 802.1X for "AAA" (Authentication, Authorization and Accounting." *See, e.g.*, INFOEX-CSCO_0014479 at INFOEX-CSCO_0014493; *see also* INFOEX-CSCO_0014337; INFOEX-CSCO_0014438; INFOEX-CSCO_0014547. By way of another example, Cisco describes how its Wireless LAN controllers (WLCs)—in conjunction with its 2800 series Lightweight Access Points (LAP) use 802.1x with PEAP as the security mechanism. Cisco, Configure

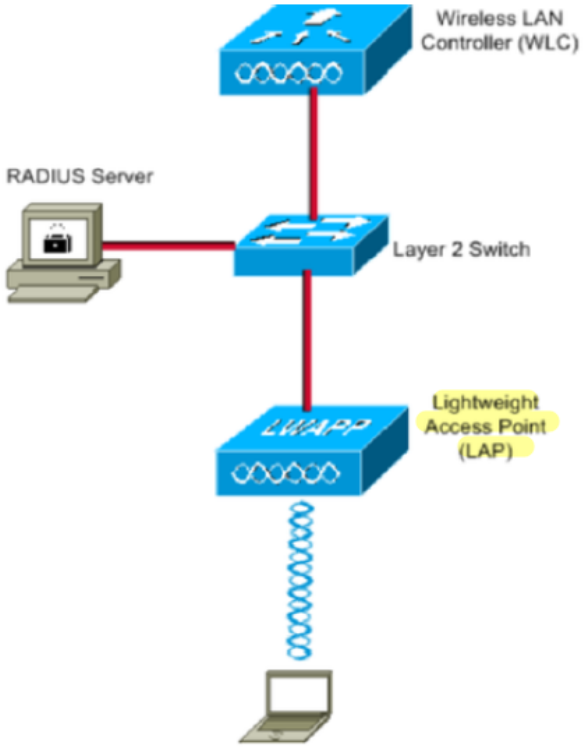
U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	Dynamic VLAN Assignment with ISE and Catalyst 9800 Wireless LAN Controller at 2-3(June 2022), https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/217043-configure-dynamic-vlan-assignment-with-c.pdf (last visited May 22, 2023). • Have functional knowledge on dynamic VLAN assignment. • Have basic knowledge of Control and Provisioning for Wireless Access Point (CAPWAP). **Components Used** The information in this document is based on these software and hardware versions: • Cisco Catalyst 9800 WLC (Catalyst 9800-CL) that runs firmware release 16.12.4a. • Cisco 2800 Series LAP in local mode. • Native Windows 10 supplicant. • Cisco Identity Service Engine (ISE) that runs version 2.7. • Cisco 3850 series switch that runs firmware release 16.9.6. The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command. Cisco, Configure Dynamic VLAN Assignment at 2.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Network Diagram

This document uses this network setup:



These are the configuration details of the components used in this diagram:

- The IP address of Cisco ISE (RADIUS) server is 10.10.1.24.
- The Management Interface address of the WLC is 10.10.1.17.
- The internal DHCP server on the controller is used to assign the IP address to wireless clients.
- This document uses 802.1x with PEAP as the security mechanism.

Cisco, Configure Dynamic VLAN Assignment at 3.

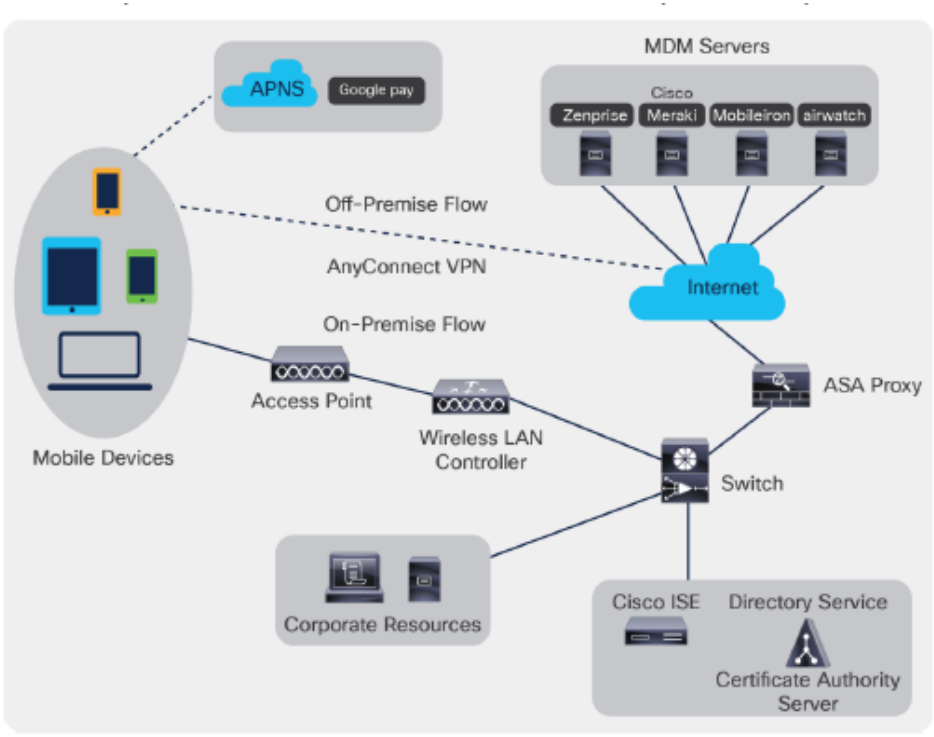
U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

18. The network gatekeeper of claim 1, wherein the communication device includes a network switch.	Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a network switch." Cisco explains that with respect to mobile device management (MDM) server integration with ISE, "ISE is the enforcement point . . . [that] then applies the appropriate access control policies to ***switches***, access routers, wireless access points, and other network access points." Randomized and Changing MAC Deployment Guide at 43; *see also* ISE 3.0 Admin Guide at 830 (same); *and also* 363 (The device administrator is the user who logs into the network devices such as switches, wireless access points, ***routers***, and gateways, (normally through SSH), to perform the configuration and maintenance of the administered devices."), 787 ("A network device, ***such as a switch or a router***, is an authentication, authorization, and accounting (AAA) client that sends AAA service requests to Cisco ISE. Defining network devices in Cisco ISE enables interactions between Cisco ISE and network devices."). Thus the "communication device" includes a "switch." A list of hardware products that are compatible with its ISE—including switches—is listed in Cisco's Identity Services Engine Network Component Compatibility documents, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014309 to INFOEX-CSCO_0014605. These Cisco documents describe "Cisco Identity Services Engine (ISE) validated compatibility with switches, wireless LAN controllers, and other policy enforcement devices as well as operating systems with which Cisco ISE interoperates." INFOEX-CSCO_0014586 at 14586.
19. The network gatekeeper of claim 1, wherein the communication device includes a router.	Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a router." Cisco explains that with respect to mobile device management (MDM) server integration with ISE, "ISE is the enforcement point . . . [that] then applies the appropriate access control policies to switches, ***access routers***, wireless access points, and other network access points." Randomized and Changing MAC Deployment Guide at 43; *see also* ISE 3.0 Admin Guide at 830 (same); *and also* 363 (The device administrator is the user who logs into the network devices such as switches, wireless access points, ***routers***, and gateways, (normally through SSH), to perform the configuration and maintenance of the administered devices."), 787 ("A network device, ***such as a***

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	switch or a router, is an authentication, authorization, and accounting (AAA) client that sends AAA service requests to Cisco ISE. Defining network devices in Cisco ISE enables interactions between Cisco ISE and network devices."). Thus the "communication device" includes a "router." A list of hardware products that are compatible with its ISE—including routers—is listed in Cisco's Identity Services Engine Network Component Compatibility documents, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014309 to INFOEX-CSCO_0014605. These Cisco documents describe "Cisco Identity Services Engine (ISE) validated compatibility with switches, wireless LAN controllers, and other policy enforcement devices as well as operating systems with which Cisco ISE interoperates." INFOEX-CSCO_0014586 at 14586.
20. The network gatekeeper of claim 1, wherein the reconfiguration of the communication device includes reconfiguring a port on the communication device such that data received at the port is passed on to elements of both the less-restricted subset	Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the reconfiguration of the communication device includes reconfiguring a port on the communication device such that data received at the port is passed on to elements of both the less-restricted subset of the protected network and the restricted subset of the protected network." As disclosed above with respect to claim element 1-c, Cisco's ISE comprises "an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit results in a determination that the access device meets the requirements of the at least one security policy, the restricted subset of the protected network including the gatekeeper." Cisco provides examples of "reconfiguring a port on the communication device such that data received at the port is passed on to elements of both the less-restricted subset of the protected network and the restricted subset of the protected network." In Mobile Device Management (MDM),Cisco describes how (with respect to claim element 1-a) that ISE enables Mobile Devices (the claimed "access devices") to access a "Cisco ISE-enabled network" (and parts thereof, such as the "Corporate Resources" depicted in the figure) (the claimed "less-restricted subset of the protected network). Therefore, ISE allows "data received at the port [to be] passed on to elements of [] the less-restricted subset of the protected network."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

of the protected network and the restricted subset of the protected network.	 **Figure 5.** Cisco ISE and MDM servers You can configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. It then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Randomized Changing MAC at 43. Additionally, after access is granted, "ISE polls the MDM server once every four hours to get compliance information and issues the appropriate Change of Authorization (CoA)." *Id.* at 47. Thus, the poll data received "received from the MDM server [regarding] compliance information" constitutes "data" that is passes on to ISE, which is "an element[] of . . . the restricted subset of the protected network.

Step 8. If the user's device is not compliant with the posture (compliance) policies that are configured on the MDM server, the user is notified that the device is out of compliance. The user must take the necessary action to ensure that the device is compliant.

Step 9. When the user's device is compliant, the MDM server updates the device's state in its internal tables.

Step 10. If the user refreshes the browser now, the control is transferred back to Cisco ISE.

Step 11. Cisco ISE polls the MDM server once every four hours to get compliance information and issues the appropriate Change of Authorization (CoA). You can configure the polling interval. Cisco ISE also checks the MDM server every five minutes to make sure that it is available.

The following figure illustrates the MDM process flow.

In another example—continuous endpoint attribute monitoring—Cisco states, "After initial posture [assessment], the AnyConnect agent scans the applications [on the endpoint, i.e. "access device"] every X minute and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications." ISE 3.0 Admin Guide at 1102-03. In this mode, the endpoint ("access device") has satisfied initial posture assessment, and thus "data received at the port is passed on to elements of [] the less-restricted subset of the protected network[.]" By having the agent communicate "the differences from the last scan to the server,"—which can then, in turn, (re)assess posture, the "data received at the port is passed on to elements of . . . the restricted subset of the protected network."

Continuous Endpoint Attribute Monitoring

You can use the AnyConnect agent to continuously monitor different endpoint attributes to ensure that dynamic changes are observed during posture assessment. This improves the overall visibility of an endpoint and helps

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	you create posture policies based on their behavior. The AnyConnect agent monitors applications that are installed and running on an endpoint. You can turn on and off the feature and configure how often the data should be monitored. By default, data is collected every 5 minutes and is stored in the database. During initial posture, AnyConnect reports a complete list of running and installed applications. After initial posture, the AnyConnect agent scans the applications every X minute and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications. ISE 3.0 Admin Guide at 1102-03.
23. The network gatekeeper of claim 1, wherein the network gatekeeper is further configured to authenticate a user of the access device.	Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the network gatekeeper is further configured to authenticate a user of the access device." Cisco's ISE comprises, as described above with respect to claim 11, employing ***authentication policies*** for determining identity. By virtue of using these authentication policies, "the network gatekeeper is further configured to authenticate a user of the access device." *See also* ISE 3.0 Admin Guide at 2 (explaining that for the TACACS+ security protocol, "Network devices can be configured to query Cisco ISE for ***authentication and authorization of device administrator actions***."); *id.* (explaining that for ISE's bring-your-own-device (BYOD) feature, "end users can use configured pathways to add their devices, and ***provision predefined authentications and levels of network access***."); *see also id.* at 183 ("UTF-8 Credential Authentication"), 214 ("Wildcard Certificates for HTTPS and Extensible Authentication Protocol Communication"), 268 (Configure Cisco ISE to Use Certificates for Authenticating Personal Devices); 269 (Create a Certificate Authentication Profile for TLS-Based Authentication); 270 (Create an Identity Source Sequence for TLS-Based Authentication); (275 (Configure the ***Dot1X Authentication Policy*** Rule for TLS-Based Authentication); 276 ("Create Authorization Profiles for ***CentralWeb Authentication*** and Supplicant-Provisioning Flows"); 278-79 ("This section lists the authorization profiles that you must create for enabling ***certificate-based authentication*** in Cisco ISE. You must have already created the ACLs (NSP-ACL and NSP-ACL-Google) on the wireless LAN controller (WLC)."); 280 (Cisco ISE CA Issues Certificates to [Adaptive Security Appliance

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	("ASA")] VPN Users) ("The ASA requests ***certificate-based authentication*** from the client. . . . The ASA proceeds to primary user ***authentication (AAA)*** using the username/ password and passes the information to the ***authentication server (ISE)***."); 354 (discussing exemplary "authentication method[s] that [are] used by the RADIUS protocol"); 428-29 (Guest Access Web Authentication Options); 429-30 (Network Access Devices with Central Web Authentication Process, "In this scenario, the network access device (NAD) makes a new authorization request to the Cisco ISE RADIUS server from an unknown endpoint connection. The endpoint then receives a url-redirect to Cisco ISE. . . . If the guest device is connected to a NAD, the guest service interaction takes the form of a MAC Authentication Bypass (MAB) request that leads to a Guest portal Central WebAuth login. The following is an outline of the subsequent ***Central Web Authentication (Central WebAuth)*** process, which applies to both wireless and wired network access devices."); 430-31 (Wireless LAN Controller with Local Web Authentication Process); 431 (Wired Network Access Device with Local Web Authentication Process); 433-34 (Device Registration Web Authentication Process); 512 ("In Cisco ISE, you can ***authenticate administrators*** via an external identity store such as Active Directory, LDAP, or RSA SecureID."); 513 (External Authentication and Authorization); 635 ("Cisco ISE can authenticate a subject (user or host) against an [Lightweight Directory Access Protocol ('LDAP')] identity source . . ."); 862 (Password-Based Authentication); 1183 (Enable Your Switch to Support StandardWeb Authentication); 1186 (Enable 802.1X Port-Based Authentication for Switch Ports and Enable EAP for Critical Authentications); 1188-90 (Enable Switch Ports for 802.1X and [MAC Authentication Bypass ("MAB")]); 1232-38 ("Live Authentications: "You can monitor recent ***RADIUS authentications*** as they occur . . .").
24. The network gatekeeper of claim 1, wherein the network gatekeeper is configured to update the access device if	Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the network gatekeeper is configured to update the access device if requirements of the security policy are not satisfied." Cisco's ISE comprises, as described above with respect to claim 3, "[t]he network gatekeeper of claim 1, wherein the network gatekeeper is further configured to update the access device using an update module." Furthermore, Cisco describes how such remediation ("updating") takes place "if requirements of the security policy are not satisfied." By way of one example—antispyware remediation—Cisco states that it "***updates clients*** with up-to-date file definitions for compliance after remediation[.]" ISE 3.0 Admin Guide at 1061. Because ISE "updates

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

requirements of the security policy are not satisfied.	clients ***for compliance***" it thereby "is configured to update the access device if requirements of the security policy are not satisfied." *See id.* at 1061-64 (similar disclosures of updates including Antivirus Remediation, Patch Management Remediation, and Windows Server Update Services (WSUS) remediations, and remediation mechanisms including downloading files, launching programs/applications, or accessing remediation resources through a URL link).
25. The network gatekeeper of claim 1, wherein the communication device includes a remote access virtual private network.	Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a remote access virtual private network." Cisco describes how ISE can administer access for communication devices which include VPN connections. ISE 3.0 Admin Guide at 1-2. A Cisco ISE administrator can gather real-time contextual data for a network, including users and user groups (who?), device type (what?), access time (when?), access location (where?), access type (wired, wireless, or VPN) (how?), and network threats and vulnerabilities. . . . . • **Asset Visibility**: Cisco ISE gives you visibility and control over who and what is on your network consistently, across wireless, wired, and VPN connections. Cisco ISE uses probes and device sensors to listen to the way devices connect to the network. The Cisco ISE profile database, which is extensive, then classifies the device. This gives the visibility and context you need to grant the right level of network access. ISE 3.0 Admin Guide at 1-2. Cisco further describes how ISE establishes connections over remote access VPNs:

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Cisco ISE CA Issues Certificates to ASA VPN Users

ISE CA issues certificates to client machines connecting over ASA VPN. Using this feature, you can automatically provision certificates to end devices that connect over ASA VPN.

Cisco ISE uses the Simple Certificate Enrollment Protocol (SCEP) for enrollment and to provision certificates to the client machines. The AnyConnect client sends the SCEP request to the ASA over an HTTPS connection. The ASA evaluates the request and enforces policies before it relays the request to Cisco ISE over an HTTP connection established between Cisco ISE and ASA. The response from the Cisco ISE CA is relayed back to the client. The ASA cannot read the contents of the SCEP message and functions as a proxy for the Cisco ISE CA. The Cisco ISE CA decrypts the SCEP message from the client and sends the response in an encrypted form.

The ISE CA SCEP URL is http://*<IP Address or FQDN of ISE CA server>*:9090/auth/caservice/pkiclient.exe. If you are using FQDN of the ISE node, the DNS server connected to ASA must be able to resolve the FQDN.

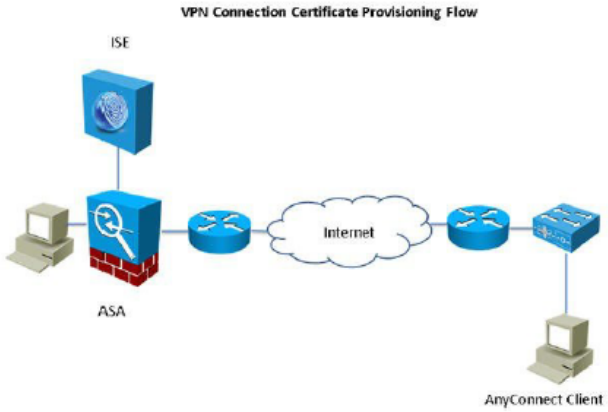
You can configure certificate renewal before expiration in the AnyConnect Client profile. If the certificate has already expired, the renewal flow is similar to a new enrollment.

Supported versions include:

- Cisco ASA 5500 Series Adaptive Security Appliances that run software version 8.x
- Cisco AnyConnect VPN version 2.4 or later

VPN Connection Certificate-Provisioning Flow

Figure 10: Certificate Provisioning for ASA VPN Users



1. The user initiates a VPN connection.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	2. The AnyConnect client scans the client machine and sends the attributes such as the unique device identifier (for example, IMEI) to the ASA. 3. The ASA requests certificate-based authentication from the client. The authentication fails because there is no certificate. 4. The ASA proceeds to primary user authentication (AAA) using the username/password and passes the information to the authentication server (ISE). a. If authentication fails, the connection is terminated immediately. b. If authentication passes, limited access is granted. You can configure dynamic access policies (DAP) for client machines that request a certificate using the aaa.cisco.sceprequired attribute. You can set the value for this attribute to "true" and apply ACLs and web ACLs. 5. The VPN connection is established after the relevant policies and ACLs are applied. The client starts key generation for SCEP only after AAA authentication succeeds and the VPN connection is established. 6. The client starts the SCEP enrollment and sends SCEP requests to ASA over HTTP. 7. ASA looks up the session information of the request and relays the request to ISE CA, if the session is allowed for enrollment. 8. ASA relays the response from ISE CA back to the client. 9. If enrollment succeeds, the client presents a configurable message to the user and disconnects the VPN session. 10. The user can again authenticate using the certificate and a normal VPN connection is established. ISE 3.0 Admin Guide at 280-81, *see also id.* at 281-84 (Configure Cisco ISE CA to Issue Certificates to ASA VPN Users).

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

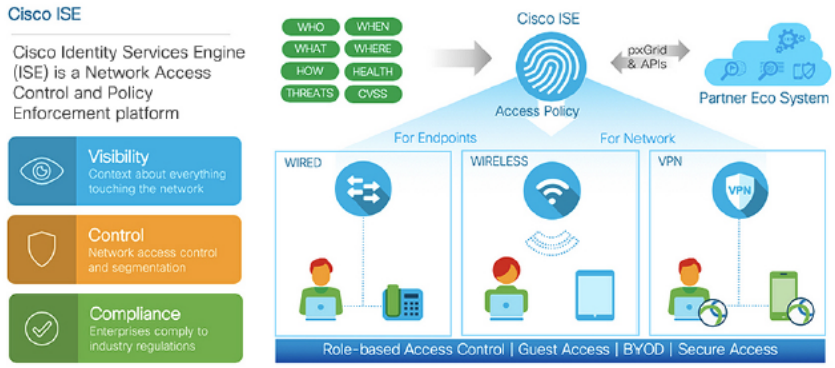
Claim 27

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

[27-preamble] A method of granting access to a protected network, the method comprising:	Cisco infringes this claim by making, using, testing, offering for sale, and selling the ISE product and system and through performance of each of the claimed steps and/or providing instructions and data from its servers to third-parties to perform at least one of the claimed steps, or induces others to do so as set forth in claim element 1-c. To the extent the preamble is limiting, Cisco's Identity Services Engine ("ISE") is "a security policy management platform that provides secure access to network resources" and thereby grants access to a protected network. **Introduction to Cisco Identity Services Engine** Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, wireless controllers, Virtual Private Network (VPN) gateways, 5GaaS networks, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation. Cisco ISE is available on secure network server appliances with different performance characterizations, and also as software that can be run on a virtual machines (VMs). Note that you can add more appliances to a deployment for better performance. Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also enables the configuration and management of distinct personas and services, thereby giving you the ability to create and apply services, where needed, in a network, but operate the Cisco ISE deployment as a complete and coordinated system. For detailed Cisco ISE ordering and licensing information, see the *Cisco Identity Services Engine Ordering Guide*. For information on monitoring and troubleshooting the system, see the "Monitoring and Troubleshooting Cisco ISE" section in the *Cisco Identity Services Engine Administrator Guide*. ISE 3.0 Release Notes at 1. Cisco further describes ISE as a "Network Access Control and Policy Enforcement platform" which thereby grants access to a protected network.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Cisco ISE Overview



Cisco Identity Services Engine (ISE) is an identity-based network access control and policy enforcement system. It functions as a common policy engine that enables endpoint access control and network device administration for enterprises.

You can leverage Cisco ISE to ensure compliance, enhance infrastructure security, and streamline service operations.

A Cisco ISE administrator can gather real-time contextual data for a network, including users and user groups (who?), device type (what?), access time (when?), access location (where?), access type (wired, wireless, or VPN) (how?), and network threats and vulnerabilities.

ISE 3.0 Admin Guide, at 1.

Cisco further describes its ISE as allowing a user "to choose . . . the network permissions on the authorization policy levels[,]" which is thereby a "method of granting access to a protected network."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Policy Sets

Cisco ISE is a policy-based, network-access-control solution, which offers network access policy sets, allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type, and similar parameters. When you install Cisco ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules.

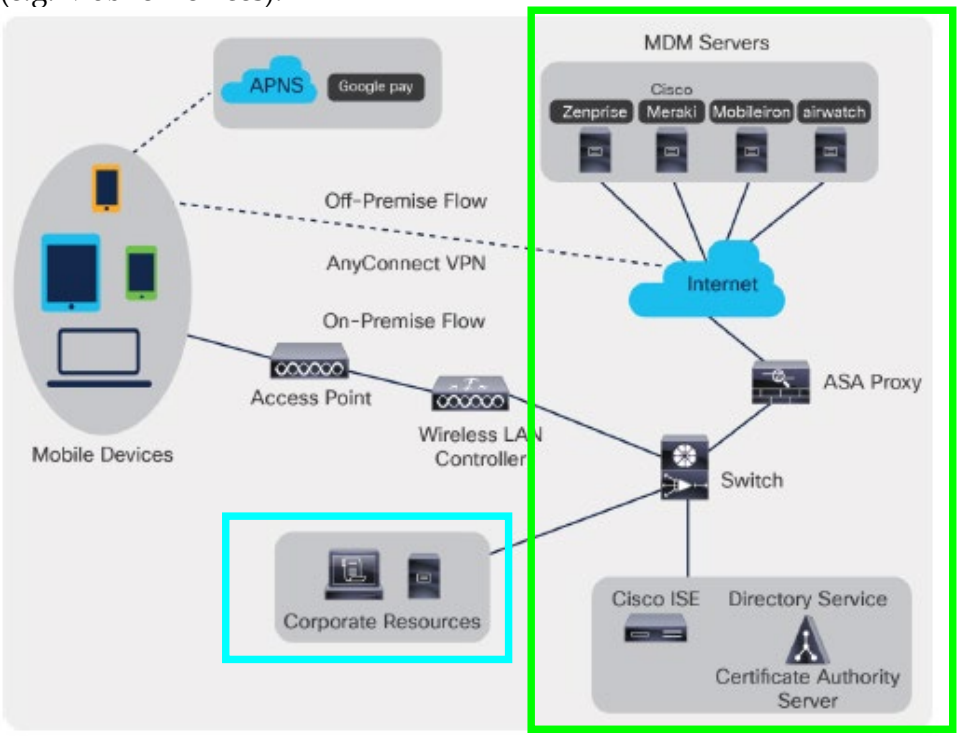
When creating policy sets, you can configure these rules (configured with conditions and results) in order to choose the network access services on the policy set level, the identity sources on the authentication policy level, and network permissions on the authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE-supported dictionaries for different vendors. Cisco ISE allows you to create conditions as individual resuable policy elements.

The network access service to be used per policy set to communicate with the network devices is defined at the top level of that policy set. Network access services include:

- Allowed protocols—the protocols configured to handle the initial request and protocol negotiation.
- A proxy service—sends requests to an external RADIUS server for processing.

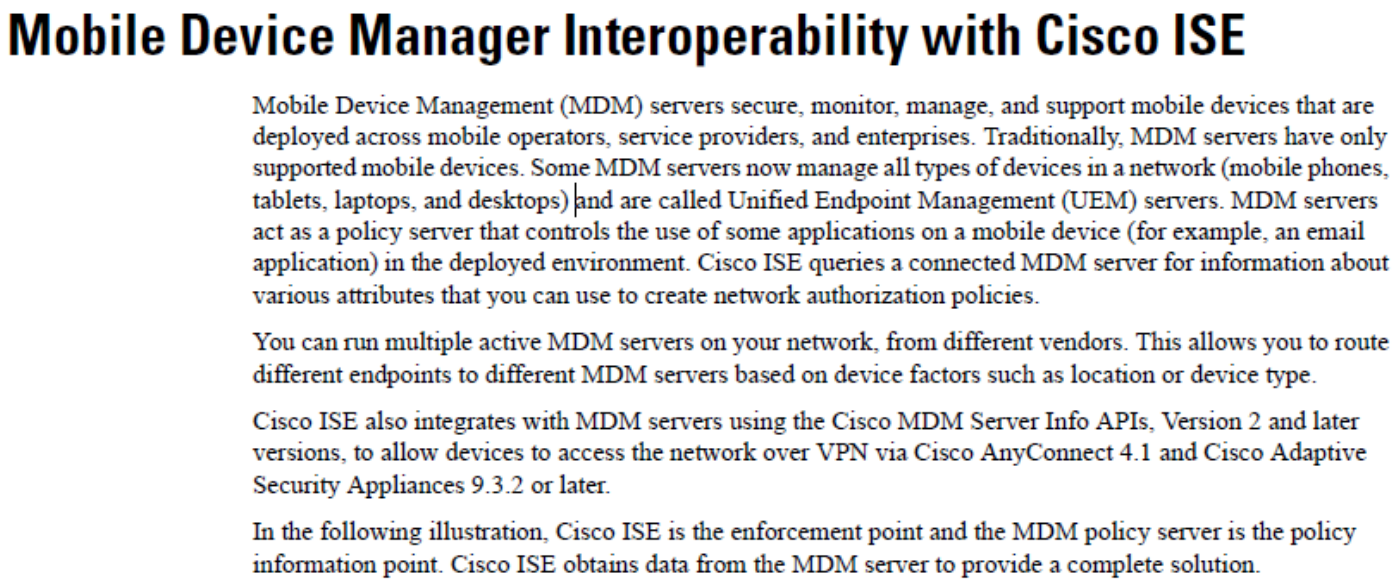
Id. at 856; *see also id.* at 546 ("A user role is a set of permissions that determine what tasks a user can perform and what services they can access on the Cisco ISE network. . . . .Cisco ISE allows you to restrict network access based on user attributes for both network access users and administrators.")

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

[27-a] receiving a request for access to a less-restricted subset of the protected network from an access device, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper;	Cisco ISE "receiv[es] a request for access to a less-restricted subset of the protected network from an access device," or induces others to do so. In this step, the Cisco ISE receives a request for a less restricted subset of the protected network (blue) from a user access device—for example, a mobile phone, tablet, or laptop computer (e.g. Mobile Devices).  Randomized and Changing MAC Deployment Guide at 43,

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Cisco also describes in its ISE 3.0 Admin Guide how Mobile Device Management (MDM) servers "secure, monitor, manage, and support mobile devices that are deployed across mobile operators, service providers, and enterprises. Traditionally, MDM servers have only supported mobile devices. Some MDM servers now manage ***all types of devices in a network (mobile phones, tablets, laptops, and desktops)***[.]"



Mobile Device Manager Interoperability with Cisco ISE

Mobile Device Management (MDM) servers secure, monitor, manage, and support mobile devices that are deployed across mobile operators, service providers, and enterprises. Traditionally, MDM servers have only supported mobile devices. Some MDM servers now manage all types of devices in a network (mobile phones, tablets, laptops, and desktops) and are called Unified Endpoint Management (UEM) servers. MDM servers act as a policy server that controls the use of some applications on a mobile device (for example, an email application) in the deployed environment. Cisco ISE queries a connected MDM server for information about various attributes that you can use to create network authorization policies.

You can run multiple active MDM servers on your network, from different vendors. This allows you to route different endpoints to different MDM servers based on device factors such as location or device type.

Cisco ISE also integrates with MDM servers using the Cisco MDM Server Info APIs, Version 2 and later versions, to allow devices to access the network over VPN via Cisco AnyConnect 4.1 and Cisco Adaptive Security Appliances 9.3.2 or later.

In the following illustration, Cisco ISE is the enforcement point and the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution.

ISE 3.0 Admin Guide at 830.

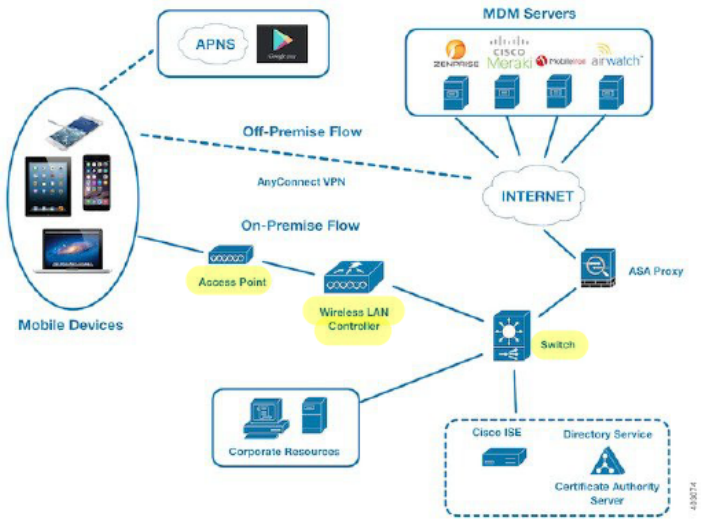
Cisco describes how the "access devices" that send "request[s] for access" are termed "endpoints" in Cisco's language. An endpoint is "typically a network-capable device that connect[s] to your network through wired and wireless network access devices and VPN. Endpoints can be personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, and so on." ISE 3.0 Admin Guide at 730; *see also id.* at 101

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	("Here, an endpoint could mean users, PCs, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, or other types of network devices."); 765 ("For example, a user registers a laptop with wired and wireless addresses."). Cisco further describes how the "request [for access] [is] received through a communication port of an access point[.]" Cisco's "access points" include its "switches, access routers, wireless access points, and other network access points." ISE 3.0 Admin Guide at 830.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Figure 33: MDM Interoperability with Cisco ISE



Configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. Cisco ISE applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network.

See also Randomized and Changing MAC Deployment Guide at 43 (same); *see also* ISE 3.0 Admin Guide at 363 ("The device administrator is the user who logs into the network devices such as ***switches, wireless access points, routers, and gateways***, (normally through SSH), to perform the configuration and maintenance of the administered devices.").

A list of "access points" that are compatible with its ISE—including switches, routers, and remote access devices (i.e. firewalls)—is listed in Cisco's Identity Services Engine Network Component Compatibility documents, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014309 to INFOEX-CSCO_0014605. These Cisco documents describe "Cisco Identity Services Engine (ISE) validated

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	compatibility with switches, wireless LAN controllers, and other policy enforcement devices as well as operating systems with which Cisco ISE interoperates." INFOEX-CSCO_0014586 at 14586. They further state, with respect to "Validated Network Access Devices," that "Cisco ISE supports interoperability with any Cisco or non-Cisco RADIUS client network access device (NAD) that implements common RADIUS behavior (similar to Cisco IOS 12.x) for standards-based authentication." INFOEX-CSCO_0014586 at 14587. These Cisco documents identify the claimed "access points" including both Cisco-made and third-party access points. Cisco also describes ISE-compatible third-party devices in its ISE 3.0 Admin Guide at 806-07, including those made by Aruba, Motorola, HP, Ruckus, Alcatel, Brocade, and Juniper. *See also* ISE 3.0 Admin Guide at 430 ("The [Wireless LAN Controller ("WLC")] can now log the guest in via the Cisco ISE RADIUS server. When this is complete, the WLC redirects the guest device's browser to the original URL destination. The Wireless LAN Controller (WLC) and the network access devices (NAD) requirements to support the original URL redirect for guest portals are WLC 5760 and ***Cisco Catalyst 3850, 3650, 2000, 3000, and 4000 Series Access Switches*** running releases IOS-XE 3.6.0.E and 15.2(2)E."); 874 (Cisco AI Endpoint Analytics receives endpoint attribute data from multiple sources, such as ***Cisco Catalyst 9000 Series devices***[.]"); 697 ("The following devices support sending [Manufacturer Usage Descriptor ("MUD")] data to Cisco ISE: Cisco Catalyst 3850 Series Switches running Cisco IOS XE Version 16.9.1 & 16.9.2[,] Cisco Catalyst Digital Building Series Switches running Cisco IOS Version 15.2(6)E2[, and] Cisco Industrial Ethernet 4000 Series Switches running Cisco IOS Version 15.2(6)E2[.]"); 788 ("Cisco TrustSec-enabled devices use the TrustSec attributes to communicate with Cisco ISE. Cisco TrustSec-enabled devices, such as the Cisco Nexus 7000 Series Switches, Cisco Catalyst 6000 Series Switches, Cisco Catalyst 4000 Series Switches, and Cisco Catalyst 3000 Series Switches are authenticated using the Cisco TrustSec attributes that you define while adding Cisco TrustSec devices."). Cisco describes in its ISE 3.0 Admin Guide an example where the request for access is received through a Cisco or third-party (that is, a non-Cisco) access point (termed a "network access device") in Cisco's literature. ISE 3.0 Admin Guide at 803-06.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Third-Party Network Device Support in Cisco ISE

Cisco ISE supports third-party network access devices (NADs) by using network device profiles. A NAD profile defines the capabilities of a third-party device with a simplified policy configuration, regardless of the vendor-side implementation. A network device profile contains the following:

- The protocols that the network device supports, such as RADIUS, TACACS+, and Cisco TrustSec. You can import into Cisco ISE any vendor-specific RADIUS dictionaries that exist for the network device.
- The attributes and values that the device uses for various authentication flows such as Wired MAB and 802.1X. These attributes and values allow Cisco ISE to detect the right authentication flow for your device according to the attributes that the network device uses.
- The Change of Authorization (CoA) capabilities of the network device. While the RADIUS protocol RFC 5176 defines a CoA request, the attributes used in a CoA request vary depending on the network device. Most non-Cisco devices with RFC 5176 support the *Push* and *Disconnect* functions. For devices that do not support the RADIUS CoA type, Cisco ISE also supports SNMP CoA.
- The attributes and protocols that the network device uses for MAB flows. Network devices from different vendors perform MAB authentication differently.
- The VLAN and ACL permissions that are used by the device. When you save the profile, Cisco ISE automatically generates authorization profiles for each configured permission.

Furthermore, in ISE, the "request [for access is] received through a ***communication port*** of an access point."

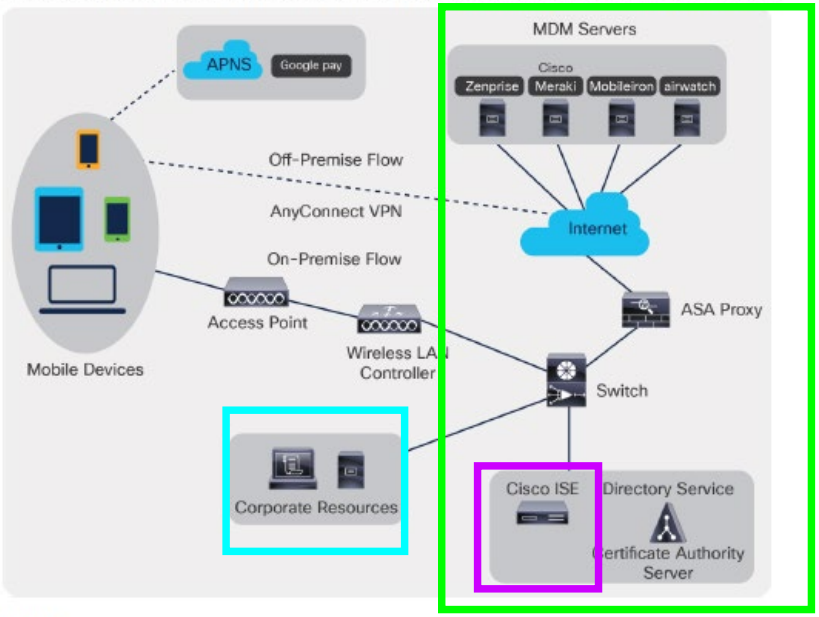
U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.
Endpoint Profile	Shows the type of endpoint that is profiled, for example, profiled to be an iPhone, Android, M Xbox, and so on.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
Authorization Profiles	Shows the authorization profile that was used for authentication.
IP Address	Shows the IP address of the endpoint device.
Network Device	Shows the IP address of the Network Access Device.
Device Port	Shows the port number at which the endpoint is connected.
Identity Group	Shows the identity group that is assigned to the user or endpoint, for which the log was genera
Posture Status	Shows the status of posture validation and details on the authentication.
Server	Indicates the policy service from which the log was generated.

ISE 3.0 Admin Guide at 354; *see also id.* at 359 (similar disclosure with respect to TACACS live logs); 377 (similar); 882 ("You can create the following unique network conditions to restrict access to the network: . . . Device Port Network Conditions—Based on the device's IP address, name, NDG, and ***port (physical port of the device*** that the endstation is connected to)."); 900 ("Configure Device Port Network Condition"); 1188-89 ("enable switch ports for 802.1X and MAB"); 1230 (with respect to RADIUS live logs, the "Device Port" field "[s]hows the port number at which the endpoint is connected"); 1231 (with respect to TACACS live logs, the "Device Port" field "[s]hows the device port number through which the access request is made"); 1236.

Furthermore, in Cisco's ISE the "communication port [is] configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper[.]"

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	As shown in the schematic below, the access device (e.g., Mobile Devices) is in communication with the restricted subset of the protected network (green), which includes a gatekeeper (e.g., Cisco's ISE) (purple). In the following illustration, Cisco ISE is the enforcement point and the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution.  **Figure 5.** Cisco ISE and MDM servers Randomized and Changing MAC Deployment Guide at 43. Cisco further explains that with respect to mobile device management (MDM) server integration with ISE, "ISE is the enforcement point . . . [that] then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Figure 5.
Cisco ISE and MDM servers

You can configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. It then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network.

Cisco further explains, with respect to MDM server integration with ISE, that access devices (termed "unregistered endpoints") "are redirected to a registration page that is hosted on the MDM server," and further that endpoints in remediation "are granted restricted access"—that is, they are "communicating [with] a restricted subset of the protected network, the restricted subset including a gatekeeper."

Supported MDM use cases

Cisco ISE performs the following functions with the external MDM server:

- Manages device registration: Unregistered endpoints that access the network are redirected to a registration page that is hosted on the MDM server. Device registration includes the user role, device type, and so on.
- Handles device remediation: Endpoints are granted restricted access during remediation.

Cisco describes this process flow elsewhere in the same document:

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	MDM integration process flow **Step 1.** The user associates a device with an SSID. **Step 2.** Cisco ISE makes an API call to the MDM server. **Step 3.** This API call returns a list of devices for the user and the posture statuses for the devices. **Note:** The input parameter is the MAC address of the endpoint device. For off-premises Apple iOS devices (any device that connects to Cisco ISE through a VPN), the input parameter is the UDID. **Step 4.** If the user's device is not on this list, it means that the device is not registered. Cisco ISE sends an authorization request to the Network Access Device (NAD) to redirect to Cisco ISE. The user is presented with the MDM server page. **Note:** You must register a device that is enrolled on the MDM server outside of a Cisco ISE network via the MDM portal. This is applicable for Cisco ISE Release 1.4 and later. Earlier Cisco ISE versions allow devices that are enrolled outside the Cisco ISE-enabled network to be automatically enrolled if they are compliant with the posture policies. **Step 5.** Cisco ISE uses MDM to provision the device and presents the appropriate window for the user to register the device. **Step 6.** The user registers the device in the MDM server, and the MDM server redirects the request to Cisco ISE through automatic redirection or manual browser refresh. **Step 7.** Cisco ISE queries the MDM server again for the posture status.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

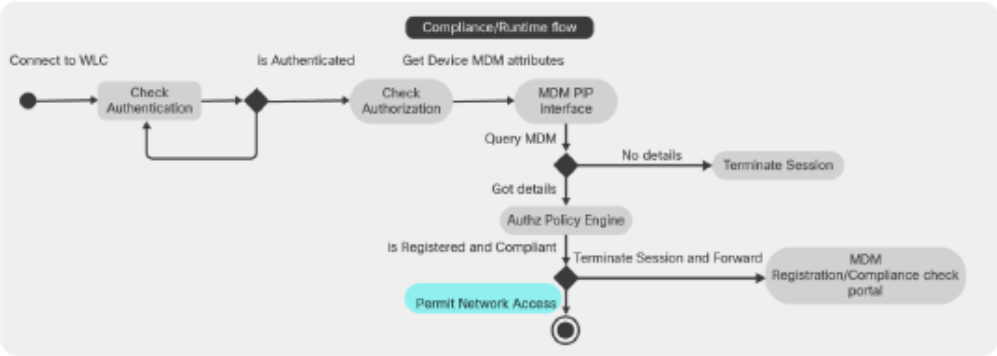
Step 8. If the user's device is not compliant with the posture (compliance) policies that are configured on the MDM server, the user is notified that the device is out of compliance. The user must take the necessary action to ensure that the device is compliant.

Step 9. When the user's device is compliant, the MDM server updates the device's state in its internal tables.

Step 10. If the user refreshes the browser now, the control is transferred back to Cisco ISE.

Step 11. Cisco ISE polls the MDM server once every four hours to get compliance information and issues the appropriate Change of Authorization (CoA). You can configure the polling interval. Cisco ISE also checks the MDM server every five minutes to make sure that it is available.

The following figure illustrates the MDM process flow.



Randomized and Changing MAC Deployment Guide at 46-47.

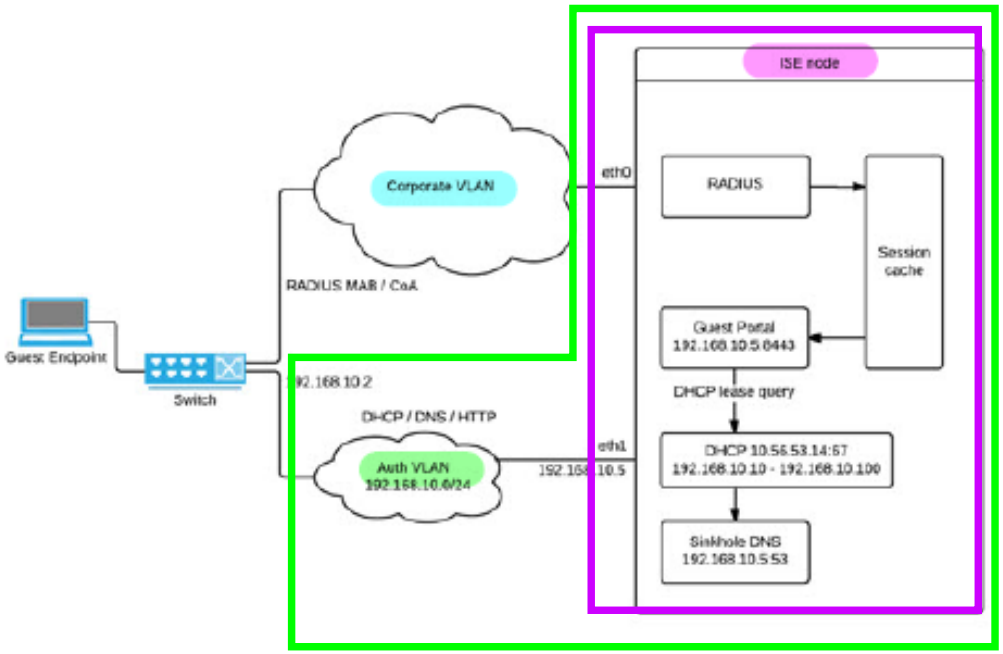
Finally, with respect to MDM servers integrated with ISE, Cisco's ISE has a gatekeeper associated with the restricted subset of the protected network. Cisco further explains how ISE can be the "enforcement point" that "applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	Cisco ISE also integrates with MDM servers using the Cisco MDM Server Info API, Version 2, to allow devices to access the network over VPN via Cisco AnyConnect 4.1 and Cisco Adaptive Security Appliances 9.3.2 or later. In the following illustration, Cisco ISE is the enforcement point and the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution. You can configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. It then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network. Randomized and Changing MAC Deployment Guide at 43. By way of a specific example, Cisco's ISE operates in conjunction with third party (i.e. non-Cisco) access points. In this setup, an access device ("guest endpoint") connects to the network through a restricted subset of the protected network (the "Authorization VLAN ('Auth VLAN')[.]" The restricted subset includes the Auth VLAN and further includes a gatekeeper in the form of its ISE node that can assess the endpoint's security posture. Cisco explains how ISE "runs the configured authentication and authorization policy[,] "validates endpoint compliance[,]" and "authorizes the endpoint[.]"

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Figure 31: Auth VLAN Connected to Cisco ISE Node



The following diagram displays a network with Auth VLAN and an IP helper.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

Multiple VLANs may be connected to one network interface card by configuring a VLAN IP helper from the NAD configuration. For more information about configuring an IP helper, see the administration guide for the network device for instructions. For guest access flows that include VLANs with IP helpers, define a guest

Admin Guide at 804-06.

By way of another specific example, Cisco's ISE has an ***Easy Connect Mode***, whereby it "enables you to easily connect users from a wired endpoint to a network in a secure manner and monitor those users by authenticating them through an Active Directory Domain Controller and not by Cisco ISE." With Easy Connect, "ISE issues a [Change of Authorization ("CoA")] after the external server (AD) authenticates the user."

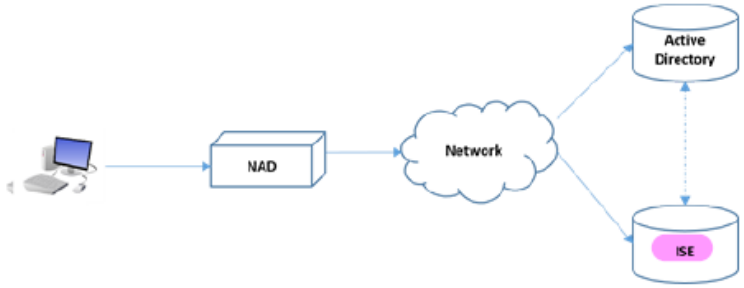
U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Easy Connect Enforcement Mode Process Flow

The Easy Connect Enforcement mode process is as follows:

1. The user connects to the NAD from a wired endpoint (such as a PC for example).
2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD.
3. The user logs in to the domain and a security audit event is sent to Cisco ISE.
4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event.
5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy.

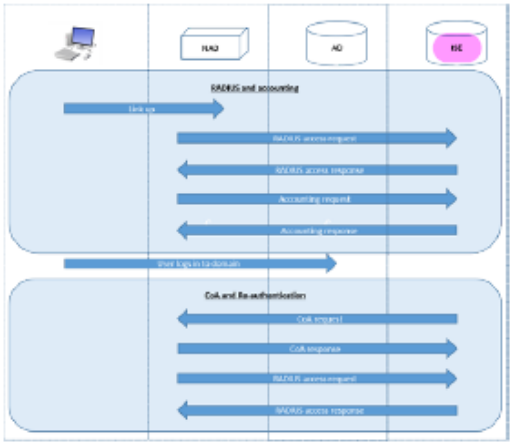
Figure 20: Easy Connect Enforcement Mode Basic Flow



ISE 3.0 Admin Guide at 581.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Figure 21: Easy Connect Enforcement Mode Detailed Flow



For more information about configuring Enforcement mode, see Configure Easy Connect Enforcement Mode, on page 582.

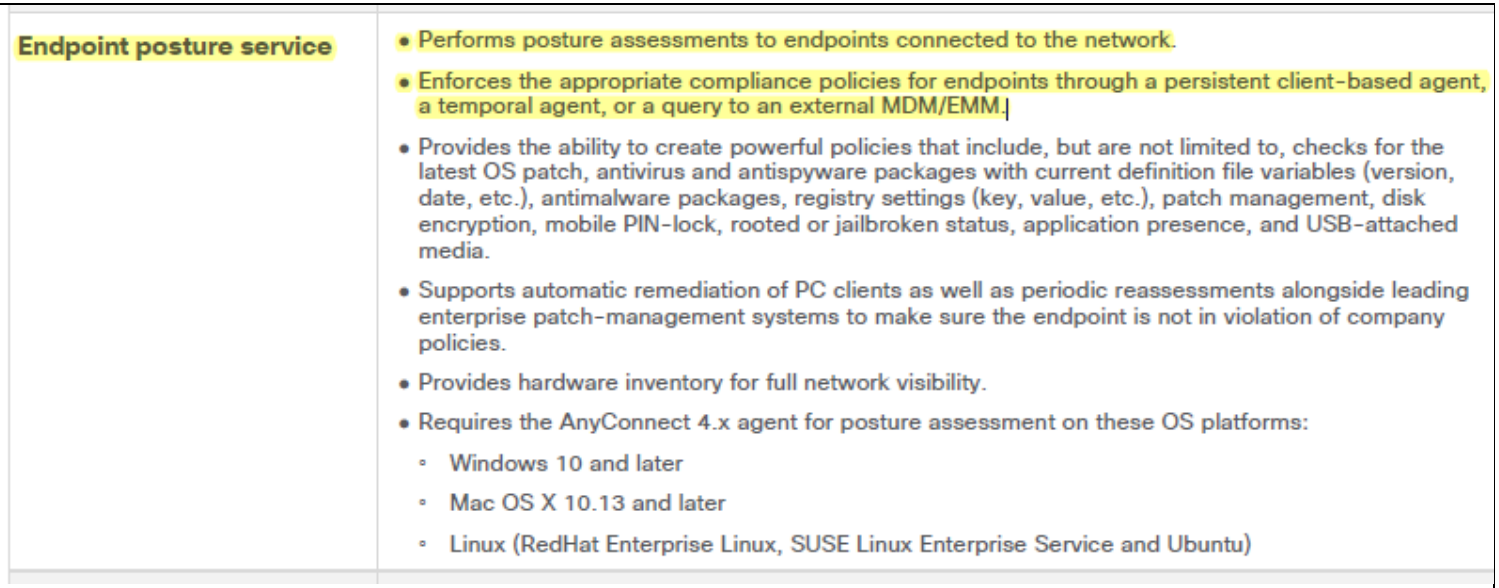
In Easy Connect Mode, "The user connects to the [network access device ("NAD"), e.g. an access point] from a wired endpoint (such as a PC for example)[,]" and after several steps, "Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and ***the user is provided access by the NAD to the network based on that policy***." Having a step whereby the user is being provided access to the network means, by implication, that the user did not have network access prior to that step. Thus, at that point, the user was restricted from certain network access, and thus "the communication port [was] configured for communicating between the access device and ***a restricted subset*** of the protected network[.]"

Moreover, Cisco's ISE has a gatekeeper associated with the restricted subset of the protected network. Cisco further explains how ISE collects certain information from the endpoint such as "the MAC address from RADIUS and the IP address" then "issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access[.]"

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

[27-b] applying a security policy to the access device, responsive to the request;	Cisco ISE "appl[ies] a security policy to the access device, responsive to the request [for access,]" or induces others to do so. Cisco explains that the "Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network." • **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods. • **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation. • **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services. ISE 3.0 Admin Guide at 2. Cisco further explains that it "[p]erforms posture assessments to endpoints connected to the network" and "enforces the appropriate compliance policies for [those] endpoints" through different mechanisms. Such "security policies" "include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages . . . antimalware packages . . . patch management . . . rooted or jailbroken status [and] application presence[,]" among others.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	 ISE Data Sheet at 7. Cisco explains how ISE "is a policy-based, network-access-control solution" whose Policy Sets "enable [the user] to logically group authentication and authorization policies within the same set."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Policy Sets

Cisco ISE is a policy-based, network-access-control solution, which offers network access policy sets, allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type, and similar parameters. When you install Cisco ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules.

When creating policy sets, you can configure these rules (configured with conditions and results) in order to choose the network access services on the policy set level, the identity sources on the authentication policy level, and network permissions on the authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE-supported dictionaries for different vendors. Cisco ISE allows you to create conditions as individual resuable policy elements.

The network access service to be used per policy set to communicate with the network devices is defined at the top level of that policy set. Network access services include:

- Allowed protocols—the protocols configured to handle the initial request and protocol negotiation.
- A proxy service—sends requests to an external RADIUS server for processing.

ISE 3.0 Admin Guide at 856; *see also id.* at 858 (Authentication Policies); 874 ("Create Authorization Policies with Endpoint-Analytics Attributes"), 882 ("Cisco ISE uses rule-based policies to provide network access. A policy is a set of rules and results, where the rules are made up of conditions."), 901 ("You can configure authorization profiles and policies in Cisco ISE using the IPv6 attributes in your rule conditions to process such requests from IPv6-enabled endpoints and ensure that the endpoint is compliant."), 940-41 (with Cisco's TrustSec Architecture, "[T]he security group tag (SGT)[] allows Cisco ISE to enforce access control policies by enabling the endpoint device to act upon the SGT to filter traffic."), 1030-31 ("Compliance Module"), 1032 ("Check Posture Compliance"), 1052 (Configure Posture Policies); 1057 ("Client Posture Assessment"), 1057-58 (Posture Assessment Options); *and see generally* 1009-1110 (Chapter 12, Titled "Compliance").

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Cisco explains that a user can "check" or "view" the "posture compliance" of endpoints through the ISE interface—thereby "applying a security policy to the access device, responsive to the request [for access.]"

Check Posture Compliance

Step 1 Log in to Cisco ISE and access the dashboard.

Step 2 In the **Posture Compliance** dashlet, hover your cursor over a stack bar or sparkline.

A tooltip provides detailed information.

Step 3 Expand the data categories for more information.

Step 4 Expand the **Posture Compliance** dashlet.

A detailed real-time report is displayed.

Note You can view the posture compliance report in the **Context Visibility** window. Navigate **Context Visibility** > **Endpoints** > **Compliance**. This window displays different charts based on **Compliance Status**, **Location**, **Endpoints**, and **Applications by Categories**.

You might see the posture status for endpoints that do not have any active sessions. For example, if the last known posture status for an endpoint is **Compliant**, the status remains **Compliant** in the **Context Visibility** window until the next update is received for the endpoint, even if the endpoint session is terminated. The posture status is retained in the **Context Visibility** window until that endpoint is deleted or purged.

Source: ISE 3.0 Admin Guide at 1032.

As described above (with respect to an MDM server integrated with ISE), ISE "ISE is the enforcement point[, which] obtains data from the MDM server [and] then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points." Randomized and Changing MAC Deployment Guide at 43. Thus, ISE "appl[ies] a security policy to the access device, responsive to the request [for access.]"

In one example, Cisco explains how ISE "appl[ies] a security policy . . ." with respect to access devices in the form of "guest devices." In particular, Cisco explains how such access devices can be required to "first download [a] posture agent that checks their posture profile and verifies if their device is compliant" with the

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

network security criteria. *Id.* at 401. By "verif[ying] if [a] device is compliant," ISE "applies a security policy" to it.

Guest Device Compliance

When guests and non-guests access the network through credentialed Guest portals, you can check their devices for compliance before they are allowed to gain access. You can route them to a Client Provisioning window and require them to first download the posture agent that checks their posture profile and verifies if their device is compliant. You can do this by enabling the option in the **Guest Device Compliance Settings** in a credentialed Guest portal, which displays the Client Provisioning window as part of the guest flow.

Note Client posture assessment in guest flow supports only the Temporal agent.

The Client Provisioning service provides posture assessments and remediations for guests. The Client Provisioning portal is available only with a Central Web Authorization (CWA) guest deployment. The guest login flow performs a CWA, and the credentialed Guest portal is redirected to the Client Provisioning portal after performing acceptable-use-policy and change-password checks. The posture subsystem performs a Change of Authorization (CoA) on the network access device to reauthenticate the client connection once the posture has been assessed.

Admin Guide at 401. Cisco describes several different posture agents that accomplish this. *See id.* at 1010-11.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	Posture Types The following posture agents monitor and enforce Cisco ISE posture policies: • **AnyConnect**: Deploys the AnyConnect agent to monitor and enforce Cisco ISE posture policies that require interaction with the client. The AnyConnect agent stays on the client. For more information about using AnyConnect in Cisco ISE, see Cisco AnyConnect Secure Mobility, on page 1099. • **AnyConnect Stealth**: Runs posture as a service, with no user interface. The agent stays on the client. When you choose the AnyConnect Stealth posture type in the posture requirement, some of the conditions, remediations, or attributes in a condition are disabled (grayed out). For example, when you enable AnyConnect Stealth requirement, the Manual Remediation Type is disabled (grayed out) because this action requires client-side interaction. When you map the posture profile to the AnyConnect configuration, and then map the AnyConnect configuration to the Client Provisioning window for AnyConnect Stealth mode deployment: • AnyConnect can read the posture profile and set it to the intended mode. • AnyConnect can send information related to the selected mode to Cisco ISE during the initial posture request. • Cisco ISE can match the right policy, based on the mode and other factors, such as identity group, OS, and compliance module.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

- **Temporal Agent**: When a client attempts to access the trusted network, Cisco ISE opens the Client Provisioning portal. The portal instructs the user to download and install the agent, and run the agent. The temporal agent checks the compliance status, and sends the status to Cisco ISE. Cisco ISE acts based on the results. The temporal agent removes itself from the client after compliance processing completes. The temporal agent does not support custom remediation. The default remediation supports only message text.

  The Temporal Agent does not support the following conditions:

  - Service Condition MAC—System Daemon check
  - Service Condition-MAC—Daemon or User Agent check
  - PM—Up To Date check
  - PM—Enabled check
  - DE—Encryption check

- For the Temporal Agent, you can only view Patch Management conditions containing the **Installation** check type in the **Requirements** window.
- Cisco ISE does not support VLAN-controlled posture with the Temporal Agent for macOS. When you change the network access from an existing VLAN to a new VLAN, the user's IP address is released before the VLAN change. The client gets a new IP address by DHCP when the user connects to the new VLAN. Recognizing the new IP address requires root privileges, but the Temporal Agent runs as a user process.
- Cisco ISE supports ACL-controlled posture environment, which does not require the refreshing of endpoint IP addresses.
- For more information about configuring the Temporal agent in Cisco ISE, see Configure Cisco Temporal Agent Workflow, on page 1074.

In another example, the Cisco ISE "appl[ies] a security policy to the access device, responsive to the request [for access]" when it operates with respect to Cisco or third-party (i.e. non-Cisco) access points. An access device connects to an access point (termed a ***network access device*** or ***NAD*** by Cisco). ISE applies a security policy—as

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

described below in step 3 (by "run[ning] the configured authentication and authorization policy") and/or step 11 (by "validat[ing] endpoint compliance").

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

ISE 3.0 Admin Guide at 804; *see also id.* at 805-06 (schematics of same).

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

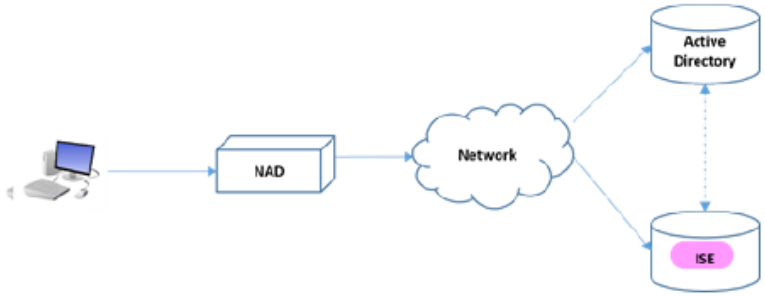
Finally, in another example—ISE's Easy Connect Enforcement Mode—ISE "collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event. [] After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD ***(based on the appropriate policy managed in the policy service node***), and the user is provided access by the NAD to the network based on ***that policy***." Thus, ISE "applies a security policy."

Easy Connect Enforcement Mode Process Flow

The Easy Connect Enforcement mode process is as follows:

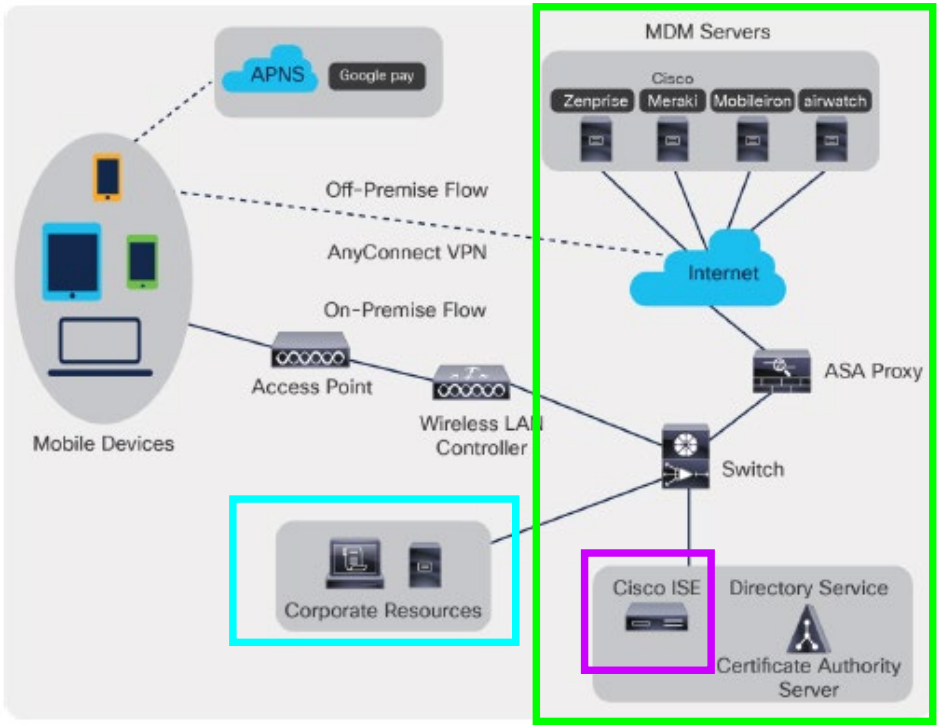
1. The user connects to the NAD from a wired endpoint (such as a PC for example).
2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD.
3. The user logs in to the domain and a security audit event is sent to Cisco ISE.
4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event.
5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy.

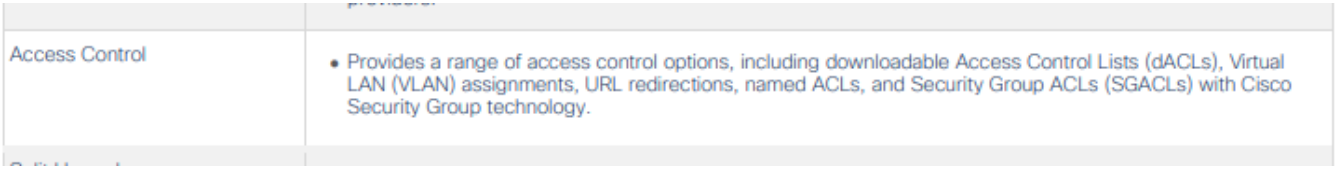
Figure 20: Easy Connect Enforcement Mode Basic Flow



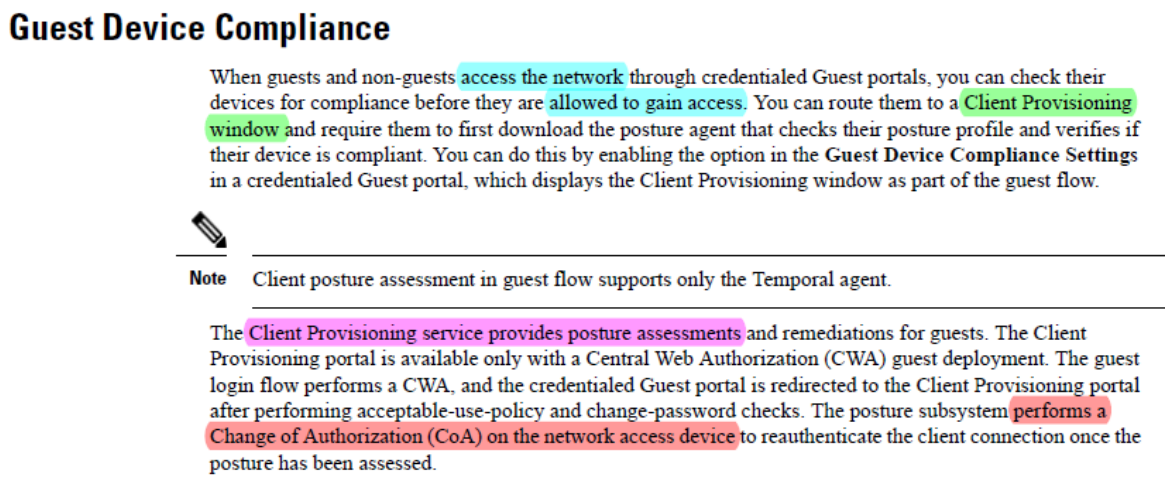
ISE 3.0 Admin Guide at 581.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

[27-c] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements of the security policy are satisfied;	Cisco ISE "reconfigur[es] the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements of the security policy are satisfied," or induces others to do so.  As shown, if ISE determines that an access device (e.g. Mobile Devices) satisfies requirements of the security policy, it reconfigures the communication port on the access point to allow the access device to communicate with the less-restricted subset of the protected network (here, "Corporate Resources)." Randomized Changing MAC at 43; *see also id.* at 57 ("If the device is registered with Cisco ISE, is registered with MDM, and is compliant with Cisco ISE and MDM policies, it is ***granted access to the network based on the access control policies configured in Cisco ISE***."). Additionally, as shown in the schematic, if the requirements of the security policy

	are satisfied, the mobile devices have access through the switch to the corporate resources. Thus, the communication port is "reconfigure[ed] for communicating data . . . without passing the data through the gatekeeper[.]" *Id.* Cisco also describes in its ISE Data Sheet "a range of access control options" for this step, "including downloadable Access Control Lists (dACLs), Virtual LAN (VLAN) assignments, URL redirections, named ACLs, and Security Group ACLs (SGACLs) with Cisco Security Group technology[.]" By using any or all of these methods, ISE "reconfigur[es] the communication port for communicating data between the access device and the less-restricted subset of the protected network"—for example, network resources. Additionally, as show above with respect to MDM servers integrated with ISE, if the requirements of the security policy are satisfied, the communication port is "reconfigure[ed] for communicating data . . . without passing the data through the gatekeeper[.]" *Id.*  ISE Data Sheet at 5. By way of an example previously described—guest device compliance—Cisco states that "the posture agent [] checks their posture profile and verifies if their device is compliant[,]" and further that "the Client Provisioning service provides posture assessments"—that is, ISE determines if "requirements of the security policy are satisfied." ISE 3.0 Admin Guide at 401. Upon such satisfaction, ISE grants the access device access to network resources, thereby "reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network[.]" *See id.* Finally, as show above with respect to MDM servers integrated with ISE, if the requirements of the security policy are satisfied, the communication port is "reconfigure[ed] for communicating data . . . without passing the data through the gatekeeper[.]" *Id.*

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)



Guest Device Compliance

When guests and non-guests access the network through credentialed Guest portals, you can check their devices for compliance before they are allowed to gain access. You can route them to a Client Provisioning window and require them to first download the posture agent that checks their posture profile and verifies if their device is compliant. You can do this by enabling the option in the **Guest Device Compliance Settings** in a credentialed Guest portal, which displays the Client Provisioning window as part of the guest flow.

Note Client posture assessment in guest flow supports only the Temporal agent.

The Client Provisioning service provides posture assessments and remediations for guests. The Client Provisioning portal is available only with a Central Web Authorization (CWA) guest deployment. The guest login flow performs a CWA, and the credentialed Guest portal is redirected to the Client Provisioning portal after performing acceptable-use-policy and change-password checks. The posture subsystem performs a Change of Authorization (CoA) on the network access device to reauthenticate the client connection once the posture has been assessed.

ISE 3.0 Admin Guide at 401-02.

In another example relates to ISE operating with respect to Cisco and third-party (i.e. non-Cisco) access points. ISE applies the security policy, as described in the prior step. Once ISE determines that "requirements of the security policy are satisfied," it "sends the [change of authorization ("CoA")], authorizes the endpoint, and bypasses the sink hole[,] and then the "the guest user receives the appropriate [network] access based on the CoA." Thus, ISE "reconfigur[es] the communication port for communicating data between the access device and the less-restricted subset of the protected network."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	Additionally, Cisco describes how a user "can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication," and shows this in the schematics. As described this way and as further shown in the schematic, if the requirements of the security policy are satisfied, the access devices have network access without passing their data through ISE—that is, "without passing the data through the gatekeeper[.]"

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

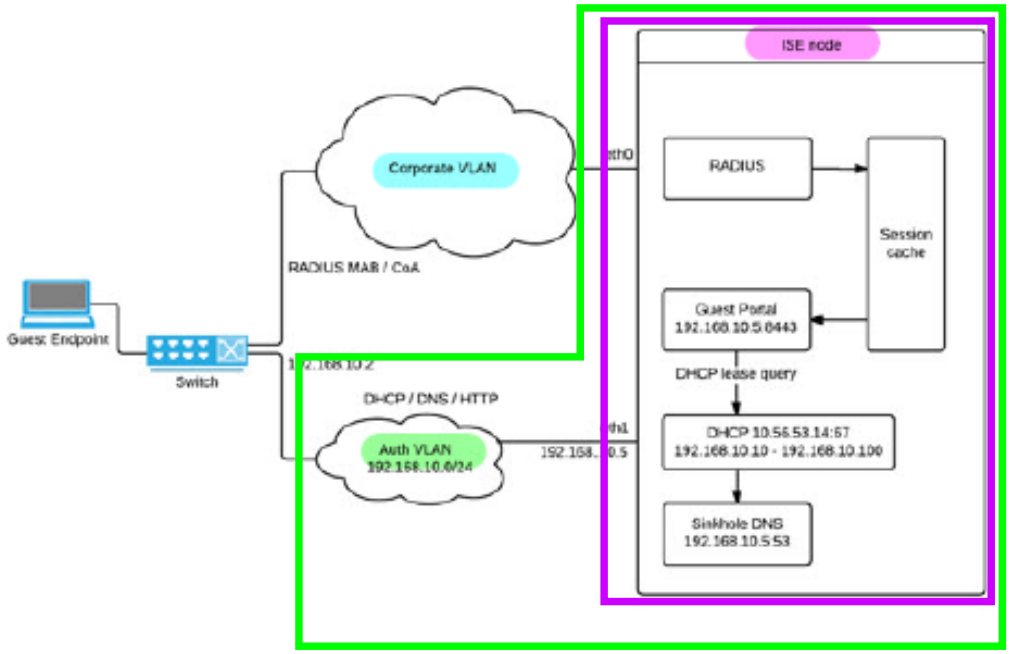
Multiple VLANs may be connected to one network interface card by configuring a VLAN IP helper from the NAD configuration. For more information about configuring an IP helper, see the administration guide for the network device for instructions. For guest access flows that include VLANs with IP helpers, define a guest

portal, and select that portal in an authorization profile that is bound to MAB authorization. For more information about guest portals, see the Cisco ISE Guest Services section in *Cisco ISE Admin Guide: Guest and BYOD* .

The following diagram displays a basic network setup when an Auth VLAN is defined (the Auth VLAN is connected directly to a Cisco ISE node).

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

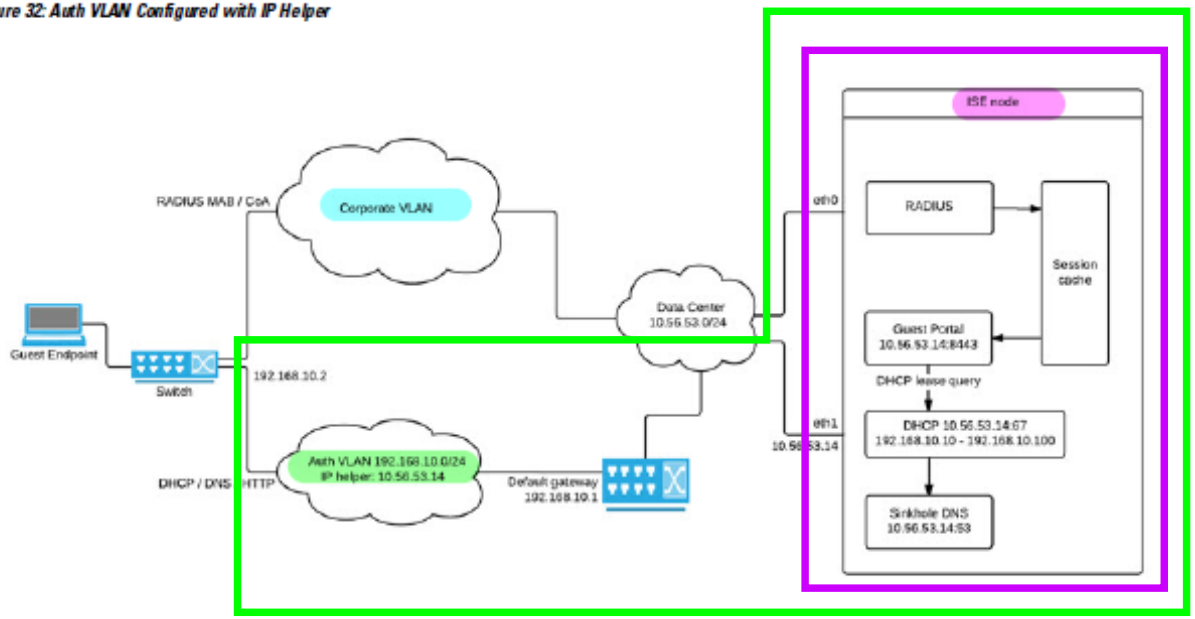
Figure 31: Auth VLAN Connected to Cisco ISE Node



The following diagram displays a network with Auth VLAN and an IP helper.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Figure 32: Auth VLAN Configured with IP Helper



ISE 3.0 Admin Guide at 804-06.

In one further example described above—ISE's Easy Connect Enforcement Mode—ISE collects certain data, after which it "issues a CoA to the [network access device, ("NAD"] (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy." ISE 3.0 Admin Guide at 580-81. By issuing a CoA to the NAD, to provide the user access to the network, ISE "reconfigur[es] the communication port for communicating data between the access device and the less-restricted subset of the protected network[.]" Additionally, as shown in the schematic, if the requirements of the security policy are satisfied, the access devices have network access without passing their data through ISE—that is, "without passing the data through the gatekeeper[.]"

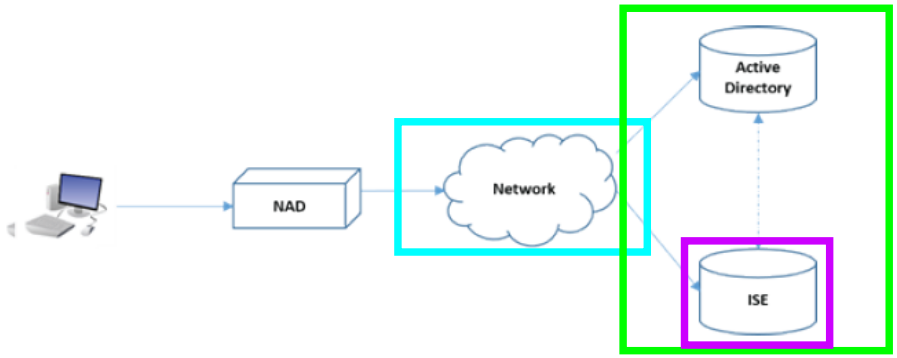
U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Easy Connect Enforcement Mode Process Flow

The Easy Connect Enforcement mode process is as follows:

1. The user connects to the NAD from a wired endpoint (such as a PC for example).
2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD.
3. The user logs in to the domain and a security audit event is sent to Cisco ISE.
4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event.
5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy.

Figure 20: Easy Connect Enforcement Mode Basic Flow



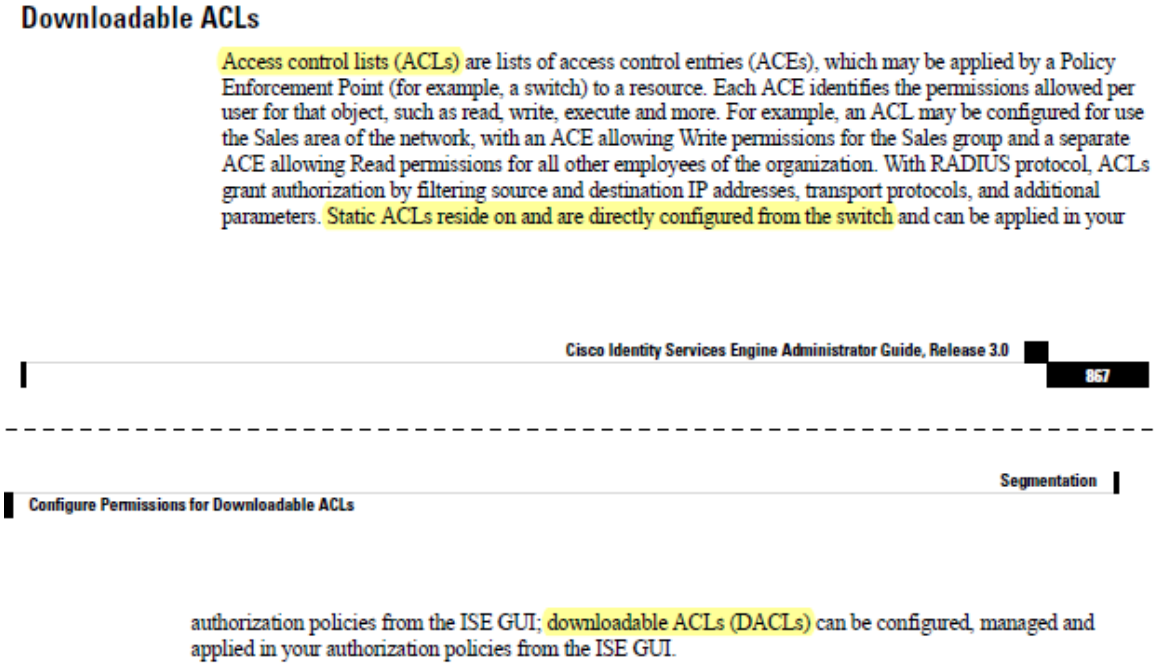
ISE 3.0 Admin Guide at 581.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

[27-d & e] reading an administrator specified configuration of the communication port from the access point; and storing the read administrator specified configuration.	Cisco ISE "read[s] an administrator specified configuration of the communication port from the access point; and stor[es] the read administrator specified configuration" or induces others to do so. As shown, Cisco ISE can have an administrator "[m]anage Cisco ISE services, policies, administrator accounts, and system configuration and operations." Thus an administrator can "specif[y] configuration of the communication port from the access point[.]" Additionally, ISE can "stori[e] the read administrator specified configuration[.]" **Cisco ISE Administrators** Administrators can use the admin portal to: • Manage deployments, help desk operations, and network devices, and node monitoring and troubleshooting. • Manage Cisco ISE services, policies, administrator accounts, and system configuration and operations. • Change administrator and user passwords. A CLI administrator can start and stop the Cisco ISE application, apply software patches and upgrades, reload or shut down the Cisco ISE appliance, and view all the system and application logs. Because of the special privileges that are granted to a CLI administrator, we recommend that you protect the CLI administrator credentials and create web-based administrators for configuring and managing Cisco ISE deployments. The username and password that you configure during setup is intended only for administrative access to the CLI. This role is considered to be the CLI admin user, also known as CLI administrator. By default, the username for a CLI admin user is admin, and the password is defined during setup. There is no default password. This CLI admin user is the default admin user, and this user account cannot be deleted. However, other administrators can edit it, including options to enable, disable, or change password for the corresponding account. You can either create an administrator, or promote an existing user to an administrator role. Administrators can also be demoted to simple network user status by disabling the corresponding administrative privileges. Administrators are users who have local privileges to configure and operate the Cisco ISE system. Administrators are assigned to one or more admin groups. Cisco, Overview of Cisco ISE, at 3, https://www.cisco.com/c/en/us/td/docs/security/ise/3-2/admin_guide/b_ise_admin_3_2/b_ISE_admin_33_overview.pdf (last accessed September 29, 2023).

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

By way of one example—***access control lists (ACLs)***—Cisco states that "Access control lists (ACLs) are lists of access control entries (ACEs), which may be applied by a Policy Enforcement Point (for example, a switch) to a resource. . . . ***Static ACLs reside on and*** are ***directly configured from the switch***[.]" ISE 3.0 Admin Guide at 867-68.



Downloadable ACLs

Access control lists (ACLs) are lists of access control entries (ACEs), which may be applied by a Policy Enforcement Point (for example, a switch) to a resource. Each ACE identifies the permissions allowed per user for that object, such as read, write, execute and more. For example, an ACL may be configured for use the Sales area of the network, with an ACE allowing Write permissions for the Sales group and a separate ACE allowing Read permissions for all other employees of the organization. With RADIUS protocol, ACLs grant authorization by filtering source and destination IP addresses, transport protocols, and additional parameters. Static ACLs reside on and are directly configured from the switch and can be applied in your

Cisco Identity Services Engine Administrator Guide, Release 3.0

867

Segmentation

Configure Permissions for Downloadable ACLs

authorization policies from the ISE GUI; downloadable ACLs (DACLs) can be configured, managed and applied in your authorization policies from the ISE GUI.

ISE 3.0 Admin Guide at 867-68

An ACL—which "identifies the permissions allowed per user for that [network resource]"—comprises an "administrator-specified configuration of the communication port." Furthermore, because the "static ACLs

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	reside on and are directly configured from the switch," ISE "read[s] [it] from the switch (the claimed "access point"). Finally, and also because the "static ACLs reside on and are directly configured from the switch," ISE "stor[es] the read administrator specified configuration."

Claim 28

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

28. A method of granting access to a protected network, the method comprising:	Cisco infringes this claim by making, using, testing, offering for sale, and selling the ISE product and system and through performance of each of the claimed steps and/or providing instructions and data from its servers to third-parties to perform at least one of the claimed steps, or induces others to do so as set forth in claim element 1-c.. Cisco ISE performs the "method of granting access to a protected network" recited in claim 28, or induces others to do so. Thus, Cisco ISE performs this method with respect to this claim.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

[28-a] receiving a request for access to a less-restricted subset of the protected network from an access device, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset	Cisco ISE "receiv[es] a request for access to a less-restricted subset of the protected network from an access device, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper[,]" or induces others to do so. As shown above with respect to claim element 27-a, Cisco ISE "receiv[es] a request for access to a less-restricted subset of the protected network from an access device, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper[.]" Thus, Cisco ISE performs this claim element.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

including a gatekeeper;	
[28-b] applying a security policy to the access device, responsive to the request;	Cisco ISE "appl[ies] a security policy to the access device, responsive to the request[,]" or induces others to do so. As shown above with respect to claim element 27-b, Cisco ISE "appl[ies] a security policy to the access device, responsive to the request[.]" Thus, Cisco ISE performs this claim element.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

[28-c] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements of the security policy are satisfied; and	Cisco ISE "reconfigure[es] the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements of the security policy are satisfied [,]" or induces others to do so. As shown above with respect to claim element 27-c, Cisco ISE "reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements of the security policy are satisfied[.]" Thus, Cisco ISE performs this claim element.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

[28-d] communicating between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port for communicating between the access device and the less-restricted subset.	Cisco ISE "communicat[es] between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port for communicating between the access device and the less-restricted subset[,]" or induces others to do so. Cisco states that after an endpoint (the claimed "access device") is granted access to network resources ("reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements of the security policy are satisfied"), ISE can use ***Continuous Endpoint Attribute Monitoring***. ISE 3.0 Admin Guide at 1002-03. With that, ISE uses the AnyConnect agent (the claimed "agent executing on the access device") to monitor the endpoint after initial posture ("reconfiguring . . ."). Cisco further states, "After initial posture, the AnyConnect agent scans the applications every X minute and sends the differences from the last scan to the server." Thus, by sending differences from the last scan to the server, ISE "communicat[es] between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port for communicating between the access device and the less-restricted subset."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	Continuous Endpoint Attribute Monitoring You can use the AnyConnect agent to continuously monitor different endpoint attributes to ensure that dynamic changes are observed during posture assessment. This improves the overall visibility of an endpoint and helps you create posture policies based on their behavior. The AnyConnect agent monitors applications that are installed and running on an endpoint. You can turn on and off the feature and configure how often the data should be monitored. By default, data is collected every 5 minutes and is stored in the database. During initial posture, AnyConnect reports a complete list of running and installed applications. After initial posture, the AnyConnect agent scans the applications every X minute and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications. ISE 3.0 Admin Guide at 1102-03.
33. The method of claim 28, wherein the access point is a network switch.	Cisco ISE performs "[t]he method of claim 28, wherein the access point is a network switch" and induces others to do so. As disclosed above with respect to claim 18, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a network switch." Thus, Cisco ISE performs the "method of [granting access to a protected network recited in] claim 28, wherein the access point is a network switch[,]" and induces others to do so.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

34. The method of claim 28, wherein the access point is a wireless access point.	Cisco ISE performs "[t]he method of claim 28, wherein the access point is a wireless access point[,]" and induces others to do so. As disclosed above with respect to claim 16, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a wireless access point." (Furthermore, as disclosed above with respect to claim 17, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a wireless access point configured to support an 802.1x standard.") Thus, Cisco ISE performs the "method of [granting access to a protected network recited in] claim 28, wherein the access point is a wireless access point[,]" and induces others to do so.
35. The method of claim 28, wherein the access point is a remote access virtual private network.	Cisco ISE performs "[t]he method of claim 28, wherein the access point is a remote access virtual private network[,]" and induces others to do so. As disclosed above with respect to claim 25, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a remote access virtual private network." Thus, Cisco's ISEperforms "[t]he method of claim 28, wherein the access point is a remote access virtual private network[,]" and induces others to do so.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

38. The method of claim 28, further including updating the access device if requirements of the security policy are not satisfied.	Cisco ISE performs "[t]he method of claim 28, further including updating the access device if requirements of the security policy are not satisfied" and induces others to do so. As disclosed above with respect to claim 24, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the network gatekeeper is configured to update the access device if requirements of the security policy are not satisfied." Thus, Cisco ISE performs "[t]he method of claim 28, further including updating the access device if requirements of the security policy are not satisfied" and induces others to do so.
39. The method of claim 28, wherein the security policy includes an audit of the access device.	Cisco ISE performs "[t]he method of claim 28, wherein the security policy includes an audit of the access device" and induces others to do so. As disclosed above with respect to claim element 1-b, Cisco's ISE comprises "a policy auditor configured to audit the access device using the at least one security policy, . . ." (Furthermore, as disclosed above with respect to claim 13, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the audit is responsive to antivirus software executing on the access device." And furthermore, as disclosed above with respect to claim 15, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the policy auditor is configured to request data from an agent on the access device.") Thus, Cisco ISE performs "[t]he method of claim 28, wherein the security policy includes an audit of the access device" and induces others to do so.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

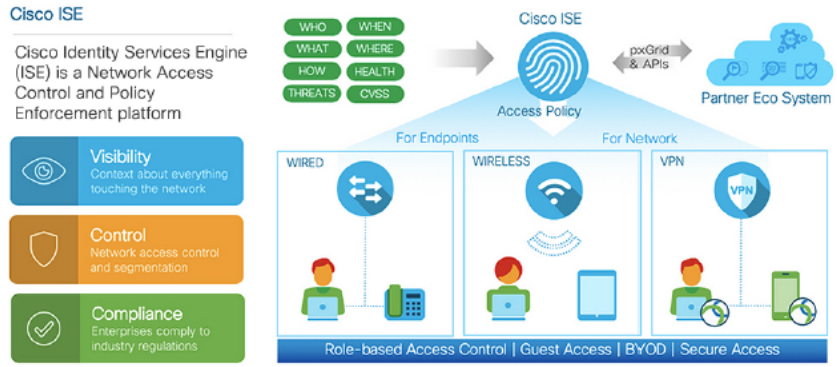
Claim 41

	Cisco's Identity Services Engine
[Claim 41 – preamble] A method of granting access to a protected network, the method comprising:	Cisco infringes this claim by making, using, testing, offering for sale, and selling the Identity Services Engine ("ISE") product and system and through performance of each of the claimed steps and/or providing instructions and data from its servers to third-parties to perform at least one of the claimed steps, or induces others to do so as set forth in claim element 1-c. To the extent the preamble is limiting, Cisco's Identity Services Engine ("ISE") is "a security policy management platform that provides secure access to network resources" and thereby grants access to a protected network. **Introduction to Cisco Identity Services Engine** Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, wireless controllers, Virtual Private Network (VPN) gateways, 5GaaS networks, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation. Cisco ISE is available on secure network server appliances with different performance characterizations, and also as software that can be run on a virtual machines (VMs). Note that you can add more appliances to a deployment for better performance. Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also enables the configuration and management of distinct personas and services, thereby giving you the ability to create and apply services, where needed, in a network, but operate the Cisco ISE deployment as a complete and coordinated system. For detailed Cisco ISE ordering and licensing information, see the *Cisco Identity Services Engine Ordering Guide*. For information on monitoring and troubleshooting the system, see the "Monitoring and Troubleshooting Cisco ISE" section in the *Cisco Identity Services Engine Administrator Guide*. ISE 3.0 Release Notes at 1.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Cisco further describes ISE as a "Network Access Control and Policy Enforcement platform" which thereby grants access to a protected network.

Cisco ISE Overview



Cisco Identity Services Engine (ISE) is an identity-based network access control and policy enforcement system. It functions as a common policy engine that enables endpoint access control and network device administration for enterprises.

You can leverage Cisco ISE to ensure compliance, enhance infrastructure security, and streamline service operations.

A Cisco ISE administrator can gather real-time contextual data for a network, including users and user groups (who?), device type (what?), access time (when?), access location (where?), access type (wired, wireless, or VPN) (how?), and network threats and vulnerabilities.

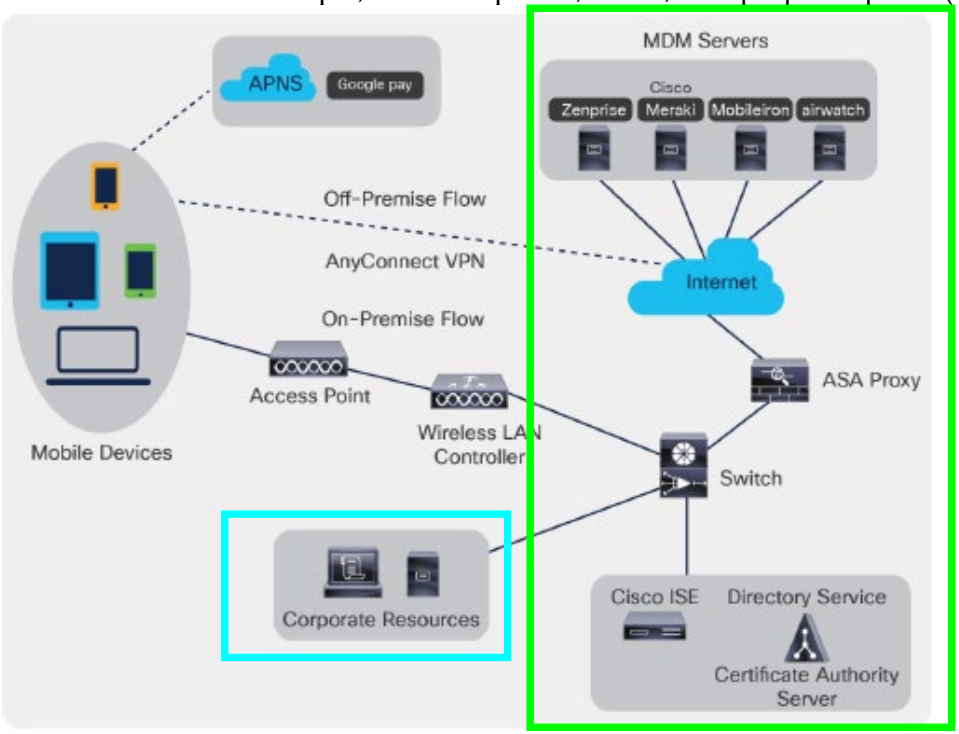
ISE 3.0 Admin Guide at 1.

Cisco further describes its ISE as allowing a user "to choose . . . the network permissions on the authorization policy levels[,]" which is thereby a "method of granting access to a protected network."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	Policy Sets Cisco ISE is a policy-based, network-access-control solution, which offers network access policy sets, allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type, and similar parameters. When you install Cisco ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules. When creating policy sets, you can configure these rules (configured with conditions and results) in order to choose the network access services on the policy set level, the identity sources on the authentication policy level, and network permissions on the authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE-supported dictionaries for different vendors. Cisco ISE allows you to create conditions as individual resuable policy elements. The network access service to be used per policy set to communicate with the network devices is defined at the top level of that policy set. Network access services include: • Allowed protocols—the protocols configured to handle the initial request and protocol negotiation. • A proxy service—sends requests to an external RADIUS server for processing. *Id.* at 856; *see also id.* at 546 ("A user role is a set of permissions that determine what tasks a user can perform and what services they can access on the Cisco ISE network. . . . .Cisco ISE allows you to restrict network access based on user attributes for both network access users and administrators.")
[41-a] receiving a request for access to a less-restricted	Cisco ISE "receiv[es] a request for access to a less-restricted subset of the protected network from an access device, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper" or induces others to do so.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

subset of the protected network from an access device, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper;	In this step, the Cisco ISE receives a request for a less restricted subset of the protected network (blue) from a user access device—for example, a mobile phone, tablet, or laptop computer (e.g. Mobile Devices).  Randomized and Changing MAC Deployment Guide at 43,

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Cisco also describes in its ISE 3.0 Admin Guide how Mobile Device Management (MDM) servers "secure, monitor, manage, and support mobile devices that are deployed across mobile operators, service providers, and enterprises. Traditionally, MDM servers have only supported mobile devices. Some MDM servers now manage ***all types of devices in a network (mobile phones, tablets, laptops, and desktops)***[.]"

Mobile Device Manager Interoperability with Cisco ISE

Mobile Device Management (MDM) servers secure, monitor, manage, and support mobile devices that are deployed across mobile operators, service providers, and enterprises. Traditionally, MDM servers have only supported mobile devices. Some MDM servers now manage all types of devices in a network (mobile phones, tablets, laptops, and desktops) and are called Unified Endpoint Management (UEM) servers. MDM servers act as a policy server that controls the use of some applications on a mobile device (for example, an email application) in the deployed environment. Cisco ISE queries a connected MDM server for information about various attributes that you can use to create network authorization policies.

You can run multiple active MDM servers on your network, from different vendors. This allows you to route different endpoints to different MDM servers based on device factors such as location or device type.

Cisco ISE also integrates with MDM servers using the Cisco MDM Server Info APIs, Version 2 and later versions, to allow devices to access the network over VPN via Cisco AnyConnect 4.1 and Cisco Adaptive Security Appliances 9.3.2 or later.

In the following illustration, Cisco ISE is the enforcement point and the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution.

ISE 3.0 Admin Guide at 830.

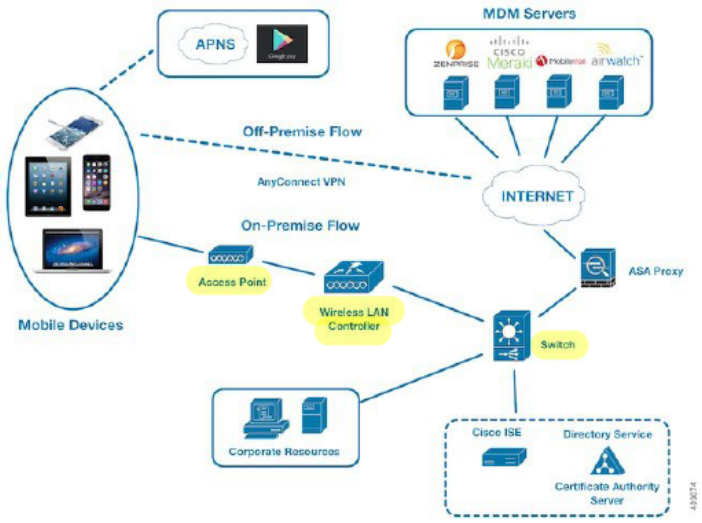
Cisco describes how the "access devices" that send "request[s] for access" are termed "endpoints" in Cisco's language. And endpoint is "typically a network-capable device that connect[s] to your network through wired and wireless network access devices and VPN. Endpoints can be personal computers, laptops, IP phones, smart phones,

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	gaming consoles, printers, fax machines, and so on." ISE 3.0 Admin Guide at 730; *see also id.* at 101 ("Here, an endpoint could mean users, PCs, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, or other types of network devices."); 765 ("For example, a user registers a laptop with wired and wireless addresses."). Cisco further describes how the "request [for access] [is] received through a communication port of an access point[.]" Cisco's "access points" include its "switches, access routers, wireless access points, and other network access points." ISE 3.0 Admin Guide at 830.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Figure 33: MDM Interoperability with Cisco ISE



Configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. Cisco ISE applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network.

See also Randomized and Changing MAC Deployment Guide at 43 (same); *see also* ISE 3.0 Admin Guide at 363 ("The device administrator is the user who logs into the network devices such as ***switches, wireless access points, routers, and gateways***, (normally through SSH), to perform the configuration and maintenance of the administered devices.").

A list of "access points" that are compatible with its ISE—including switches, routers, and remote access devices (i.e. firewalls)—is listed in Cisco's Identity Services Engine Network Component Compatibility documents, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014309 to INFOEX-CSCO_0014605. These Cisco documents describe "Cisco Identity Services Engine (ISE) validated

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	compatibility with switches, wireless LAN controllers, and other policy enforcement devices as well as operating systems with which Cisco ISE interoperates." INFOEX-CSCO_0014586 at 14586. They further state, with respect to "Validated Network Access Devices," that "Cisco ISE supports interoperability with any Cisco or non-Cisco RADIUS client network access device (NAD) that implements common RADIUS behavior (similar to Cisco IOS 12.x) for standards-based authentication." INFOEX-CSCO_0014586 at 14587. These Cisco documents identify the claimed "access points" including both Cisco-made and third-party access points. Cisco also describes ISE-compatible third-party devices in its ISE 3.0 Admin Guide at 806-07, including those made by Aruba, Motorola, HP, Ruckus, Alcatel, Brocade, and Juniper. *See also* ISE 3.0 Admin Guide at 430 ("The [Wireless LAN Controller ("WLC")] can now log the guest in via the Cisco ISE RADIUS server. When this is complete, the WLC redirects the guest device's browser to the original URL destination. The Wireless LAN Controller (WLC) and the network access devices (NAD) requirements to support the original URL redirect for guest portals are WLC 5760 and ***Cisco Catalyst 3850, 3650, 2000, 3000, and 4000 Series Access Switches*** running releases IOS-XE 3.6.0.E and 15.2(2)E."); 874 (Cisco AI Endpoint Analytics receives endpoint attribute data from multiple sources, such as ***Cisco Catalyst 9000 Series devices***[.]"); 697 ("The following devices support sending [Manufacturer Usage Descriptor ("MUD")] data to Cisco ISE: Cisco Catalyst 3850 Series Switches running Cisco IOS XE Version 16.9.1 & 16.9.2[,] Cisco Catalyst Digital Building Series Switches running Cisco IOS Version 15.2(6)E2[, and] Cisco Industrial Ethernet 4000 Series Switches running Cisco IOS Version 15.2(6)E2[."); 788 ("Cisco TrustSec-enabled devices use the TrustSec attributes to communicate with Cisco ISE. Cisco TrustSec-enabled devices, such as the Cisco Nexus 7000 Series Switches, Cisco Catalyst 6000 Series Switches, Cisco Catalyst 4000 Series Switches, and Cisco Catalyst 3000 Series Switches are authenticated using the Cisco TrustSec attributes that you define while adding Cisco TrustSec devices."). Cisco describes in its ISE 3.0 Admin Guide an example where the request for access is received through a Cisco or third-party (that is, a non-Cisco) access point (termed a "network access device") in Cisco's literature. ISE 3.0 Admin Guide at 803-06.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

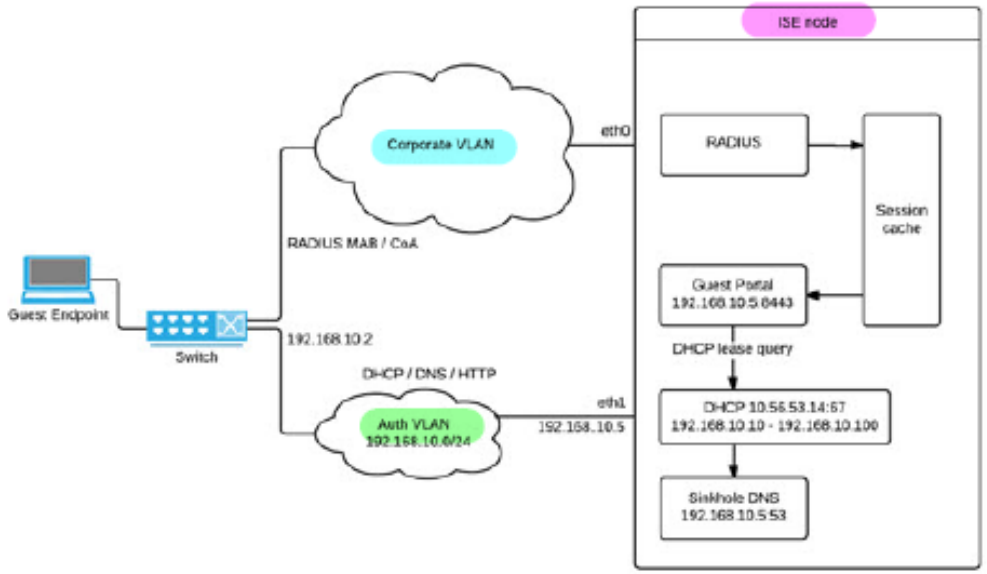
Third-Party Network Device Support in Cisco ISE

Cisco ISE supports third-party network access devices (NADs) by using network device profiles. A NAD profile defines the capabilities of a third-party device with a simplified policy configuration, regardless of the vendor-side implementation. A network device profile contains the following:

- The protocols that the network device supports, such as RADIUS, TACACS+, and Cisco TrustSec. You can import into Cisco ISE any vendor-specific RADIUS dictionaries that exist for the network device.
- The attributes and values that the device uses for various authentication flows such as Wired MAB and 802.1X. These attributes and values allow Cisco ISE to detect the right authentication flow for your device according to the attributes that the network device uses.
- The Change of Authorization (CoA) capabilities of the network device. While the RADIUS protocol RFC 5176 defines a CoA request, the attributes used in a CoA request vary depending on the network device. Most non-Cisco devices with RFC 5176 support the *Push* and *Disconnect* functions. For devices that do not support the RADIUS CoA type, Cisco ISE also supports SNMP CoA.
- The attributes and protocols that the network device uses for MAB flows. Network devices from different vendors perform MAB authentication differently.
- The VLAN and ACL permissions that are used by the device. When you save the profile, Cisco ISE automatically generates authorization profiles for each configured permission.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

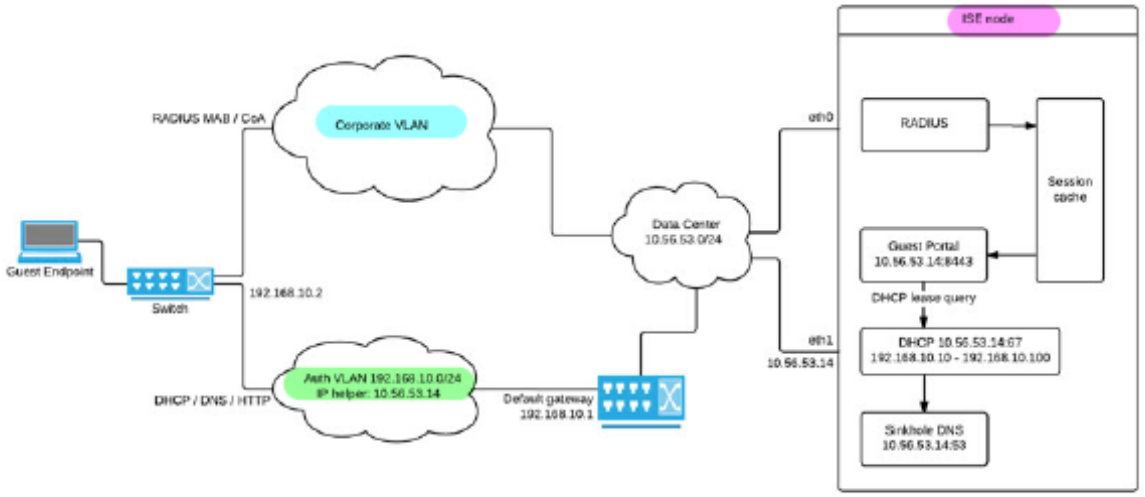
Figure 31: Auth VLAN Connected to Cisco ISE Node



The following diagram displays a network with Auth VLAN and an IP helper.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Figure 32: Auth VLAN Configured with IP Helper



Furthermore, in ISE, the "request [for access is] received through a ***communication port*** of an access point."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.
Endpoint Profile	Shows the type of endpoint that is profiled, for example, profiled to be an iPhone, Android, M Xbox, and so on.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
Authorization Profiles	Shows the authorization profile that was used for authentication.
IP Address	Shows the IP address of the endpoint device.
Network Device	Shows the IP address of the Network Access Device.
Device Port	Shows the port number at which the endpoint is connected.
Identity Group	Shows the identity group that is assigned to the user or endpoint, for which the log was genera
Posture Status	Shows the status of posture validation and details on the authentication.
Server	Indicates the policy service from which the log was generated.

ISE 3.0 Admin Guide at 354; *see also id.* at 359 (similar disclosure with respect to TACACS live logs); 377 (similar); 882 ("You can create the following unique network conditions to restrict access to the network: . . . Device Port Network Conditions—Based on the device's IP address, name, NDG, and ***port (physical port of the device*** that the endstation is connected to)."); 900 ("Configure Device Port Network Condition"); 1188-89 ("enable switch ports for 802.1X and MAB"); 1230 (with respect to RADIUS live logs, the "Device Port" field "[s]hows the port number at which the endpoint is connected"); 1231 (with respect to TACACS live logs, the "Device Port" field "[s]hows the device port number through which the access request is made"); 1236.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Furthermore, in Cisco's ISE, the "communication port [is] configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper[.]"

As shown in the schematic below, the access device (e.g., Mobile Devices) is in communication with the restricted subset of the protected network (green), which includes a gatekeeper (e.g., Cisco's ISE) (purple).

In the following illustration, Cisco ISE is the enforcement point and the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution.

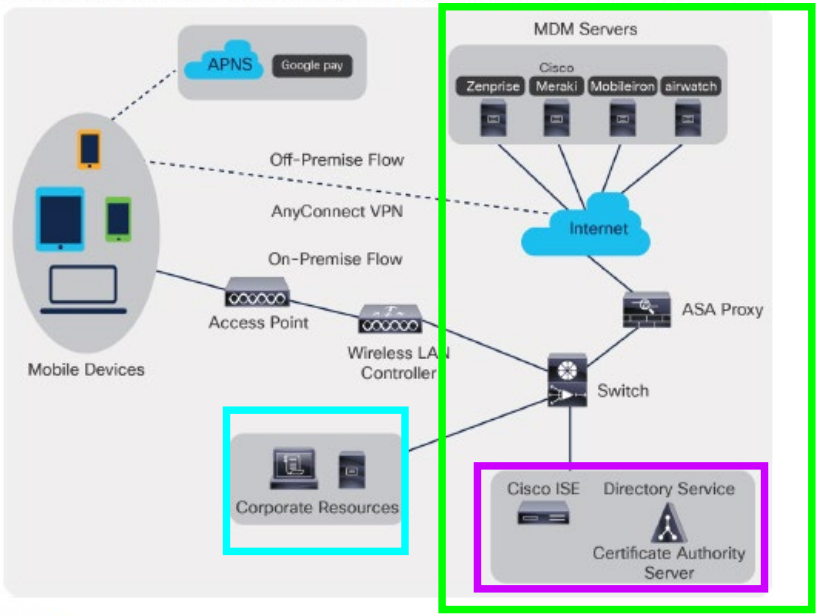


Figure 5.
Cisco ISE and MDM servers

Randomized and Changing MAC Deployment Guide at 43. Cisco further explains that with respect to mobile device management (MDM) server integration with ISE, "ISE is the enforcement point . . . [that] then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

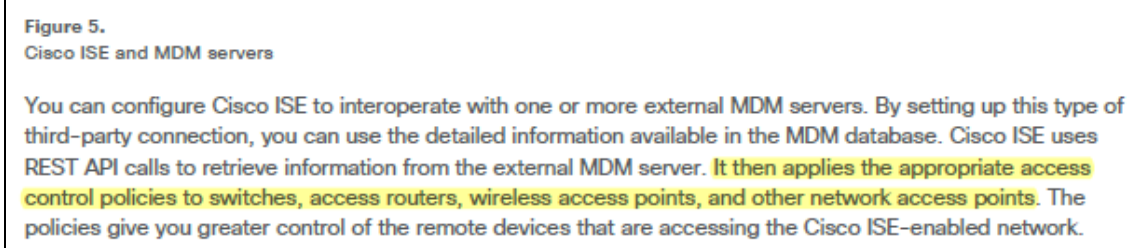


Figure 5.
Cisco ISE and MDM servers

You can configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. It then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network.

Cisco further explains, with respect to MDM server integration with ISE, that access devices (termed "unregistered endpoints") "are redirected to a registration page that is hosted on the MDM server," and further that endpoints in remediation "are granted restricted access"—that is, they are "communicating [with] a restricted subset of the protected network, the restricted subset including a gatekeeper."

Supported MDM use cases

Cisco ISE performs the following functions with the external MDM server:

- Manages device registration: Unregistered endpoints that access the network are redirected to a registration page that is hosted on the MDM server. Device registration includes the user role, device type, and so on.
- Handles device remediation: Endpoints are granted restricted access during remediation.

Cisco describes this process flow elsewhere in the same document:

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	MDM integration process flow **Step 1.** The user associates a device with an SSID. **Step 2.** Cisco ISE makes an API call to the MDM server. **Step 3.** This API call returns a list of devices for the user and the posture statuses for the devices. **Note:** The input parameter is the MAC address of the endpoint device. For off-premises Apple iOS devices (any device that connects to Cisco ISE through a VPN), the input parameter is the UDID. **Step 4.** If the user's device is not on this list, it means that the device is not registered. Cisco ISE sends an authorization request to the Network Access Device (NAD) to redirect to Cisco ISE. The user is presented with the MDM server page. **Note:** You must register a device that is enrolled on the MDM server outside of a Cisco ISE network via the MDM portal. This is applicable for Cisco ISE Release 1.4 and later. Earlier Cisco ISE versions allow devices that are enrolled outside the Cisco ISE-enabled network to be automatically enrolled if they are compliant with the posture policies. **Step 5.** Cisco ISE uses MDM to provision the device and presents the appropriate window for the user to register the device. **Step 6.** The user registers the device in the MDM server, and the MDM server redirects the request to Cisco ISE through automatic redirection or manual browser refresh. **Step 7.** Cisco ISE queries the MDM server again for the posture status.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

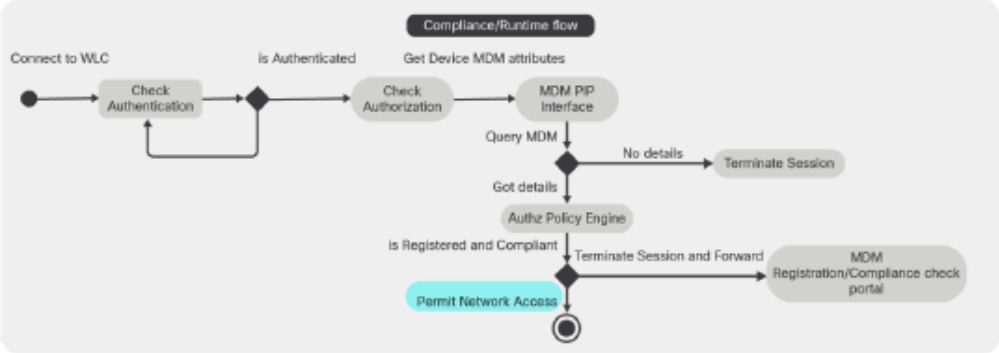
Step 8. If the user's device is not compliant with the posture (compliance) policies that are configured on the MDM server, the user is notified that the device is out of compliance. The user must take the necessary action to ensure that the device is compliant.

Step 9. When the user's device is compliant, the MDM server updates the device's state in its internal tables.

Step 10. If the user refreshes the browser now, the control is transferred back to Cisco ISE.

Step 11. Cisco ISE polls the MDM server once every four hours to get compliance information and issues the appropriate Change of Authorization (CoA). You can configure the polling interval. Cisco ISE also checks the MDM server every five minutes to make sure that it is available.

The following figure illustrates the MDM process flow.



Randomized and Changing MAC Deployment Guide at 46-47.

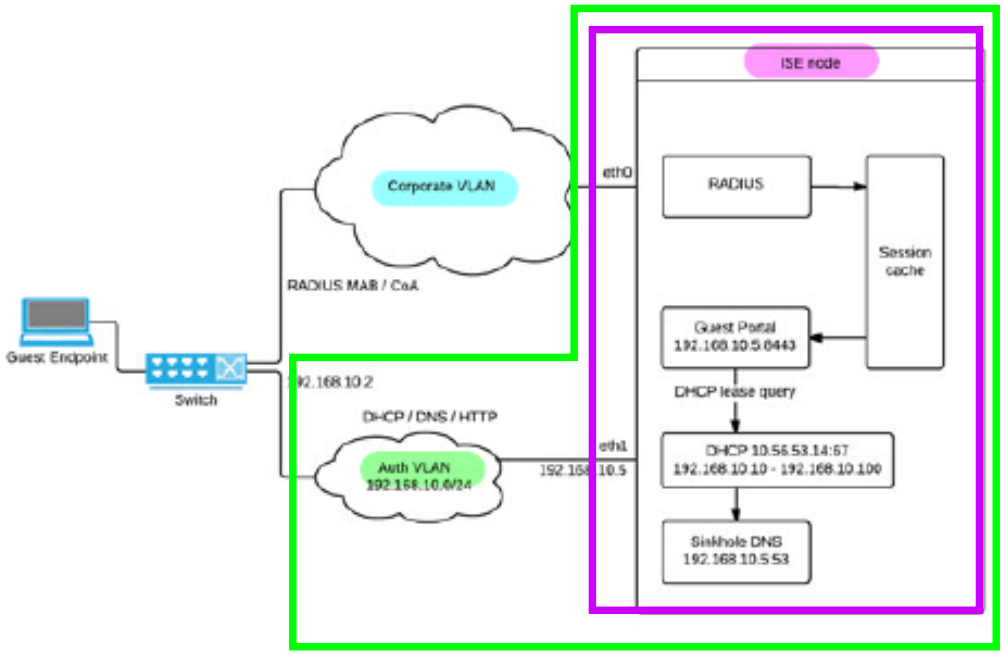
Finally, with respect to MDM servers integrated with ISE, Cisco's ISE has a gatekeeper associated with the restricted subset of the protected network. Cisco further explains how ISE can be the "enforcement point" that "applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	Cisco ISE also integrates with MDM servers using the Cisco MDM Server Info API, Version 2, to allow devices to access the network over VPN via Cisco AnyConnect 4.1 and Cisco Adaptive Security Appliances 9.3.2 or later. In the following illustration, Cisco ISE is the enforcement point and the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution. You can configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. It then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network. Randomized and Changing MAC Deployment Guide at 43. By way of a specific example, Cisco's ISE can also operate in conjunction with access points including Cisco or third party (i.e. non-Cisco) "network access devices (NAD)" (the claimed "access points"). ISE 3.0 Admin Guide at 804-06. In this setup, a "guest endpoint" (a claimed "access device") requests access to the network, including the Corporate VLAN (the claimed "less-restricted subset of the protected network"). The guest endpoint sends this request through a communication port of the network access device (the claimed "access point"). When the guest endpoint sends a request to connect, the communication port is configured for communicating between the guest endpoint and the green region of the network, including an Authorization VLAN or "Auth VLAN" (the green zone being the claimed "restricted subset of the protected network"). The restricted subset further includes a gatekeeper in the form of its ISE node that can assess the endpoint's security posture.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

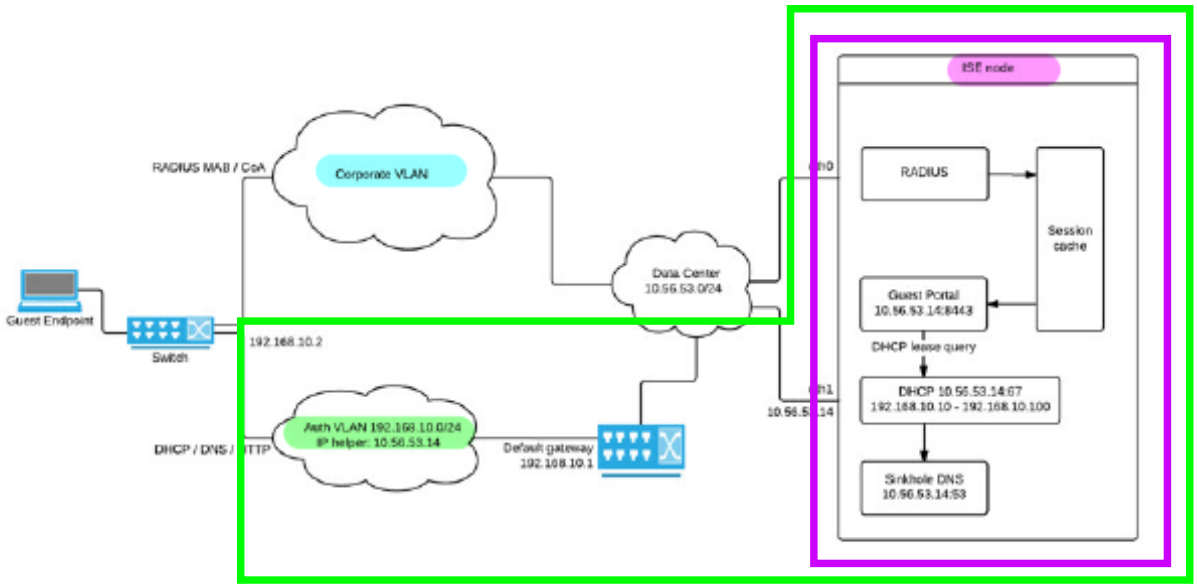
Figure 31: Auth VLAN Connected to Cisco ISE Node



The following diagram displays a network with Auth VLAN and an IP helper.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Figure 32: Auth VLAN Configured with IP Helper



U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

Multiple VLANs may be connected to one network interface card by configuring a VLAN IP helper from the NAD configuration. For more information about configuring an IP helper, see the administration guide for the network device for instructions. For guest access flows that include VLANs with IP helpers, define a guest

Admin Guide at 804-06.

By way of another specific example, Cisco's ISE has an ***Easy Connect Mode***, whereby it "enables you to easily connect users from a wired endpoint to a network in a secure manner and monitor those users by authenticating them through an Active Directory Domain Controller and not by Cisco ISE." With Easy Connect, "ISE issues a [Change of Authorization ("CoA")] after the external server (AD) authenticates the user."

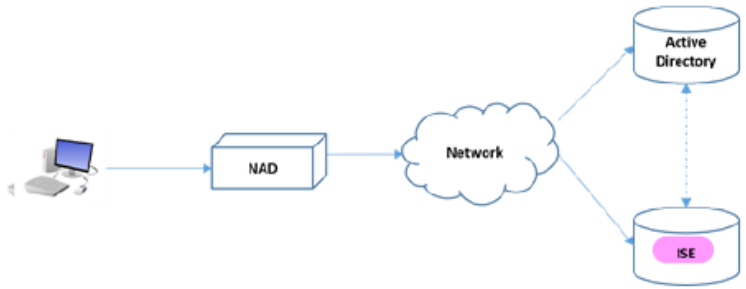
U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Easy Connect Enforcement Mode Process Flow

The Easy Connect Enforcement mode process is as follows:

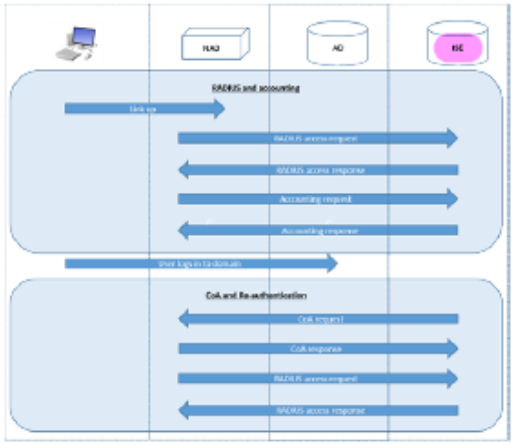
1. The user connects to the NAD from a wired endpoint (such as a PC for example).
2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD.
3. The user logs in to the domain and a security audit event is sent to Cisco ISE.
4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event.
5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy.

Figure 20: Easy Connect Enforcement Mode Basic Flow



U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Figure 21: Easy Connect Enforcement Mode Detailed Flow



For more information about configuring Enforcement mode, see Configure Easy Connect Enforcement Mode, on page 582.

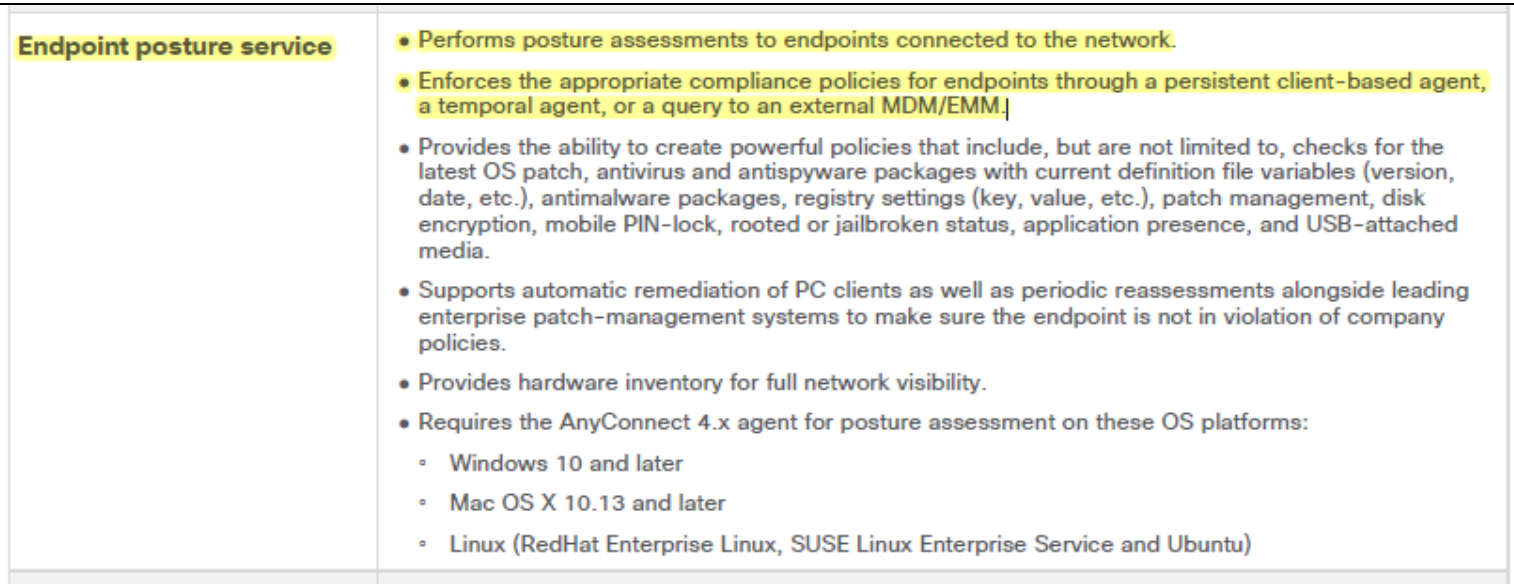
In Easy Connect Mode, "The user connects to the [network access device ("NAD"), e.g. an access point] from a wired endpoint (such as a PC for example)[,]" and after several steps, "Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and ***the user is provided access by the NAD to the network based on that policy***." Having a step whereby the user is being provided access to the network means, by implication, that the user did not have network access prior to that step. Thus, at that point, the user was restricted from certain network access, and thus "the communication port [was] configured for communicating between the access device and ***a restricted subset*** of the protected network[.]"

Moreover, Cisco's ISE has a gatekeeper associated with the restricted subset of the protected network. Cisco further explains how ISE collects certain information from the endpoint such as "the MAC address from RADIUS and the IP address" then "issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access[.]"

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

[41-b] applying a security policy to the access device, responsive to the request;	Cisco ISE "appl[ies] a security policy to the access device, responsive to the request [for access,]" or induces others to do so. Cisco explains that the "Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network." • **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods. • **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation. • **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services. ISE 3.0 Admin Guide at 2. Cisco further explains that it "[p]erforms posture assessments to endpoints connected to the network" and "enforces the appropriate compliance policies for [those] endpoints" through different mechanisms. Such "security policies" "include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages . . . antimalware packages . . . patch management . . . rooted or jailbroken status [and] application presence[,]" among others.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	 ISE Data Sheet at 7. Cisco explains how ISE "is a policy-based, network-access-control solution" whose Policy Sets "enable [the user] to logically group authentication and authorization policies within the same set."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Policy Sets

Cisco ISE is a policy-based, network-access-control solution, which offers network access policy sets, allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type, and similar parameters. When you install Cisco ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules.

When creating policy sets, you can configure these rules (configured with conditions and results) in order to choose the network access services on the policy set level, the identity sources on the authentication policy level, and network permissions on the authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE-supported dictionaries for different vendors. Cisco ISE allows you to create conditions as individual resuable policy elements.

The network access service to be used per policy set to communicate with the network devices is defined at the top level of that policy set. Network access services include:

- Allowed protocols—the protocols configured to handle the initial request and protocol negotiation.
- A proxy service—sends requests to an external RADIUS server for processing.

ISE 3.0 Admin Guide at 856; *see also id.* at 858 (Authentication Policies); 874 ("Create Authorization Policies with Endpoint-Analytics Attributes"), 882 ("Cisco ISE uses rule-based policies to provide network access. A policy is a set of rules and results, where the rules are made up of conditions."), 901 ("You can configure authorization profiles and policies in Cisco ISE using the IPv6 attributes in your rule conditions to process such requests from IPv6-enabled endpoints and ensure that the endpoint is compliant."), 940-41 (with Cisco's TrustSec Architecture, "[T]he security group tag (SGT)[] allows Cisco ISE to enforce access control policies by enabling the endpoint device to act upon the SGT to filter traffic."), 1030-31 ("Compliance Module"), 1032 ("Check Posture Compliance"), 1052 (Configure Posture Policies); 1057 ("Client Posture Assessment"), 1057-58 (Posture Assessment Options); *and see generally* 1009-1110 (Chapter 12, Titled "Compliance").

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Cisco explains that a user can "check" or "view" the "posture compliance" of endpoints through the ISE interface—thereby "applying a security policy to the access device, responsive to the request [for access.]"

Check Posture Compliance

Step 1 Log in to Cisco ISE and access the dashboard.

Step 2 In the **Posture Compliance** dashlet, hover your cursor over a stack bar or sparkline.

A tooltip provides detailed information.

Step 3 Expand the data categories for more information.

Step 4 Expand the **Posture Compliance** dashlet.

A detailed real-time report is displayed.

Note You can view the posture compliance report in the **Context Visibility** window. Navigate **Context Visibility** > **Endpoints** > **Compliance**. This window displays different charts based on **Compliance Status**, **Location**, **Endpoints**, and **Applications by Categories**.

You might see the posture status for endpoints that do not have any active sessions. For example, if the last known posture status for an endpoint is **Compliant**, the status remains **Compliant** in the **Context Visibility** window until the next update is received for the endpoint, even if the endpoint session is terminated. The posture status is retained in the **Context Visibility** window until that endpoint is deleted or purged.

Source: ISE 3.0 Admin Guide at 1032.

As described above (with respect to an MDM server integrated with ISE), ISE "ISE is the enforcement point[, which] obtains data from the MDM server [and] then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points." Randomized and Changing MAC Deployment Guide at 43. Thus, ISE "appl[ies] a security policy to the access device, responsive to the request [for access.]"

In one example, Cisco explains how ISE "appl[ies] a security policy . . ." with respect to access devices in the form of "guest devices." In particular, Cisco explains how such access devices can be required to "first download [a] posture agent that checks their posture profile and verifies if their device is compliant" with the network security criteria. *Id.* at 401. By "verif[ying] if [a] device is compliant," ISE "applies a security policy" to it.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Guest Device Compliance

When guests and non-guests access the network through credentialed Guest portals, you can check their devices for compliance before they are allowed to gain access. You can route them to a Client Provisioning window and require them to first download the posture agent that checks their posture profile and verifies if their device is compliant. You can do this by enabling the option in the **Guest Device Compliance Settings** in a credentialed Guest portal, which displays the Client Provisioning window as part of the guest flow.

Note Client posture assessment in guest flow supports only the Temporal agent.

The Client Provisioning service provides posture assessments and remediations for guests. The Client Provisioning portal is available only with a Central Web Authorization (CWA) guest deployment. The guest login flow performs a CWA, and the credentialed Guest portal is redirected to the Client Provisioning portal after performing acceptable-use-policy and change-password checks. The posture subsystem performs a Change of Authorization (CoA) on the network access device to reauthenticate the client connection once the posture has been assessed.

Admin Guide at 401. Cisco describes several different posture agents that accomplish this. *See id.* at 1010-11.

Posture Types

The following posture agents monitor and enforce Cisco ISE posture policies:

- **AnyConnect**: Deploys the AnyConnect agent to monitor and enforce Cisco ISE posture policies that require interaction with the client. The AnyConnect agent stays on the client. For more information about using AnyConnect in Cisco ISE, see Cisco AnyConnect Secure Mobility, on page 1099.
- **AnyConnect Stealth**: Runs posture as a service, with no user interface. The agent stays on the client.

  When you choose the AnyConnect Stealth posture type in the posture requirement, some of the conditions, remediations, or attributes in a condition are disabled (grayed out). For example, when you enable AnyConnect Stealth requirement, the Manual Remediation Type is disabled (grayed out) because this action requires client-side interaction.

  When you map the posture profile to the AnyConnect configuration, and then map the AnyConnect configuration to the Client Provisioning window for AnyConnect Stealth mode deployment:

  - AnyConnect can read the posture profile and set it to the intended mode.
  - AnyConnect can send information related to the selected mode to Cisco ISE during the initial posture request.
  - Cisco ISE can match the right policy, based on the mode and other factors, such as identity group, OS, and compliance module.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

- **Temporal Agent**: When a client attempts to access the trusted network, Cisco ISE opens the Client Provisioning portal. The portal instructs the user to download and install the agent, and run the agent. The temporal agent checks the compliance status, and sends the status to Cisco ISE. Cisco ISE acts based on the results. The temporal agent removes itself from the client after compliance processing completes. The temporal agent does not support custom remediation. The default remediation supports only message text.

  The Temporal Agent does not support the following conditions:

  - Service Condition MAC—System Daemon check
  - Service Condition-MAC—Daemon or User Agent check
  - PM—Up To Date check
  - PM—Enabled check
  - DE—Encryption check

- For the Temporal Agent, you can only view Patch Management conditions containing the **Installation** check type in the **Requirements** window.
- Cisco ISE does not support VLAN-controlled posture with the Temporal Agent for macOS. When you change the network access from an existing VLAN to a new VLAN, the user's IP address is released before the VLAN change. The client gets a new IP address by DHCP when the user connects to the new VLAN. Recognizing the new IP address requires root privileges, but the Temporal Agent runs as a user process.
- Cisco ISE supports ACL-controlled posture environment, which does not require the refreshing of endpoint IP addresses.
- For more information about configuring the Temporal agent in Cisco ISE, see Configure Cisco Temporal Agent Workflow, on page 1074.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	In another example, the Cisco ISE "appl[ies] a security policy to the access device, responsive to the request [for access]" when it operates with respect to access points (including both Cisco and third-party (i.e. non-Cisco)) access points. There, as explained above with respect to claim element 41-1, a "guest endpoint" (the claimed "access device") connects to the network via a (non-Cisco) ***network access device*** or ***NAD*** (the claimed "access point"). ISE applies a security policy to the guest endpoint—as described below in step 3 (by "run[ning] the configured authentication and authorization policy") and/or step 11 (by "validat[ing] endpoint compliance" and "author[izing] the endpoint").

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

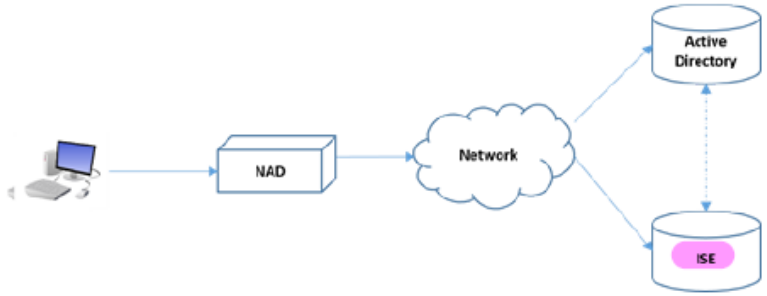
1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

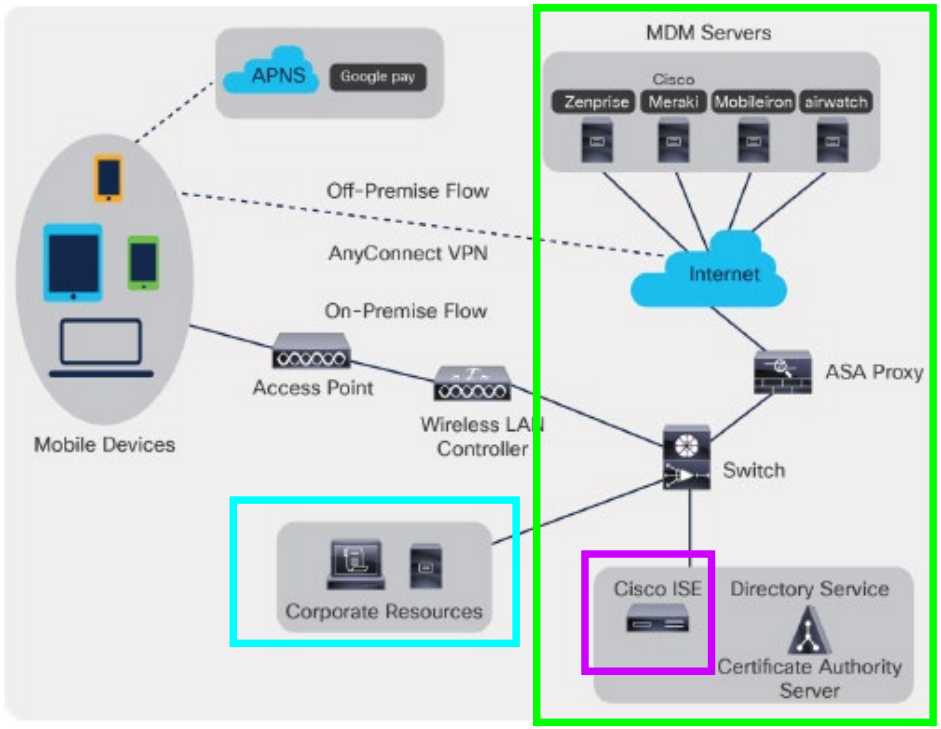
ISE 3.0 Admin Guide at 804; *see also id.* at 805-06 (schematics of same).

Finally, in another example—ISE's Easy Connect Enforcement Mode—ISE "collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event. [] After all data is collected and merged in the session directory, Cisco ISE issues a CoA to

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

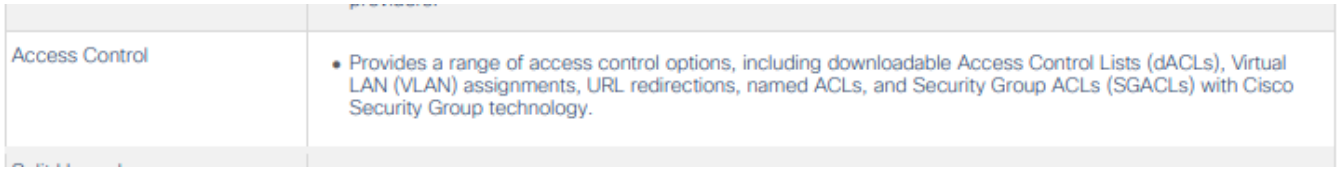
	the NAD ***(based on the appropriate policy managed in the policy service node***), and the user is provided access by the NAD to the network based on ***that policy***." Thus, ISE "applies a security policy." **Easy Connect Enforcement Mode Process Flow** The Easy Connect Enforcement mode process is as follows: 1. The user connects to the NAD from a wired endpoint (such as a PC for example). 2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD. 3. The user logs in to the domain and a security audit event is sent to Cisco ISE. 4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event. 5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy. ***Figure 20: Easy Connect Enforcement Mode Basic Flow*** 
[41-c] reconfiguring the communicatio n port for communicatin	Cisco ISE "reconfigur[es] the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements of the security policy are satisfied," or induces others to do so.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

g data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements of the security policy are satisfied; and	 As shown, if ISE determines that an access device (e.g. Mobile Devices) satisfies requirements of the security policy, it reconfigures the communication port on the access point to allow the access device to communicate with the less-restricted subset of the protected network (here, "Corporate Resources)." Randomized Changing MAC at 43; *see also id.* at 57 ("If the device is registered with Cisco ISE, is registered with MDM, and is compliant with Cisco ISE and MDM policies, it is ***granted access to the network based on the access control policies configured in Cisco ISE***."). Additionally, as shown isn the schematic, if the requirements of the security policy are satisfied, the mobile devices have access through the switch to the corporate resources. Thus, the communication port is "reconfigure[ed] for communicating data . . . without passing the data through the gatekeeper[.]" *Id.*

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Cisco also describes in its Data Sheet "a range of access control options" for this step, "including downloadable Access Control Lists (dACLs), Virtual LAN (VLAN) assignments, URL redirections, named ACLs, and Security Group ACLs (SGACLs) with Cisco Security Group technology[.]" By using any or all of these methods, ISE "reconfigur[es] the communication port for communicating data between the access device and the less-restricted subset of the protected network"—for example, network resources. Additionally, as show above with respect to MDM servers integrated with ISE, if the requirements of the security policy are satisfied, the communication port is "reconfigure[ed] for communicating data . . . without passing the data through the gatekeeper[.]" *Id.*



Access Control	• Provides a range of access control options, including downloadable Access Control Lists (dACLs), Virtual LAN (VLAN) assignments, URL redirections, named ACLs, and Security Group ACLs (SGACLs) with Cisco Security Group technology.

ISE Data Sheet at 5.

By way of an example previously described—guest device compliance—Cisco states that "the posture agent [] checks their posture profile and verifies if their device is compliant[,]" and further that "the Client Provisioning service provides posture assessments"—that is, ISE determines if "requirements of the security policy are satisfied." ISE 3.0 Admin Guide at 401. Upon such satisfaction, ISE grants the access device access to network resources, thereby "reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network[.]" *See id.* Finally, as show above with respect to MDM servers integrated with ISE, if the requirements of the security policy are satisfied, the communication port is "reconfigure[ed] for communicating data . . . without passing the data through the gatekeeper[.]" *Id.*

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Guest Device Compliance

When guests and non-guests access the network through credentialed Guest portals, you can check their devices for compliance before they are allowed to gain access. You can route them to a Client Provisioning window and require them to first download the posture agent that checks their posture profile and verifies if their device is compliant. You can do this by enabling the option in the **Guest Device Compliance Settings** in a credentialed Guest portal, which displays the Client Provisioning window as part of the guest flow.

Note Client posture assessment in guest flow supports only the Temporal agent.

The Client Provisioning service provides posture assessments and remediations for guests. The Client Provisioning portal is available only with a Central Web Authorization (CWA) guest deployment. The guest login flow performs a CWA, and the credentialed Guest portal is redirected to the Client Provisioning portal after performing acceptable-use-policy and change-password checks. The posture subsystem performs a Change of Authorization (CoA) on the network access device to reauthenticate the client connection once the posture has been assessed.

ISE 3.0 Admin Guide at 401-02.

A third example relates to ISE operating with respect to access points including third-party (i.e. non-Cisco) access points. As previously described with respect to claim element 41-b, ISE "runs the configured authentication and authorization policy[,] "validates endpoint compliance[,]" and "authorizes the endpoint"—and thus "applies a security policy to the access device, responsive to the request." ISE 3.0 Admin Guide at 804.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	Once ISE determines that "requirements of the security policy are satisfied," it "sends the [change of authorization ("CoA")], authorizes the endpoint, and bypasses the sink hole[,] and then the "the guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network." By granting "appropriate access" and issuing a change of authorization (CoA), ISE" "reconfigur[es] the communication port for communicating data between the access device and the less-restricted subset of the protected network." Additionally, Cisco describes how a user "can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication," and shows this in the schematics. As described this way and as further shown in the schematic, if the requirements of the security policy are satisfied, the guest endpoints "communicat[e] data [to] the less-restricted subset of the protected network without passing the data through" through ISE—that is, "without passing the data through the gatekeeper[.]"

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

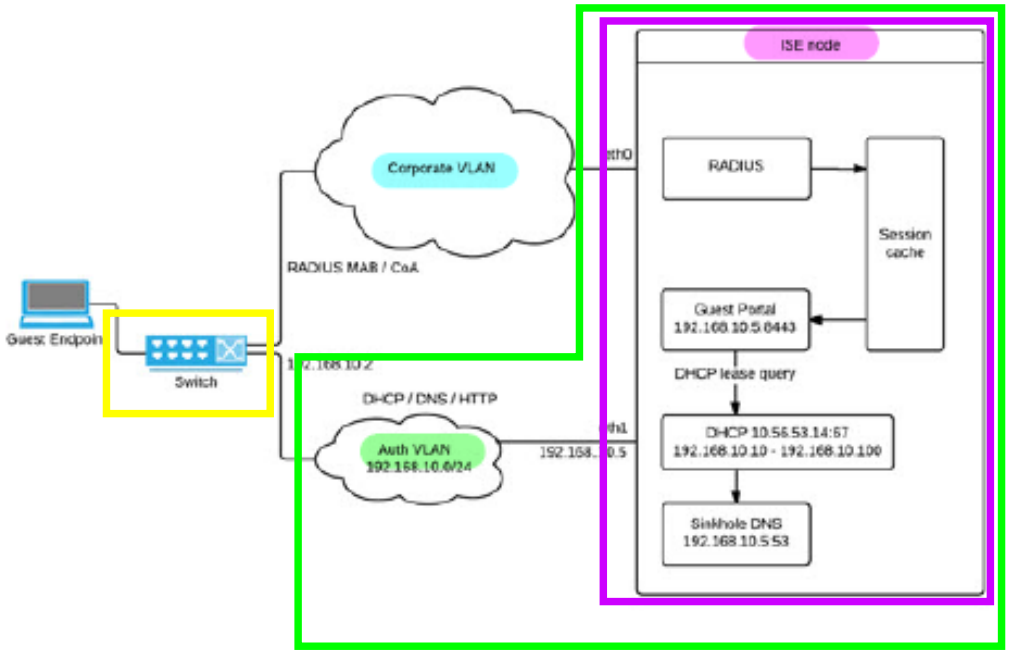
You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

Multiple VLANs may be connected to one network interface card by configuring a VLAN IP helper from the NAD configuration. For more information about configuring an IP helper, see the administration guide for the network device for instructions. For guest access flows that include VLANs with IP helpers, define a guest portal, and select that portal in an authorization profile that is bound to MAB authorization. For more information about guest portals, see the Cisco ISE Guest Services section in *Cisco ISE Admin Guide: Guest and BYOD* .

The following diagram displays a basic network setup when an Auth VLAN is defined (the Auth VLAN is connected directly to a Cisco ISE node).

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

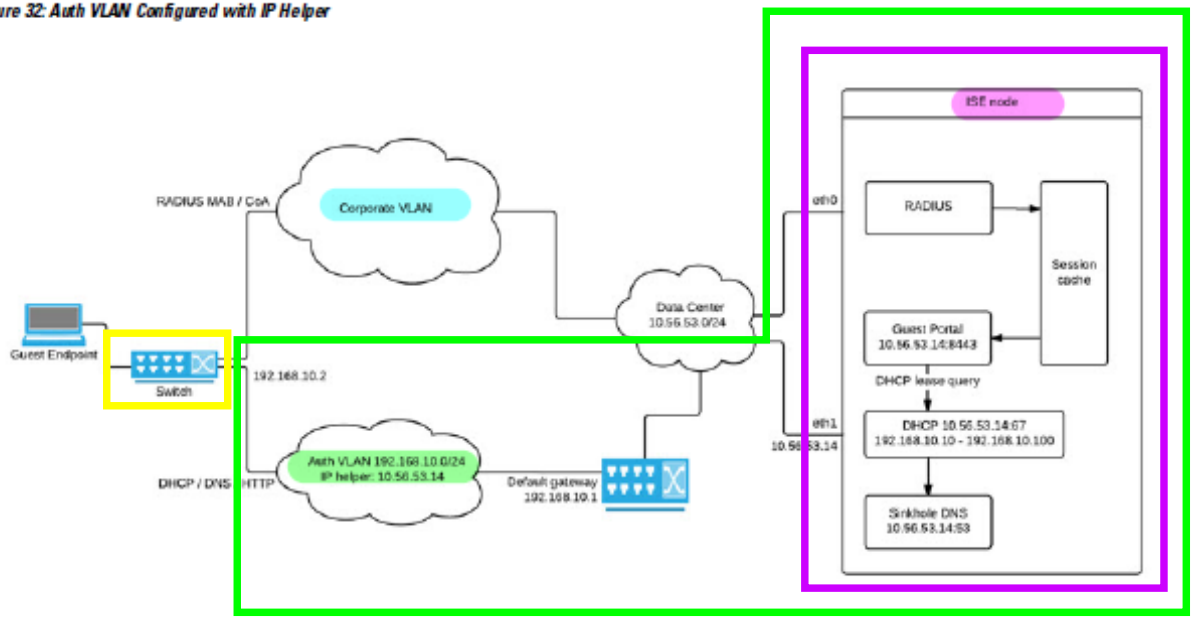
Figure 31: Auth VLAN Connected to Cisco ISE Node



The following diagram displays a network with Auth VLAN and an IP helper.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

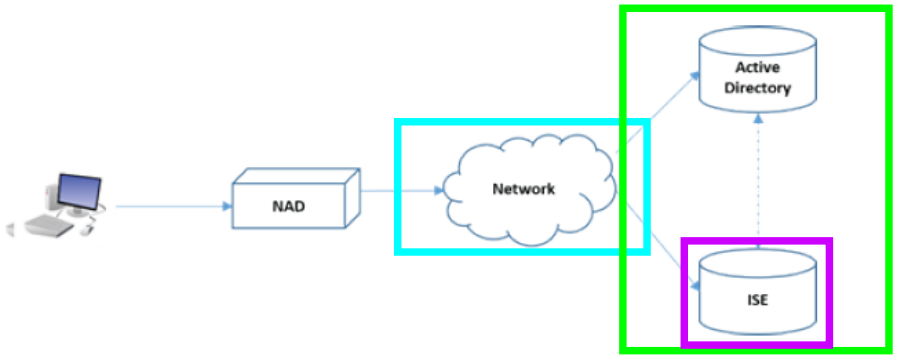
Figure 32: Auth VLAN Configured with IP Helper



ISE 3.0 Admin Guide at 804-06.

In one further example described above—ISE's Easy Connect Enforcement Mode—ISE collects certain data, after which it "issues a CoA to the [network access device, ("NAD"] (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy." ISE 3.0 Admin Guide at 580-81. By issuing a CoA to the NAD, to provide the user access to the network, ISE "reconfigur[es] the communication port for communicating data between the access device and the less-restricted subset of the protected network[.]" Additionally, as shown in the schematic, if the requirements of the security policy are satisfied, the access devices have network access without passing their data through ISE—that is, "without passing the data through the gatekeeper[.]"

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	Easy Connect Enforcement Mode Process Flow The Easy Connect Enforcement mode process is as follows: 1. The user connects to the NAD from a wired endpoint (such as a PC for example). 2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD. 3. The user logs in to the domain and a security audit event is sent to Cisco ISE. 4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event. 5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy. *Figure 20: Easy Connect Enforcement Mode Basic Flow* 
[41-d] updating the access device if requirements of the security	Cisco ISE "update[es] the access device if requirements of the security policy are not satisfied[,]" or induces others to do so. Cisco describes "Posture Remediation Options," and also "Custom Posture Remediation Actions," which include "a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) remediation types." ISE 3.0 Admin Guide at 1059, 1061.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

policy are not satisfied.

Posture Remediation Options

The following table provides a list of posture remediation options that are supported by the Cisco ISE Posture Agents for Windows and Macintosh, and the Web Agent for Windows.

Table 162: Posture Remediation Options

ISE Posture Agent for Windows	ISE Posture Agent for Macintosh OS X
Message Text (Local Check)	Message Text (Local Check)
URL Link (Link Distribution)	URL Link (Link Distribution)
File Distribution	—
Launch Program	—
Antivirus Definition Update	Antivirus Live Update
Antispyware Definition Update	Antispyware Live Update
Patch Management Remediation (AC 4.1 - and ISE 1.4)	—
Windows Update	—
WSUS	—

Custom Posture Remediation Actions

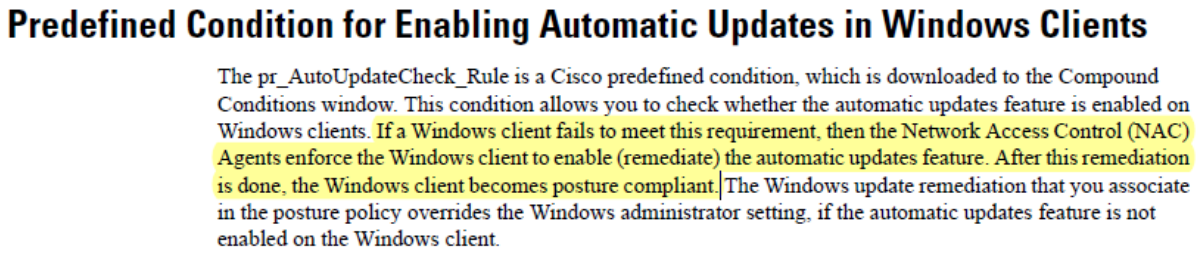
A custom posture remediation action is a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) remediation types.

By "remediat[ing]" an endpoint, Cisco ISE "update[es] the access device if requirements of the security policy are not satisfied." *See also* ISE 3.0 Admin Guide at 1061-64 ("Add an Antispyware Remediation: You can create an antispyware remediation, which ***updates clients*** with up-to-date file definitions for compliance after remediation."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

and similar disclosures of updates including Antivirus Remediation, Patch Management Remediation, and Windows Server Update Services (WSUS) remediations, and remediation mechanisms including downloading files, launching programs/applications, or accessing remediation resources through a URL link).

See also ISE 3.0 Admin Guide at 1029 (automatic updates in Windows clients):



Predefined Condition for Enabling Automatic Updates in Windows Clients

The pr_AutoUpdateCheck_Rule is a Cisco predefined condition, which is downloaded to the Compound Conditions window. This condition allows you to check whether the automatic updates feature is enabled on Windows clients. If a Windows client fails to meet this requirement, then the Network Access Control (NAC) Agents enforce the Windows client to enable (remediate) the automatic updates feature. After this remediation is done, the Windows client becomes posture compliant. The Windows update remediation that you associate in the posture policy overrides the Windows administrator setting, if the automatic updates feature is not enabled on the Windows client.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

and at 1048-50 (Patch Management Condition Settings):

Patch Management Condition Settings

The following table describes the fields in the **Patch Management Conditions** window. To view this window, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Patch Management Condition**.

Table 157: Patch Management Condition

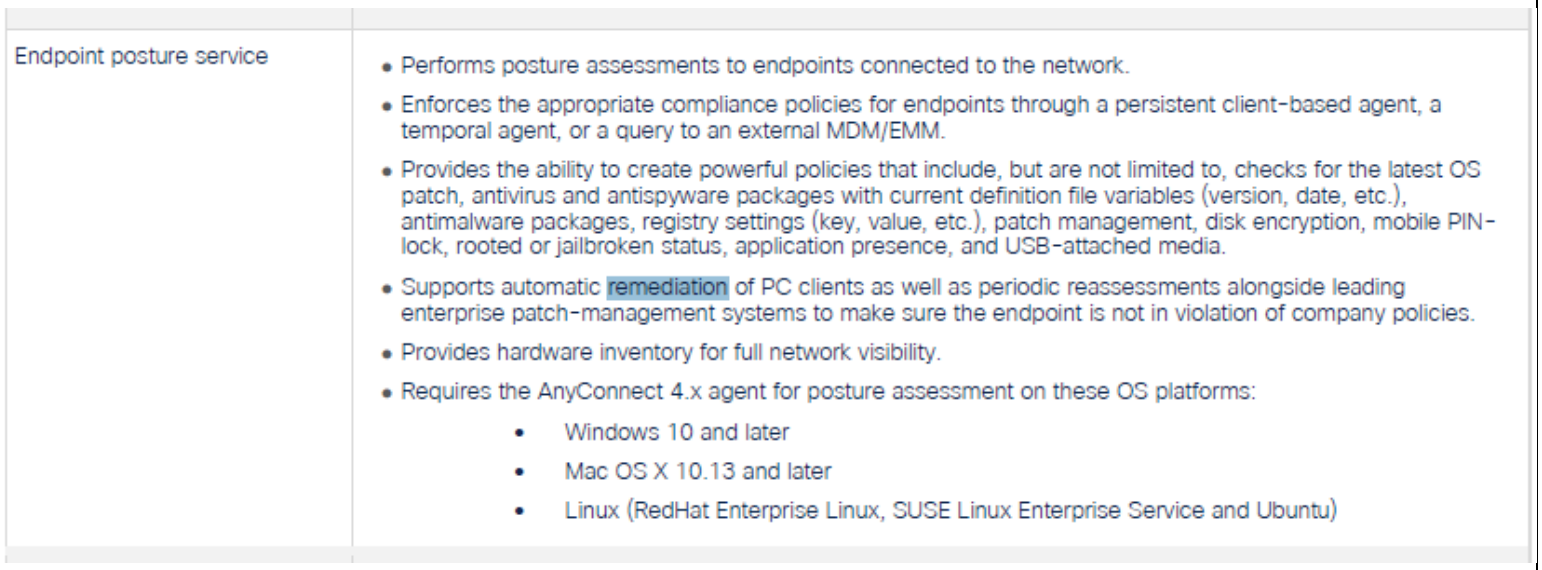
Field Name	Usage Guidelines
Name	Enter the name of the patch management condition.
Description	Enter a description for the patch management condition.
Operating System	Choose an operating system to check the installation of a patch management software on the endpoint, or check the latest patch management definition file updates to which the condition is applied. You can select the Windows OS or macOS. You can also select more than one version of an operating system to create the patch management condition.
Vendor Name	Choose a vendor from the **Vendor Name** drop-down list. Based on your selection, the patch management products and their supported versions, check type, and minimum compliant module support details are displayed in the **Products for Selected Vendor** table. The list in the table changes according to the selected operating system.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Field Name	Usage Guidelines
Check Patches Installed	(Available only when you select the **Up To Date** check type) You can configure severity levels for missing patches, which are then deployed based on the severity. Choose one of the following options: • **Critical Only**: To check if critical software patches are installed on the endpoints in your deployment. • **Important and Critical**: To check if important and critical software patches are installed on the endpoints in your deployment. • **Moderate, Important, and Critical**: To check if moderate, important, and critical software patches are installed on the endpoints in your deployment. • **Low To Critical**: To check if low, moderate, important, and critical software patches are installed on the endpoints in your deployment. • **All**: To install the missing patches for all severity levels.

and also Randomized Changing MAC at 44 ("Cisco ISE performs the following functions with the external MDM server: . . . Handles device remediation: Endpoints are granted restricted access during remediation."); *and also* ISE Data Sheet at 4 ("Automated device-compliance checks for device-posture and ***remediation*** options using Cisco Secure Client (formerly Anyconnect agent), Temporal and Agentless options . . ." and 7 ("Supports automatic ***remediation*** of PC clients as well as periodic reassessments . . .")

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	Automated device-compliance checks for device-posture and remediation options using Cisco Secure Client (formerly Anyconnect agent), Temporal and Agentless options with custom scripts support. Cisco Secure Client Temporal and Agentless are two different ways to gather posture from endpoints beyond a full agent. Agentless option is supported from ISE 3.0 onwards lo Cisco Secure client also provide advanced VPN services for desktop and laptop checks. ISE also integrates with market-leading Mobile Device Management/Enterprise Mobility Management (MDM/EMM) vendors. MDM integration helps ensure that a mobile device is both secure and policy compliant before it is given access to the network. . . .  Endpoint posture service • Performs posture assessments to endpoints connected to the network. • Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM. • Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media. • Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies. • Provides hardware inventory for full network visibility. • Requires the AnyConnect 4.x agent for posture assessment on these OS platforms: • Windows 10 and later • Mac OS X 10.13 and later • Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu) ISE Data Sheet at 4, 7.
42. The method of claim 41, wherein the	Cisco ISE performs "[t]he method of claim 41, wherein the security policy includes an audit of the access device[,]" and induces others to do so.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

security policy includes an audit of the access device.	As disclosed above with respect to claim 39, Cisco's ISE performs "[t]he method of claim 28, wherein the security policy includes an audit of the access device." Thus, Cisco ISE performs "[t]he method of claim 41, wherein the security policy includes an audit of the access device[,]" and induces others to do so.
43. The method of claim 41, further including communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine if the access device satisfies	Cisco ISE performs "[t]he method of claim 41, further including communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine if the access device satisfies the requirements of the security policy[,]"and induces others to do so. As disclosed above with respect to claim element 41-b, Cisco's ISE uses "posture agents" (the claimed "agent executing on the access device"). Furthermore, as disclosed above with respect to claim 4, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the network gatekeeper is further configured to obtain ***system data*** from the access device." It is further disclosed with respect to claim 4 how Cisco's ISE obtains data (including the claimed "system data") from access devices through different methods and devices. These methods and devices include, for example, • The AnyConnect Agent (which can "report[] a complete list of running and installed applications" on the access device, ISE 3.0 Admin Guide at 1102-03); • The AnyConnect Stealth Agent (which reports certain information back to ISE, *id.* at 1010-11), and Also as disclosed above with respect to claim 4, Cisco's ISE obtains "system data," including (by way of three non-limiting examples) "hardware attributes," "endpoint attribute data" and "simple posture conditions." Therefore, Cisco ISE "communicat[es] between the gatekeeper and an agent executing on the access device to obtain system data from the access device," or induces others to do so. Furthermore, as disclosed above with respect to claim 5, Cisco's ISE comprises "[t]he network gatekeeper of claim 4, wherein the network gatekeeper is further configured to use the system data [of claim 4] to determine if the access device meets requirements of a security policy, . . ." Therefore, Cisco ISE "appl[ies] the security policy includes

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

the requirements of the security policy.	using the system data to determine if the access device satisfies the requirements of the security policy[,]" or induces others to do so. Thus, Cisco ISE performs "[t]he method of claim 41, further including communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine if the access device satisfies the requirements of the security policy[,]"and induces others to do so.
48. The method of claim 41, wherein the access point is a network switch.	Cisco ISE performs "[t]he method of claim 41, wherein the access point is a network switch[,]" and induces others to do so. As disclosed above with respect to claim 18, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a network switch." Thus, Cisco ISE performs the "method of [granting access to a protected network recited in] claim 28, wherein the access point is a network switch[,]" and induces others to do so.
49. The method of claim 41, wherein the access point is a wireless access point.	Cisco ISE performs "[t]he method of claim 41, wherein the access point is a wireless access point[,]" and induces others to do so. As disclosed above with respect to claim 16, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a wireless access point." (Furthermore, as disclosed above with respect to claim 17, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a wireless access point configured to support an 802.1x standard.") Thus, Cisco ISE performs "[t]he method of claim 41, wherein the access point is a wireless access point[,]"and induces others to do so.
50. The method of claim 41,	Cisco ISE performs "[t]he method of claim 41, wherein the access point is a remote access virtual private network[,]"and induces others to do so.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

wherein the access point is a remote access virtual private network.	As disclosed above with respect to claim 25, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a remote access virtual private network." Thus, Cisco ISE performs "[t]he method of claim 41, wherein the access point is a remote access virtual private network[,]"and induces others to do so.
53. The method of claim 41, further including authenticating a user of the access device.	Cisco ISE performs "[t]he method of claim 41, further including authenticating a user of the access device." As disclosed above with respect to claim 23, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the network gatekeeper is further configured ***to authenticate a user of the access device***." Furthermore, as disclosed above with respect to claim 11, Cisco's ISE comprises ***authentication policies*** for determining identity. Furthermore, as disclosed above with respect to claim 17, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a wireless access point configured to support an 802.1x standard" — an authentication standard. Finally, as disclosed above with respect to claim element 41-a ("receiving a request for access to a less-restricted subset of the protected network from an access device, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper;"), Cisco discloses (by way of two non-limiting examples) that ISE "authenticates" a user of an access device: (1) access points (including those of both Cisco and third-party (i.e., non-Cisco) and Easy Connect mode. Thus, Cisco ISE performs "[t]he method of claim 41, further including authenticating a user of the access device."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Claim 57

[57-preamble] A method of granting access to a protected network, the method comprising:	Cisco infringes this claim by making, using, testing, offering for sale, and selling the ISE product and system and through performance of each of the claimed steps and/or providing instructions and data from its servers to third-parties to perform at least one of the claimed steps, or induces others to do so as set forth in claim element 1-c. Cisco ISE performs "[a] method of granting access to a protected network[,]"as disclosed above with respect to claim 41.
[57-a] receiving a first communication from an access device at a communication port, the communication port being configured to pass the first communication to a restricted subset of the protected network, the restricted subset including a	Cisco ISE "receiv[es] a first communication from an access device at a communication port, the communication port being configured to pass the first communication to a restricted subset of the protected network, the restricted subset including a gatekeeper configured to enforce a security policy for access to a less-restricted subset of the protected network[,]" and induces others to do so. As disclosed above with respect to claim element 41-a, Cisco ISE "receiv[es] a request for access to a less-restricted subset of the protected network from an access device, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper" or induces others to do so. The "request for access . . . from an access device" described with respect to claim element 41-a is one example of a "first communication from an access device" recited in claim 57-a. Furthermore, in claim 41-a, the "communication port of an access point [is] configured for communicating between the access device and a restricted subset of the protected network[.]" Thus, as to claim 57-a, "the communication port [is] configured to pass the first communication to a restricted subset of the protected network " And finally, with respect to claim 41, "the restricted subset include[es] a gatekeeper[.]" Thus with respect to claim 57-a, "the restricted subset including a gatekeeper configured to enforce a security policy for access to a less-restricted subset of the protected network[.]"

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

gatekeeper configured to enforce a security policy for access to a less-restricted subset of the protected network;	
[57-b] receiving a command from the gatekeeper, the command being responsive to the received first communication and being configured to reconfigure the communication port to communicate data to the less-restricted subset of the	Cisco ISE "receiv[es] a command from the gatekeeper, the command being responsive to the received first communication and being configured to reconfigure the communication port to communicate data to the less-restricted subset of the protected network[,]" and induces others to do so. As described above with respect to claim elements 41-b & c, Cisco ISE "[41-b] appl[ies]a security policy to the access device, responsive to the request; [and] [41-c] reconfigu[es] the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements of the security policy are satisfied[,]" and induces others to do so. Thus, Cisco ISE "receiv[es]a command from the gatekeeper, . . . being configured to reconfigure the communication port to communicate data to the less-restricted subset of the protected network[.]" Also as described above with respect to claim elements 41-c (the "reconfiguring . . ." step), are three examples whereby Cisco's ISE issues (and thus "receives") commands, which are "configured to reconfigure the communication port . . .": • Guest devices (whereby "the posture subsystem performs a change of authorization (CoA) on the network access device");

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

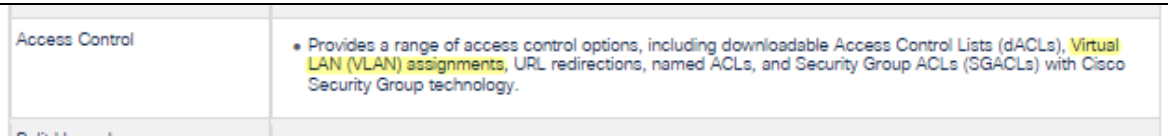
protected network;	• Access points (including Cisco and (third-party (i.e. non-Cisco)) access points, whereby Cisco ISE similarly "sends the CoA")); and • Easy connect mode (whereby Cisco's ISE "issues a CoA to the [network access device, ("NAD"] (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy." Thus, Cisco ISE "receiv[es] a command from the gatekeeper, the command being responsive to the received first communication and being configured to reconfigure the communication port to communicate data to the less-restricted subset of the protected network[,]" and induces others to do so.
[57-c] configuring the communication port to communicate data to the less-restricted subset of the protected network rather than merely the restricted subset of the protected network, responsive to the received command; and	Cisco ISE "configur[es] the communication port to communicate data to the less-restricted subset of the protected network rather than merely the restricted subset of the protected network, responsive to the received command[,]" and induces others to do so. As described above with respect to the prior claim element 57-b, Cisco's ISE "receiv[es] a command from the gatekeeper, the command being responsive to the received first communication and being configured to reconfigure the communication port to communicate data to the less-restricted subset of the protected network[.]" Receiving such commands "configur[es] the communication port . . ." as is recited in this step.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

[57-d] receiving a second communication from the access device at the communication port, the communication port now being configured to pass the second communication to the less-restricted subset of the protected network.	Cisco ISE "receiv[es] a second communication from the access device at the communication port, the communication port now being configured to pass the second communication to the less-restricted subset of the protected network[,]" and induces others to do so. As described above with respect to the prior claim element 57-c, Cisco's ISE "configur[es] the communication port to communicate data to the less-restricted subset of the protected network rather than merely the restricted subset of the protected network, responsive to the received command[.]" Because the communication port on the access device has been "configure[ed," and the access device can, as this point, "communicat[e] data [to] the less-restricted subset of the protected network without passing the data through the gatekeeper," (*see* claim element 41-c, incorporated above as to claim 57-b), subsequent communications from the access device are now "pass[ed] to the less-restricted subset of the protected network."
58. The method of claim 57, wherein configuring the communication port includes associating the communication	Cisco ISE performs "[t]he method of claim 57, wherein configuring the communication port includes associating the communication port with a VLAN[,]" and induces others to do so. Cisco discloses that generally, ISE "provides a range of access control options, including . . . Virtual LAN (VLAN) assignments. ISE Data Sheet at 5.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

port with a VLAN.



Access Control	• Provides a range of access control options, including downloadable Access Control Lists (dACLs), Virtual LAN (VLAN) assignments, URL redirections, named ACLs, and Security Group ACLs (SGACLs) with Cisco Security Group technology.

By way of a specific example, Cisco discloses that its can perform dynamic VLAN assignment with a RADIUS server. Cisco, Configure Dynamic VLAN Assignment with ISE and Catalyst 9800 Wireless LAN Controller at 3, 25 (June 2022), https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/217043-configure-dynamic-vlan-assignment-with-c.pdf (last visited May 22, 2023).

Introduction

This document describes the concept of dynamic VLAN assignment and how to configure the Catalyst 9800 wireless LAN controller (WLC) and Cisco Identity Service Engine (ISE) to assign wireless LAN (WLAN) in order to accomplish this for the wireless clients.

Requirements

Cisco recommends that you have knowledge of these topics:

- Have basic knowledge of the WLC and Lightweight Access Points (LAPs).
- Have functional knowledge of the AAA server such as ISE.
- Have a thorough knowledge of wireless networks and wireless security issues.

Configure Dynamic VLAN Assignment with ISE at 1.

By way of another example—Adaptive Network Control—Cisco describes how ISE can "quarantine" a user "essentially" by "mov[ing] an endpoint ***from its default VLAN*** to a ***specified Quarantine VLAN***." ISE 3.0 Admin Guide at 300. Similarly, ISE can "unquarantined" a user by "returning the endpoint to its original VLAN" and thus "permit[ting] full access to the network for an endpoint." By changing VLANs (from quarantine to original), Cisco ISE "configur[es] the communication port includes associating the communication port with a VLAN."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Adaptive Network Control

Adaptive Network Control (ANC) is a service that runs on the Administration node. This service monitors and controls network access of endpoints. ANC is invoked by the ISE administrator on the admin GUI, and also can be invoked through pxGrid from third-party systems. ANC supports wired and wireless deployments and requires an Advantage License.

You can use ANC to change the authorization state without having to modify the overall authorization policy of the system. ANC allows you to set the authorization state when you quarantine an endpoint. As a result, the established authorization policies where authorization policies are defined to check for ANCPolicy to limit or deny network access. You can unquarantine an endpoint for full network access. You can also shut down the port on the network attached system (NAS) that disconnects the endpoint from the network.

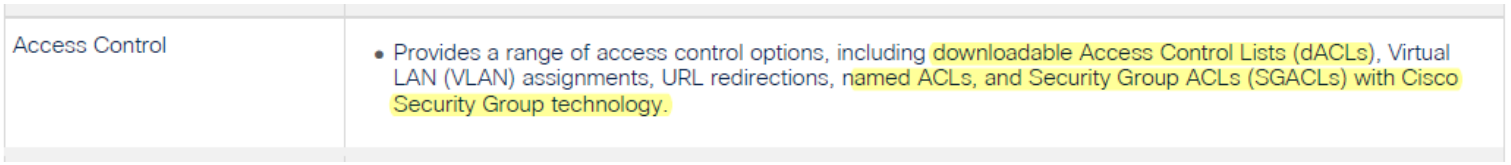
There are no limits to the number of users that can be quarantined at one time. Also, there are no time constraints on the quarantine period length.

You can perform the following operations to monitor and control network access through ANC:

- Quarantine: Allows you to use Exception policies (authorization policies) to limit or deny an endpoint access to the network. You must create Exception policies to assign different authorization profiles (permissions) depending on the ANCPolicy. Setting to the Quarantine state essentially moves an endpoint from its default VLAN to a specified Quarantine VLAN. You must define the Quarantine VLAN previously that is supported on the same NAS as the endpoint.
- Unquarantine: Allows you to reverse the quarantine status that permits full access to the network for an endpoint. This happens by returning the endpoint to its original VLAN.
- Shutdown: Allows you to deactivate a port on the NAS and disconnect the endpoint from the network. Once the port is shut down on the NAS to which an endpoint is connected, manually reset the port on the NAS again. This allows an endpoint to connect to the network, which is not available for wireless deployments.

Thus, Cisco ISE performs "[t]he method of claim 57, wherein configuring the communication port includes associating the communication port with a VLAN[,]" and induces others to do so.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

59. The method of claim 57, wherein the communication port is limited to communicating with the restricted subset of the protected network by an access control list, when the first communication is received.	Thus, Cisco ISE performs "[t]he method of claim 57, wherein the communication port is limited to communicating with the restricted subset of the protected network by an access control list, when the first communication is received." Cisco describes in its ISE Data Sheet "a range of access control options" for this step, "including ***downloadable Access Control Lists (dACLs)***, Virtual LAN (VLAN) assignments, URL redirections, ***named ACLs, and Security Group ACLs (SGACLs)*** with Cisco Security Group technology[.]"  ISE Data Sheet at 5; *see also* ISE 3.0 Admin Guide at 2 ("Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, ***access control lists***, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation."); *id.* at 867-68 ("Static ACLs reside on and are directly configured from the switch. . . . downloadable ACLs (DACLs) can be configured, managed and applied in your authorization policies from the ISE GUI.")
61. The method of claim 59, wherein the communication port is coupled with a network switch.	Cisco ISE performs "[t]he method of claim 59, wherein the communication port is coupled with a network switch[,]" and induces others to do so. As disclosed above with respect to claim 18, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a network switch." Cisco further discloses that its switches can be configured to run an IPv4-based Access Control List. Cisco, Configure IPv4-based Access Control List (ACL) and Access Control Entry (ACE) on a Switch,

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-350-series-managed-switches/smb3025-configure-ipv4-based-access-control-list-acl-and-access-cont.pdf (last visited September 27, 2023).

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Configure IPv4-based Access Control List (ACL) and Access Control Entry (ACE) on a Switch

Objective

An Access Control List (ACL) is a list of network traffic filters and correlated actions used to improve security. It blocks or allows users to access specific resources. An ACL contains the hosts that are permitted or denied access to the network device.

The IPv4-based ACL is a list of source IPv4 addresses that use Layer 3 information to permit or deny access to traffic. IPv4 ACLs restrict IP-related traffic based on the configured IP filters. A filter contains the rules to match an IP packet, and if the packet matches, the rule also stipulates if the packet should be permitted or denied.

An Access Control Entry (ACE) contains the actual access rule criteria. Once the ACE is created, it is applied to an ACL.

You should use access lists to provide a basic level of security for accessing your network. If you do not configure access lists on your network devices, all packets passing through the switch or router could be allowed onto all parts of your network.

This article provides instructions on how to configure IPv4-based ACL and ACE on your managed switch.

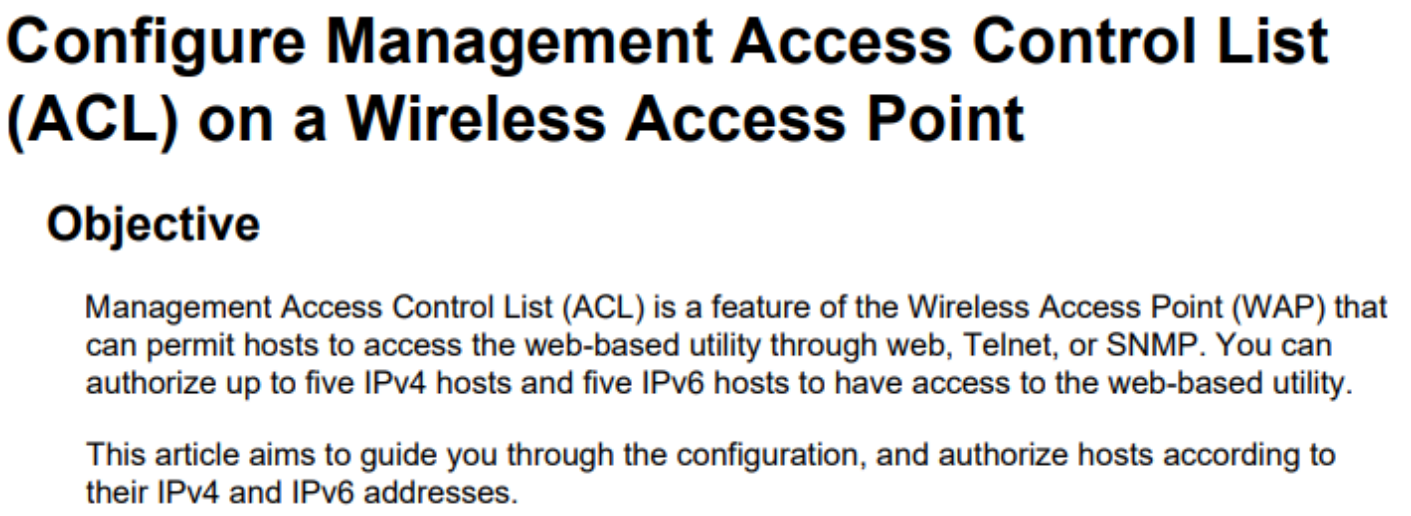
Applicable Devices

- Sx350 Series
- SG350X Series
- Sx500 Series
- Sx550X Series

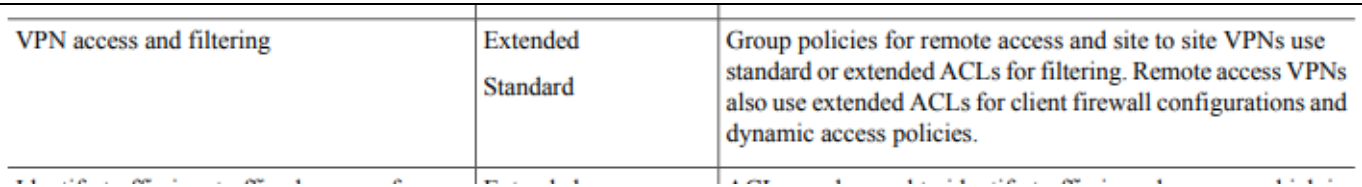
U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	Thus, Cisco ISE performs "[t]he method of claim 59, wherein the communication port is coupled with a network switch[,]" and induces others to do so.
62. The method of claim 59, wherein the communication port is coupled with a wireless access point.	Cisco ISE performs "[t]he method of claim 59, wherein the communication port is coupled with a wireless access point [,]" and induces others to do so. As disclosed above with respect to claim 16, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a wireless access point." (Furthermore, as disclosed above with respect to claim 17, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a wireless access point configured to support an 802.1x standard.") Cisco further discloses that its wireless access points can be configured to run a ***Management ACL***. Cisco, Configure Management Access Control List (ACL) on a Wireless Access Point, https://www.cisco.com/c/en/us/support/docs/smb/wireless/cisco-small-business-100-series-wireless-access-points/smb5282-configure-management-access-control-list-acl-on-a-wireless-a.pdf (last visited September 27, 2023).

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	 Thus, Cisco ISE performs "[t]he method of claim 59, wherein the communication port is coupled with a wireless access point[,]" and induces others to do so.
63. The method of claim 59, wherein the communication port is coupled with a remote access virtual private network.	Cisco ISE performs "[t]he method of claim 59, wherein the communication port is coupled with a remote access virtual private network[,]"and induces others to do so. As disclosed above with respect to claim 25, Cisco's ISE comprises "[t]he network gatekeeper of claim 1, wherein the communication device includes a remote access virtual private network." Cisco further discloses (in its guide for its ASA series firewalls) that "Remote access VPNs also use extended ACLs for client firewall configurations and dynamic access points."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	 Cisco, ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide, 7.10, at 38, https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/asdm710/firewall/asdm-710-firewall-config.pdf; *see generally id.* at 59-74 (chapter 4 on access control lists); *and* 2 ("To implement identity control, do any combination of the following: . . . Install Cisco Identity Services Engine (ISE) on a separate server to implement Cisco Trustsec.") Thus, Cisco ISE performs "[t]he method of claim 59, wherein the communication port is coupled with a remote access virtual private network[,]"and induces others to do so.
65. The method of claim 57, further including authenticating a user of the access device.	Cisco ISE performs "[t]he method of claim 57, further including authenticating a user of the access device[,]" and induces others to do so. As disclosed above with respect to claim 53, Cisco ISE performs "[t]he method of claim 41, further including authenticating a user of the access device." By virtue of that same evidence, Cisco ISE performs "[t]he method of claim 57, further including authenticating a user of the access device[,]" and induces others to do so.
66. The method of claim 65, further including obtaining system data from the access	Cisco ISE performs "[t]he method of claim 65, further including obtaining system data from the access device, and wherein applying the security policy includes using the system data to determine if the access device satisfies the requirements of the security policy[,]"and induces others to do so. As disclosed above with respect to claim 43, Cisco ISE performs "[t]he method of claim 41, further including communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine if the access

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

device, and wherein applying the security policy includes using the system data to determine if the access device satisfies the requirements of the security policy.	device satisfies the requirements of the security policy[,]"and induces others to do so. By virtue of that same evidence, Cisco ISE performs "[t]he method of claim 65, further including obtaining system data from the access device, and wherein applying the security policy includes using the system data to determine if the access device satisfies the requirements of the security policy[,]"and induces others to do so.
68. The method of claim 57, further including communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein	Cisco ISE performs "[t]he method of claim 57, further including communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine if the access device satisfies the requirements of the security policy[,]" and induces others to do so. As disclosed above with respect to claim 43, Cisco ISE performs "[t]he method of claim 41, further including communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine if the access device satisfies the requirements of the security policy[,]"and induces others to do so. By virtue of that same evidence, Cisco's ISE performs "[t]he method of claim 57, further including communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine if the access device satisfies the requirements of the security policy[,]" and induces others to do so.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

applying the security policy includes using the system data to determine if the access device satisfies the requirements of the security policy.	
71. The method of claim 57, further including communicating between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication	Cisco's ISE performs "[t]he method of claim 57, further including communicating between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port for communicating between the access device and the less-restricted subset[,]" and induces others to do so. Cisco states that after an endpoint (the claimed "access device") is granted access to network resources ("after reconfiguring the communication port for communicating between the access device and the less-restricted subset"), ISE can use ***Continuous Endpoint Attribute Monitoring***. ISE 3.0 Admin Guide at 1002-03. With ***Continuous Endpoint Attribute Monitoring***, ISE uses the AnyConnect agent (the claimed "agent executing on the access device") to monitor the endpoint after initial posture ("after reconfiguring . . ."). Cisco further states, "After initial posture, the AnyConnect agent scans the applications every X minute and sends the differences from the last scan to the server." Thus, by sending differences from the last scan to the server, ISE "communicat[es] between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port for communicating between the access device and the less-restricted subset[." Thus, Cisco's ISE performs this method and induces others to do so.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

port for communicating between the access device and the less-restricted subset.	**Continuous Endpoint Attribute Monitoring** You can use the AnyConnect agent to continuously monitor different endpoint attributes to ensure that dynamic changes are observed during posture assessment. This improves the overall visibility of an endpoint and helps Compliance Cisco Web Agent you create posture policies based on their behavior. The AnyConnect agent monitors applications that are installed and running on an endpoint. You can turn on and off the feature and configure how often the data should be monitored. By default, data is collected every 5 minutes and is stored in the database. During initial posture, AnyConnect reports a complete list of running and installed applications. After initial posture, the AnyConnect agent scans the applications every X minute and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications. ISE 3.0 Admin Guide at 1102-03.

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

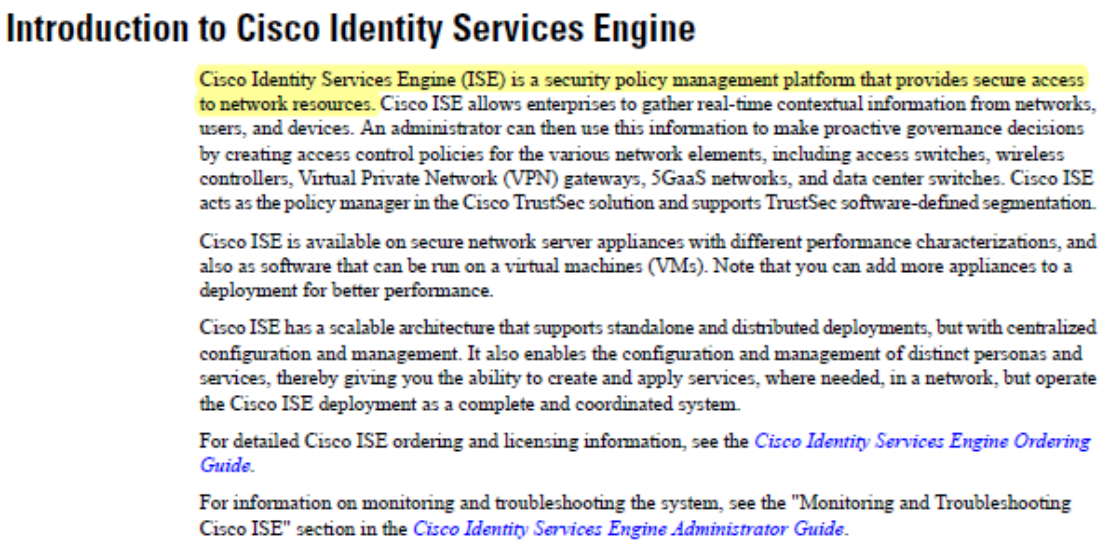
Claim 82

[82-preamble] A computer readable medium including computer code configured for controlling access to a computer network, the computer code comprising:	Cisco infringes this claim by making, using, testing, offering for sale, and selling the ISE product and system and through performance of each of the claimed steps and/or providing instructions and data from its servers to third-parties to perform at least one of the claimed steps, or induces others to do so as set forth in claim element 1-c. Further, subsequent to Cisco's making, using, testing, offering for sale, and selling of the ISE, Cisco offers services to third-parties and customers with respect to the ISE. For example, these can include "Technical Services," "Advisory Services," and "Cisco Talos Incidence Response" services. (https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/ise-licensing-guide-og.html). For technical services, for example, Cisco encourages customers to purchase "Cisco Smart Net Total Care" for Cisco ISE physical appliances and Software Support (SWSS) contracts for Cisco ISE virtual machines. For advisory services, Cisco offers Expert Services to address "your business objectives with the technology we offer" (including ISE). *Id*. And for the Talos Incident Response, Cisco provides a full suite of proactive and emergency services to help third-parties prepare, respond, and recover from a cybersecurity breach. Cisco explains that third-parties can "order and transact Cisco Talos Incident Response when ordering Cisco ISE subscriptions." *Id*. Additionally, and as set forth in InfoExpress's 3-1 disclosures, Cisco's ISE also includes Cisco's ISE (NAC) appliance. Specifically, these are Cisco-provided tangible hardware and "virtual appliances" on which ISE can be deployed. A list of accused ISE (NAC) Appliances (also referred to as "hardware platforms") which ISE supports, are disclosed in InfoExpress's Disclosure of Asserted Claims and Infringement Contentions per Patent L.R. 3-1 and 3-2 at Section II.B.2. These ISE (NAC) Appliances are listed in Cisco's Identity Services Engine Administrator Guides, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0001603 to 0014308, and also their Release Notes for ISE Releases 1.04, 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014606 to 0015185. Cisco's ISE (NAC) appliances are directed to "[g]ranting and denying network access" and using "attributes related to users and their devices" in "determining authorized network access." https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/datasheet-c78-

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

726524.html. Cisco further explains that its NAC appliance (known in one example as "The Cisco Secure Network Server") "supports Cisco's powerful network access and control security applications." *Id*. Further, Cisco explains that the "Cisco Secure Network Server… is configured specifically to support the Cisco Identity Services Engine (ISE) security application." *Id*.

To the extent the preamble is limiting, Cisco's ISE is "a security policy management platform that provides secure access to network resources" and thereby grants access to a protected network.



Introduction to Cisco Identity Services Engine

Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, wireless controllers, Virtual Private Network (VPN) gateways, 5GaaS networks, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation.

Cisco ISE is available on secure network server appliances with different performance characterizations, and also as software that can be run on a virtual machines (VMs). Note that you can add more appliances to a deployment for better performance.

Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also enables the configuration and management of distinct personas and services, thereby giving you the ability to create and apply services, where needed, in a network, but operate the Cisco ISE deployment as a complete and coordinated system.

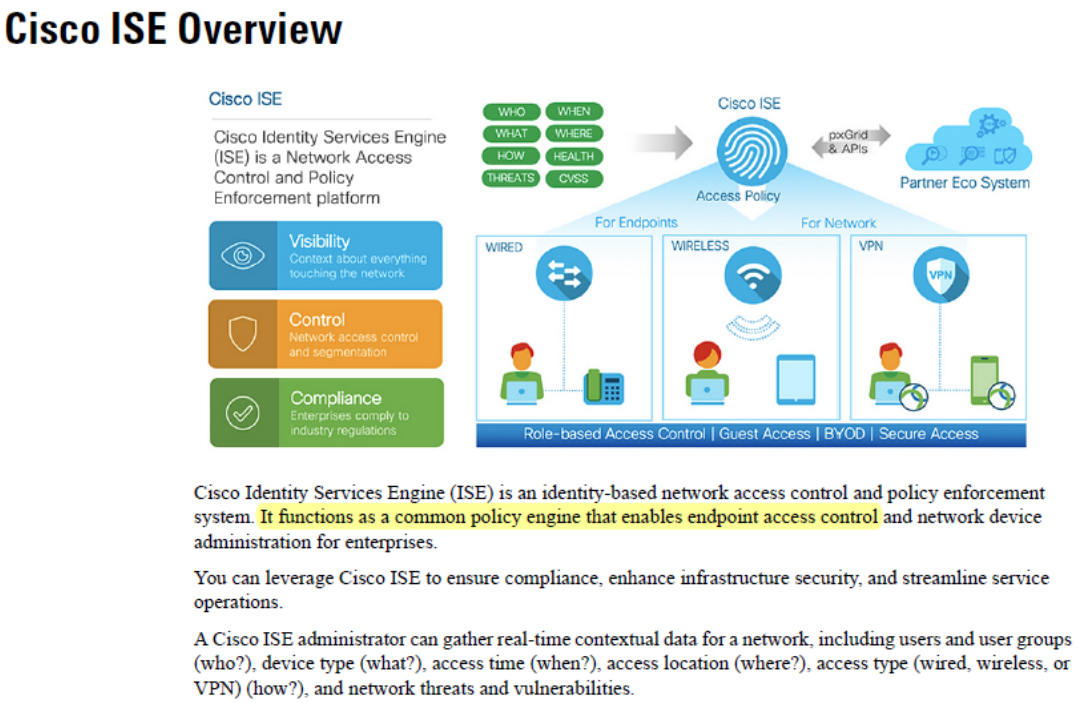
For detailed Cisco ISE ordering and licensing information, see the *Cisco Identity Services Engine Ordering Guide*.

For information on monitoring and troubleshooting the system, see the "Monitoring and Troubleshooting Cisco ISE" section in the *Cisco Identity Services Engine Administrator Guide*.

Release Notes for Cisco Identity Services Engine, Release 3.0 ("ISE 3.0 Release Notes") at 1, *available at* https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/release_notes/b_ise_30_rn.html (last accessed June 26, 2023).

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

Cisco further describes ISE as a "Network Access Control and Policy Enforcement platform" which thereby grants access to a protected network.



Source: Cisco, Identity Services Engine Administrator Guide, Release 3.0 ("ISE 3.0 Admin Guide"), at 1, *available at* https://www.cisco.com/c/en/us/td/docs/security/ise/30/admin_guide /b_ISE_admin_3_0.pdf (last visited May 31, 2023).

Cisco further describes its ISE as permitting different "network permissions on the authorization policy levels[,]" which is thereby a "method of granting access to a protected network."

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

	Policy Sets Cisco ISE is a policy-based, network-access-control solution, which offers network access policy sets, allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type, and similar parameters. When you install Cisco ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules. When creating policy sets, you can configure these rules (configured with conditions and results) in order to choose the network access services on the policy set level, the identity sources on the authentication policy level, and network permissions on the authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE-supported dictionaries for different vendors. Cisco ISE allows you to create conditions as individual resuable policy elements. The network access service to be used per policy set to communicate with the network devices is defined at the top level of that policy set. Network access services include: • Allowed protocols—the protocols configured to handle the initial request and protocol negotiation. • A proxy service—sends requests to an external RADIUS server for processing. *Id.* at 856; *see also id.* at 546 ("A user role is a set of permissions that determine what tasks a user can perform and what services they can access on the Cisco ISE network. . . . .Cisco ISE allows you to restrict network access based on user attributes for both network access users and administrators.")
[82-a] a code segment configured for receiving a request for access to a less-restricted	As disclosed above with respect to claim element 27-a, Cisco's ISE— "receiv[es] a request for access to a less-restricted subset of the protected network from an access device, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper[.]" Thus, Cisco's ISE (NAC) Appliances comprise "[a] computer readable medium including computer code configured for controlling access to a computer network, the computer code comprising: a code segment configured for receiving a request for access to a less-restricted subset of the protected network from an access device, the request being

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

subset of the protected network from an access device, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper;	received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper[.]"
[82-b]	As disclosed above with respect to claim element 27-b, Cisco's ISE "apply[ies] a security policy to the access device, responsive to the request [.]" Thus, Cisco's ISE (NAC) Appliances comprise "[a] computer readable medium

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

a code segment configured for applying a security policy to the access device, responsive to the request;	including computer code configured for controlling access to a computer network, the computer code comprising: . . . a code segment configured for applying a security policy to the access device, responsive to the request[.]"
[82-c] a code segment configured for reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements	As disclosed above with respect to claim element 27-c, Cisco's ISE "reconfigure[es] the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements of the security policy are satisfied [.]" Thus, Cisco's ISE (NAC) Appliances comprise "[a] computer readable medium including computer code configured for controlling access to a computer network, the computer code comprising: . . . a code segment configured for reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements of the security policy are satisfied[.]"

U.S. Patent No. 7,523,484 (Cisco Identity Services Engine)

of the security policy are satisfied;	
[82-d] a code segment configured for reading an administrator specified configuration of the communication port from the access point; and	As disclosed above with respect to claim element 27-d, Cisco's ISE "read[s] an administrator specified configuration of the communication port from the access point[.]" Thus, Cisco's ISE (NAC) Appliances comprise "[a] computer readable medium including computer code configured for controlling access to a computer network, the computer code comprising: . . . a code segment configured for reading an administrator specified configuration of the communication port from the access point[.]"
[82-e] a code segment configured for storing the read administrator specified configuration.	As disclosed above with respect to claim element 27-e, Cisco's ISE "stor[es] the read administrator specified configuration[.]" Thus, Cisco's NAC Appliances comprise "[a] computer readable medium including computer code configured for controlling access to a computer network, the computer code comprising: . . . a code segment configured for storing the read administrator specified configuration[.]"

EXHIBIT F-2

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

Claim 1

U.S. Patent No. 8,051,460	**Cisco's Identity Services Engine**
[Claim 1—preamble] A method of granting access to a protected network, the method comprising:	Cisco infringes this claim by making, using, testing, offering for sale, and selling the ISE product and system and through performance of each of the claimed steps and/or providing instructions and data from its servers to third-parties to perform at least one of the claimed steps. Further, subsequent to Cisco's making, using, testing, offering for sale, and selling of the ISE, Cisco offers services to third-parties and customers with respect to the ISE. For example, these can include "Technical Services," "Advisory Services," and "Cisco Talos Incidence Response" services. (https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/ise-licensing-guide-og.html). For technical services, for example, Cisco encourages customers to purchase "Cisco Smart Net Total Care" for Cisco ISE physical appliances and Software Support (SWSS) contracts for Cisco ISE virtual machines. For advisory services, Cisco offers Expert Services to address "your business objectives with the technology we offer" (including ISE). *Id*. And for the Talos Incident Response, Cisco provides a full suite of proactive and emergency services to help third-parties prepare, respond, and recover from a cybersecurity breach. Cisco explains that third-parties can "order and transact Cisco Talos Incident Response when ordering Cisco ISE subscriptions." *Id*. Additionally, and as set forth in InfoExpress's 3-1 disclosures, Cisco's ISE also includes Cisco's ISE (NAC) appliance. Specifically, these are Cisco-provided tangible hardware and "virtual appliances" on which ISE can be deployed. A list of accused ISE (NAC) Appliances (also referred to as "hardware platforms") which ISE supports, are disclosed in InfoExpress's Disclosure of Asserted Claims and Infringement Contentions per Patent L.R. 3-1 and 3-2 at Section II.B.2. These ISE (NAC) Appliances are listed in Cisco's Identity Services Engine

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	Administrator Guides, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0001603 to 0014308, and also their Release Notes for ISE Releases 1.04, 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014606 to 0015185. Cisco's ISE (NAC) appliances are directed to "[g]ranting and denying network access" and using "attributes related to users and their devices" in "determining authorized network access." .[1] Cisco further explains that its NAC appliance (known in one example as "The Cisco Secure Network Server") "supports Cisco's powerful network access and control security applications." *Id*. Further, Cisco explains that the "Cisco Secure Network Server… is configured specifically to support the Cisco Identity Services Engine (ISE) security application." *Id*.

[1] Certain portions of the evidence cited herein identify and relate to the "Cisco Secure Network Server Data Sheet" for Cisco SNS-3715, SNS-3755, and SNS-3795 Secure Network Server. We understand that each other version of the Accused Technology relating to the Cisco ISE (NAC) appliances including ISE-3315-K9, ISE-3355-K9, and ISE-3395-K9; SNS-3415-K9 and SNS-3495-K9; SNS -3515-K9 and SNS-3595-K9; SNS-3615-K9, SNS-3655-K9, and SNS-3695-K9; and ISE Virtual Machine (S/M/L)-K9 are operationally and functionally the same with respect to and for the purposes of identifying infringement for each of the Asserted Claims.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

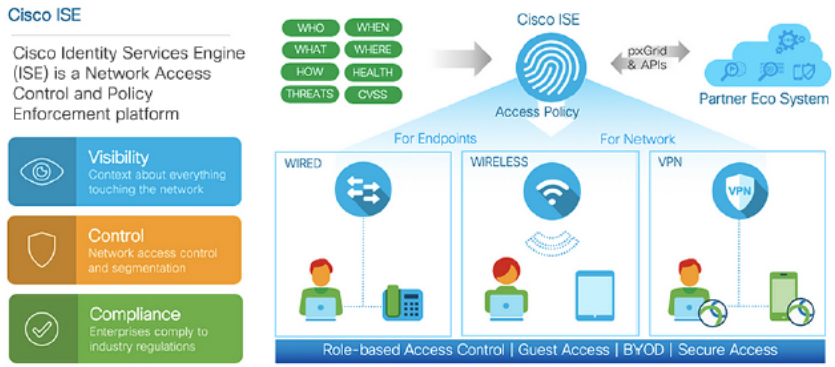
	To the extent the preamble is limiting, Cisco's Identity Services Engine ("ISE")[2] is "a security policy management platform that provides secure access to network resources" and thereby grants access to a protected network. **Introduction to Cisco Identity Services Engine** Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, wireless controllers, Virtual Private Network (VPN) gateways, 5GaaS networks, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation. Cisco ISE is available on secure network server appliances with different performance characterizations, and also as software that can be run on a virtual machines (VMs). Note that you can add more appliances to a deployment for better performance. Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also enables the configuration and management of distinct personas and services, thereby giving you the ability to create and apply services, where needed, in a network, but operate the Cisco ISE deployment as a complete and coordinated system. For detailed Cisco ISE ordering and licensing information, see the *Cisco Identity Services Engine Ordering Guide*. For information on monitoring and troubleshooting the system, see the "Monitoring and Troubleshooting Cisco ISE" section in the *Cisco Identity Services Engine Administrator Guide*. Release Notes for Cisco Identity Services Engine, Release 3.0 ("ISE 3.0 Release Notes") at 1, *available at* https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/release_notes/b_ise_30_rn.html (last accessed June 26, 2023).

[2] Certain portions of the evidence cited herein identify and relate to the Cisco Identity Services Engine, Release version 3.0. We understand that each version of the Accused Technology is operationally and functionally the same with respect to and for the purposes of identifying infringement for each of the Asserted Claims.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

Cisco further describes ISE as a "Network Access Control and Policy Enforcement platform" which thereby grants access to a protected network.

Cisco ISE Overview



Cisco Identity Services Engine (ISE) is an identity-based network access control and policy enforcement system. It functions as a common policy engine that enables endpoint access control and network device administration for enterprises.

You can leverage Cisco ISE to ensure compliance, enhance infrastructure security, and streamline service operations.

A Cisco ISE administrator can gather real-time contextual data for a network, including users and user groups (who?), device type (what?), access time (when?), access location (where?), access type (wired, wireless, or VPN) (how?), and network threats and vulnerabilities.

Source: Cisco, Identity Services Engine Administrator Guide, Release 3.0 ("ISE 3.0 Admin Guide"), at 1, *available at* https://www.cisco.com/c/en/us/td/docs/security/ise/30/admin_guide/b_ISE_admin_3_0.pdf (last visited May 31, 2023).

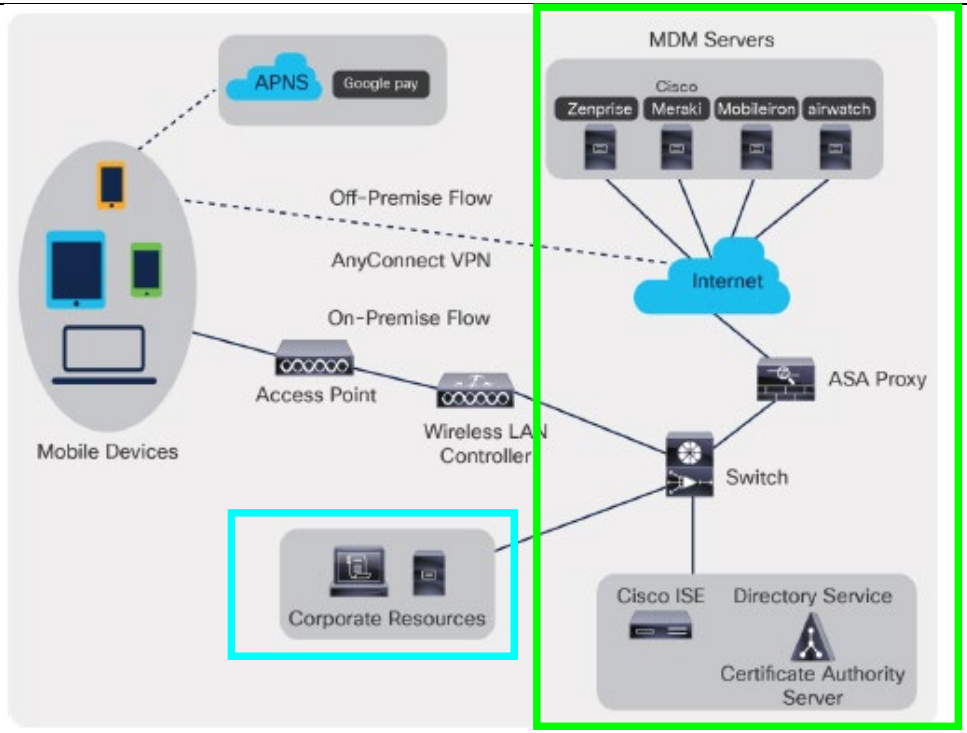
U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	Cisco further describes its ISE as permitting different "network permissions on the authorization policy levels[,]" which is thereby a "method of granting access to a protected network." **Policy Sets** Cisco ISE is a policy-based, network-access-control solution, which offers network access policy sets, allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type, and similar parameters. When you install Cisco ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules. When creating policy sets, you can configure these rules (configured with conditions and results) in order to choose the network access services on the policy set level, the identity sources on the authentication policy level, and network permissions on the authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE-supported dictionaries for different vendors. Cisco ISE allows you to create conditions as individual resuable policy elements. The network access service to be used per policy set to communicate with the network devices is defined at the top level of that policy set. Network access services include: • Allowed protocols—the protocols configured to handle the initial request and protocol negotiation. • A proxy service—sends requests to an external RADIUS server for processing. *Id.* at 856; *see also id.* at 546 ("A user role is a set of permissions that determine what tasks a user can perform and what services they can access on the Cisco ISE network. . . . .Cisco ISE allows you to restrict network access based on user attributes for both network access users and administrators.")

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

[1—a] receiving a request for access to a less-restricted subset of the protected network from an access device, the request received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper;	Cisco ISE "receiv[es] a request for access to a less-restricted subset of the protected network from an access device, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper" or induces others to do so. In this step, the Cisco ISE receives a request for a less restricted subset of the protected network (blue) from a user access device—for example, a mobile phone, tablet, or laptop computer (e.g. Mobile Devices).

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)



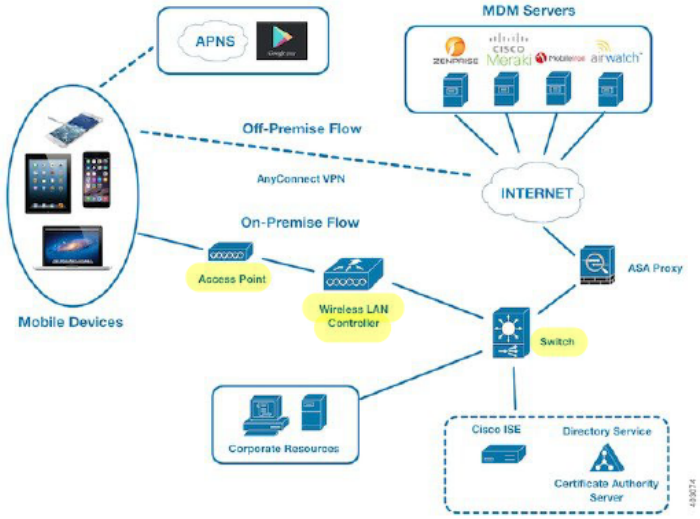
Cisco, Randomized and Changing MAC Deployment Guide (2022) at 43, https://www.cisco.cowm/c/en/us/products/collateral/wireless/randomized-changing-mac-dg.pdf (last visited June 27, 2023).

Cisco also describes in its ISE 3.0 Admin Guide how Mobile Device Management (MDM) servers "secure, monitor, manage, and support mobile devices that are deployed across mobile operators, service providers, and enterprises. Traditionally, MDM servers have only supported

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	mobile devices. Some MDM servers now manage ***all types of devices in a network (mobile phones, tablets, laptops, and desktops)***[.]" **Mobile Device Manager Interoperability with Cisco ISE** Mobile Device Management (MDM) servers secure, monitor, manage, and support mobile devices that are deployed across mobile operators, service providers, and enterprises. Traditionally, MDM servers have only supported mobile devices. Some MDM servers now manage all types of devices in a network (mobile phones, tablets, laptops, and desktops) and are called Unified Endpoint Management (UEM) servers. MDM servers act as a policy server that controls the use of some applications on a mobile device (for example, an email application) in the deployed environment. Cisco ISE queries a connected MDM server for information about various attributes that you can use to create network authorization policies. You can run multiple active MDM servers on your network, from different vendors. This allows you to route different endpoints to different MDM servers based on device factors such as location or device type. Cisco ISE also integrates with MDM servers using the Cisco MDM Server Info APIs, Version 2 and later versions, to allow devices to access the network over VPN via Cisco AnyConnect 4.1 and Cisco Adaptive Security Appliances 9.3.2 or later. In the following illustration, Cisco ISE is the enforcement point and the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution. ISE 3.0 Admin Guide at 830. Cisco describes how the "access devices" that send "request[s] for access" are termed "endpoints" in Cisco's language. And endpoint is "typically a network-capable device that connect[s] to your network through wired and wireless network access devices and VPN. Endpoints can be personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, and so on." ISE 3.0 Admin Guide at 730; *see also id.* at 101 ("Here, an endpoint could mean users, PCs, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, or other types of network devices."); 765 ("For example, a user registers a laptop with wired and wireless addresses.").

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	Cisco further describes how the "request [for access] [is] received through a communication port of an access point[.]" Cisco's "access points" include its "switches, access routers, wireless access points, and other network access points." ISE 3.0 Admin Guide at 830. ***Figure 33: MDM Interoperability with Cisco ISE***  Configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. Cisco ISE applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network. *See also* Randomized and Changing MAC Deployment Guide at 43 (same); *see also* ISE 3.0 Admin Guide at 363 ("The device administrator is the user who logs into the network devices

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	such as ***switches, wireless access points, routers, and gateways***, (normally through SSH), to perform the configuration and maintenance of the administered devices."). Cisco makes, uses, sells, and offers for sale a variety of ISE-validated products which customers oftentimes require with its ISE solutions including wireless access points, switches, LAN controllers, routers, servers, and remote access devices. A list of "access points" that are compatible with its ISE—including switches, routers, and remote access devices (i.e. firewalls)—is listed in Cisco's Identity Services Engine Network Component Compatibility documents, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014309 to INFOEX-CSCO_0014605. These Cisco documents describe "Cisco Identity Services Engine (ISE) validated compatibility with switches, wireless LAN controllers, and other policy enforcement devices as well as operating systems with which Cisco ISE interoperates." INFOEX-CSCO_0014586 at 14586. They further state, with respect to "Validated Network Access Devices," that "Cisco ISE supports interoperability with any Cisco or non-Cisco RADIUS client network access device (NAD) that implements common RADIUS behavior (similar to Cisco IOS 12.x) for standards-based authentication." INFOEX-CSCO_0014586 at 14587. These Cisco documents identify the claimed "access points" including both Cisco-made and third-party access points. Cisco also describes ISE-compatible third-party devices in its ISE 3.0 Admin Guide at 806-07, including those made by Aruba, Motorola, HP, Ruckus, Alcatel, Brocade, and Juniper. *See also* ISE 3.0 Admin Guide at 430 ("The [Wireless LAN Controller ("WLC")] can now log the guest in via the Cisco ISE RADIUS server. When this is complete, the WLC redirects the guest device's browser to the original URL destination. The Wireless LAN Controller (WLC) and the network access devices (NAD) requirements to support the original URL redirect for guest portals are WLC 5760 and ***Cisco Catalyst 3850, 3650, 2000, 3000, and 4000 Series Access***

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

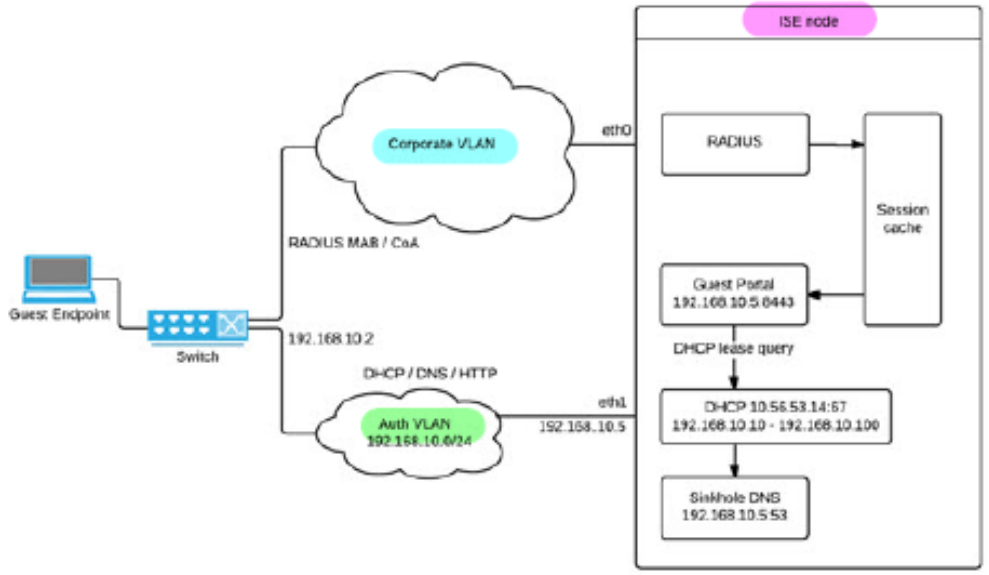
	Switches running releases IOS-XE 3.6.0.E and 15.2(2)E."); 874 (Cisco AI Endpoint Analytics receives endpoint attribute data from multiple sources, such as ***Cisco Catalyst 9000 Series devices***[.]"); 697 ("The following devices support sending [Manufacturer Usage Descriptor ("MUD")] data to Cisco ISE: Cisco Catalyst 3850 Series Switches running Cisco IOS XE Version 16.9.1 & 16.9.2[,] Cisco Catalyst Digital Building Series Switches running Cisco IOS Version 15.2(6)E2[, and] Cisco Industrial Ethernet 4000 Series Switches running Cisco IOS Version 15.2(6)E2[.]"); 788 ("Cisco TrustSec-enabled devices use the TrustSec attributes to communicate with Cisco ISE. Cisco TrustSec-enabled devices, such as the Cisco Nexus 7000 Series Switches, Cisco Catalyst 6000 Series Switches, Cisco Catalyst 4000 Series Switches, and Cisco Catalyst 3000 Series Switches are authenticated using the Cisco TrustSec attributes that you define while adding Cisco TrustSec devices.").

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	Cisco describes in its ISE 3.0 Admin Guide an example where the request for access is received through a Cisco or third-party (that is, a non-Cisco) access point (termed a "network access device") in Cisco's literature. ISE 3.0 Admin Guide at 803-06. **Third-Party Network Device Support in Cisco ISE** Cisco ISE supports third-party network access devices (NADs) by using network device profiles. A NAD profile defines the capabilities of a third-party device with a simplified policy configuration, regardless of the vendor-side implementation. A network device profile contains the following: • The protocols that the network device supports, such as RADIUS, TACACS+, and Cisco TrustSec. You can import into Cisco ISE any vendor-specific RADIUS dictionaries that exist for the network device. • The attributes and values that the device uses for various authentication flows such as Wired MAB and 802.1X. These attributes and values allow Cisco ISE to detect the right authentication flow for your device according to the attributes that the network device uses. • The Change of Authorization (CoA) capabilities of the network device. While the RADIUS protocol RFC 5176 defines a CoA request, the attributes used in a CoA request vary depending on the network device. Most non-Cisco devices with RFC 5176 support the *Push* and *Disconnect* functions. For devices that do not support the RADIUS CoA type, Cisco ISE also supports SNMP CoA. • The attributes and protocols that the network device uses for MAB flows. Network devices from different vendors perform MAB authentication differently. • The VLAN and ACL permissions that are used by the device. When you save the profile, Cisco ISE automatically generates authorization profiles for each configured permission.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

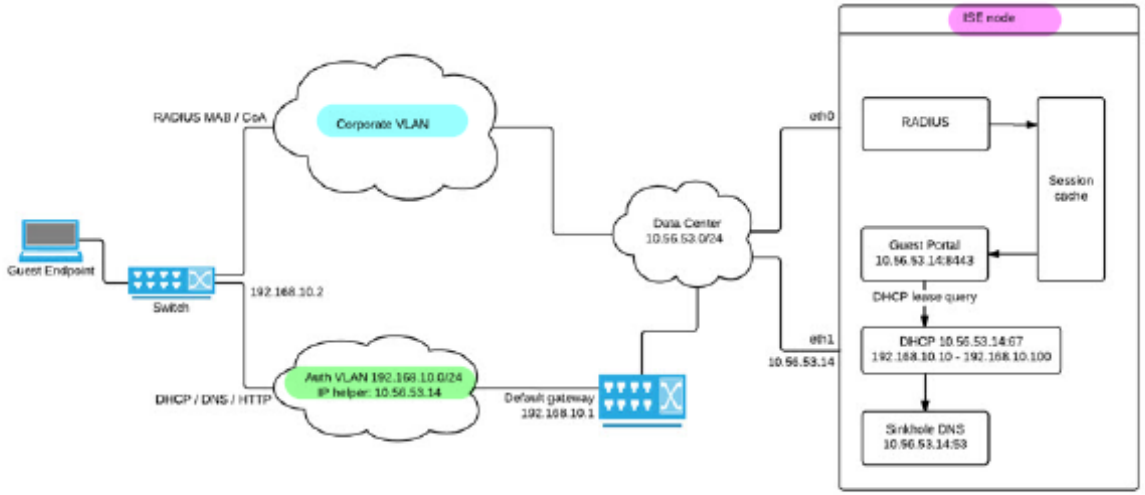
Figure 31: Auth VLAN Connected to Cisco ISE Node



The following diagram displays a network with Auth VLAN and an IP helper.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

Figure 32: Auth VLAN Configured with IP Helper



U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

Furthermore, in ISE, the "request [for access is] received through a ***communication port*** of an access point."

Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.
Endpoint Profile	Shows the type of endpoint that is profiled, for example, profiled to be an iPhone, Android, M Xbox, and so on.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
Authorization Profiles	Shows the authorization profile that was used for authentication.
IP Address	Shows the IP address of the endpoint device.
Network Device	Shows the IP address of the Network Access Device.
Device Port	Shows the port number at which the endpoint is connected.
Identity Group	Shows the identity group that is assigned to the user or endpoint, for which the log was genera
Posture Status	Shows the status of posture validation and details on the authentication.
Server	Indicates the policy service from which the log was generated.

ISE 3.0 Admin Guide at 354; *see also id.* at 359 (similar disclosure with respect to TACACS live logs); 377 (similar); 882 ("You can create the following unique network conditions to restrict access to the network: . . . ***Device Port*** Network Conditions—Based on the device's IP address, name, NDG, and ***port (physical port of the device*** that the endstation is connected to)."); 900 ("Configure Device Port Network Condition"); 1188-89 ("enable ***switch ports*** for 802.1X and MAB"); 1230 (with respect to RADIUS live logs, the "***Device Port***" field "[s]hows the port number at which the endpoint is connected"); 1231 (with respect to TACACS live logs, the "Device Port" field "[s]hows the device port number through which the access request is made"); 1236.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	Furthermore, in Cisco's ISE the "communication port [is] configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper[.]" As shown in the schematic below, the access device (e.g., Mobile Devices) is in communication with the restricted subset of the protected network (green), which includes a gatekeeper (e.g., Cisco's ISE) (purple).

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

In the following illustration, Cisco ISE is the enforcement point and the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution.

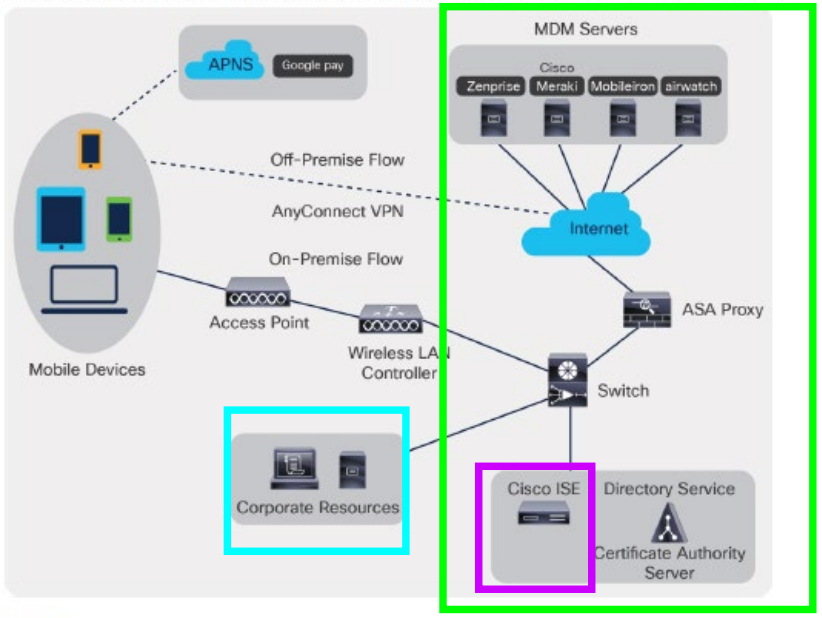


Figure 5.
Cisco ISE and MDM servers

Randomized and Changing MAC Deployment Guide at 43. Cisco further explains that with respect to mobile device management (MDM) server integration with ISE, "ISE is the enforcement point . . . [that] then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points."

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

Figure 5.
Cisco ISE and MDM servers

You can configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. It then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network.

Cisco further explains, with respect to MDM server integration with ISE, that access devices (termed "unregistered endpoints") "are redirected to a registration page that is hosted on the MDM server," and further that endpoints in remediation "are granted restricted access"—that is, they are "communicating [with] a restricted subset of the protected network, the restricted subset including a gatekeeper."

Supported MDM use cases

Cisco ISE performs the following functions with the external MDM server:

- Manages device registration: Unregistered endpoints that access the network are redirected to a registration page that is hosted on the MDM server. Device registration includes the user role, device type, and so on.
- Handles device remediation: Endpoints are granted restricted access during remediation.

Cisco describes this process flow elsewhere in the same document:

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	MDM integration process flow **Step 1.** The user associates a device with an SSID. **Step 2.** Cisco ISE makes an API call to the MDM server. **Step 3.** This API call returns a list of devices for the user and the posture statuses for the devices. **Note:** The input parameter is the MAC address of the endpoint device. For off-premises Apple iOS devices (any device that connects to Cisco ISE through a VPN), the input parameter is the UDID. **Step 4.** If the user's device is not on this list, it means that the device is not registered. Cisco ISE sends an authorization request to the Network Access Device (NAD) to redirect to Cisco ISE. The user is presented with the MDM server page. **Note:** You must register a device that is enrolled on the MDM server outside of a Cisco ISE network via the MDM portal. This is applicable for Cisco ISE Release 1.4 and later. Earlier Cisco ISE versions allow devices that are enrolled outside the Cisco ISE-enabled network to be automatically enrolled if they are compliant with the posture policies. **Step 5.** Cisco ISE uses MDM to provision the device and presents the appropriate window for the user to register the device. **Step 6.** The user registers the device in the MDM server, and the MDM server redirects the request to Cisco ISE through automatic redirection or manual browser refresh. **Step 7.** Cisco ISE queries the MDM server again for the posture status.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

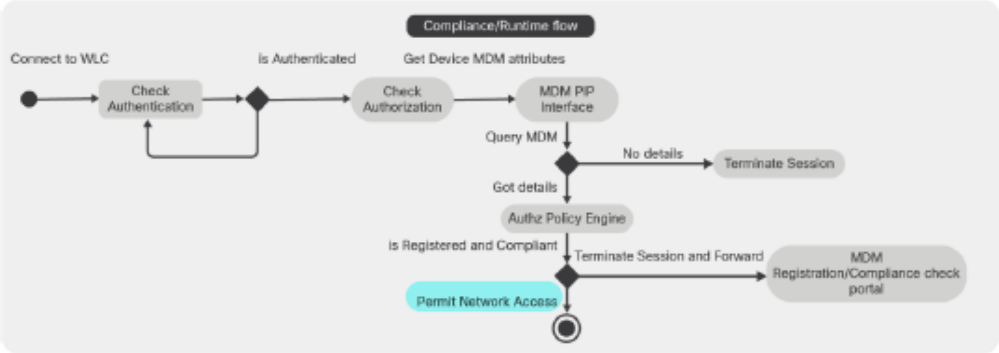
Step 8. If the user's device is not compliant with the posture (compliance) policies that are configured on the MDM server, the user is notified that the device is out of compliance. The user must take the necessary action to ensure that the device is compliant.

Step 9. When the user's device is compliant, the MDM server updates the device's state in its internal tables.

Step 10. If the user refreshes the browser now, the control is transferred back to Cisco ISE.

Step 11. Cisco ISE polls the MDM server once every four hours to get compliance information and issues the appropriate Change of Authorization (CoA). You can configure the polling interval. Cisco ISE also checks the MDM server every five minutes to make sure that it is available.

The following figure illustrates the MDM process flow.



Randomized and Changing MAC Deployment Guide at 46-47.

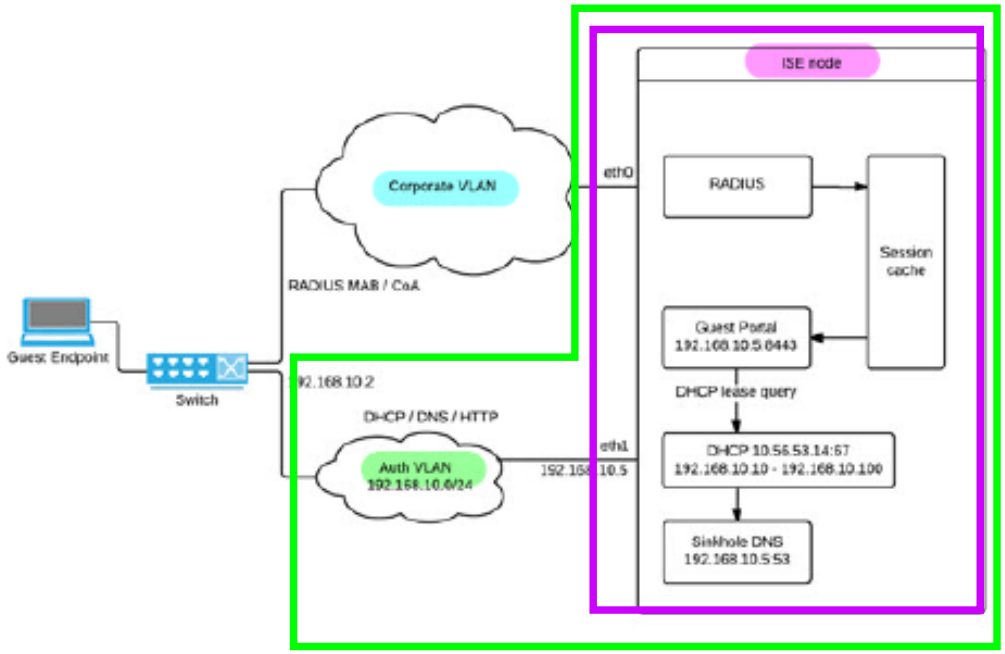
Finally, with respect to MDM servers integrated with ISE, Cisco's ISE has a gatekeeper associated with the restricted subset of the protected network. Cisco further explains how ISE can be the "enforcement point" that "applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points."

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	Cisco ISE also integrates with MDM servers using the Cisco MDM Server Info API, Version 2, to allow devices to access the network over VPN via Cisco AnyConnect 4.1 and Cisco Adaptive Security Appliances 9.3.2 or later. In the following illustration, Cisco ISE is the enforcement point and the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution. You can configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. It then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network. Randomized and Changing MAC Deployment Guide at 43. By way of a specific example, Cisco's ISE also operates in conjunction with its own or third party (i.e. non-Cisco) access points. In this setup, an access device ("guest endpoint") connects to the network through a restricted subset of the protected network (the "Authorization VLAN ('Auth VLAN')[.]" The restricted subset includes the Auth VLAN and further includes a gatekeeper in the form of its ISE node that can assess the endpoint's security posture. Cisco explains how ISE "runs the configured authentication and authorization policy[,] "validates endpoint compliance[,]" and "authorizes the endpoint[.]"

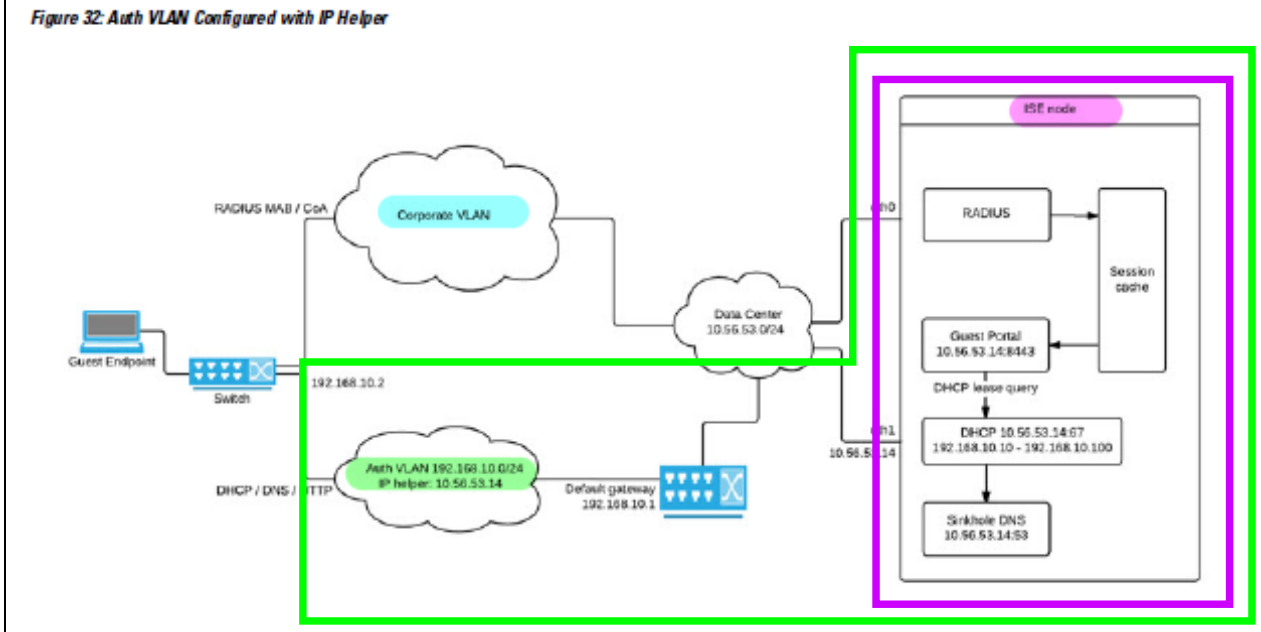
U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

Figure 31: Auth VLAN Connected to Cisco ISE Node



The following diagram displays a network with Auth VLAN and an IP helper.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)



U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

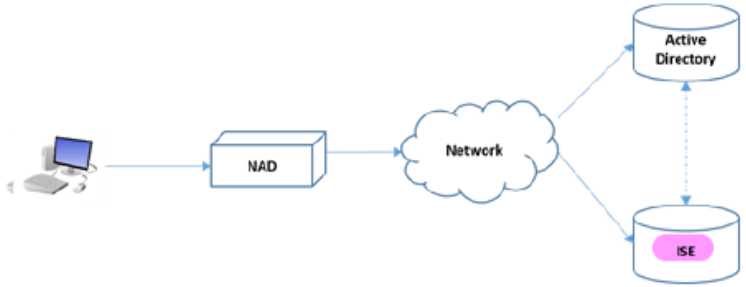
1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

Multiple VLANs may be connected to one network interface card by configuring a VLAN IP helper from the NAD configuration. For more information about configuring an IP helper, see the administration guide for the network device for instructions. For guest access flows that include VLANs with IP helpers, define a guest

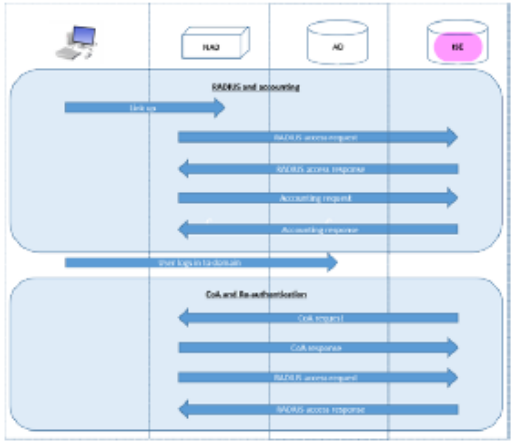
Admin Guide at 804-06.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	By way of another specific example, Cisco's ISE has an ***Easy Connect Mode***, whereby "ISE issues a [Change of Authorization ("CoA")] after the external server (AD) authenticates the user." **Easy Connect Enforcement Mode Process Flow** The Easy Connect Enforcement mode process is as follows: 1. The user connects to the NAD from a wired endpoint (such as a PC for example). 2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD. 3. The user logs in to the domain and a security audit event is sent to Cisco ISE. 4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event. 5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy. ***Figure 20: Easy Connect Enforcement Mode Basic Flow***  ISE Admin Guide at 581.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

Figure 21: Easy Connect Enforcement Mode Detailed Flow



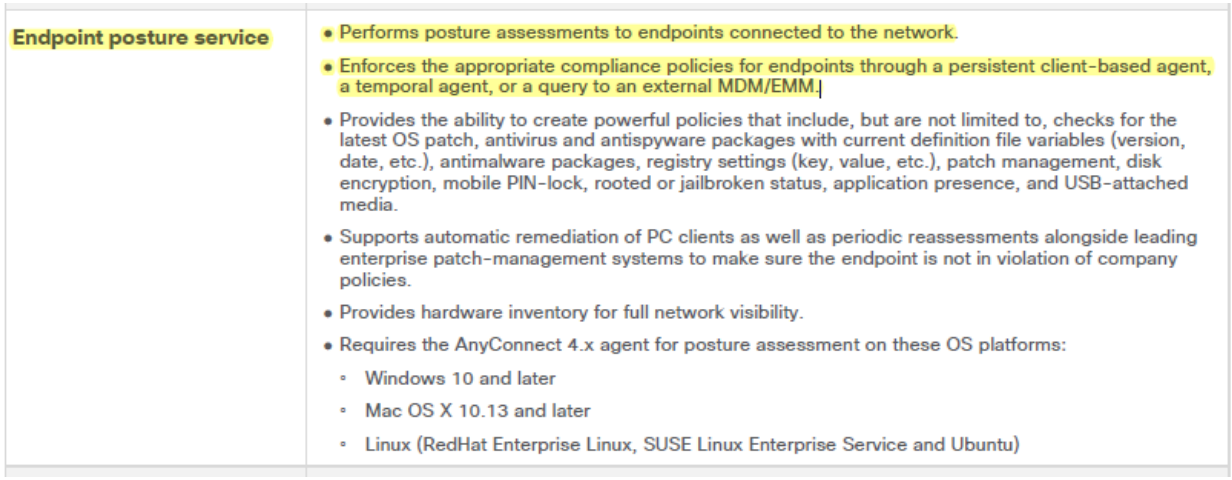
For more information about configuring Enforcement mode, see Configure Easy Connect Enforcement Mode, on page 582.

In Easy Connect Mode, "The user connects to the [network access device ("NAD"), e.g. an access point] from a wired endpoint (such as a PC for example)[,]" and after several steps, "Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and ***the user is provided access by the NAD to the network based on that policy***." Having a step whereby the user is being provided access to the network means, by implication, that the user did not have network access prior to that step. Thus, at that point, the user was restricted from certain network access, and thus "the communication port [was] configured for communicating between the access device and ***a restricted subset*** of the protected network[.]"

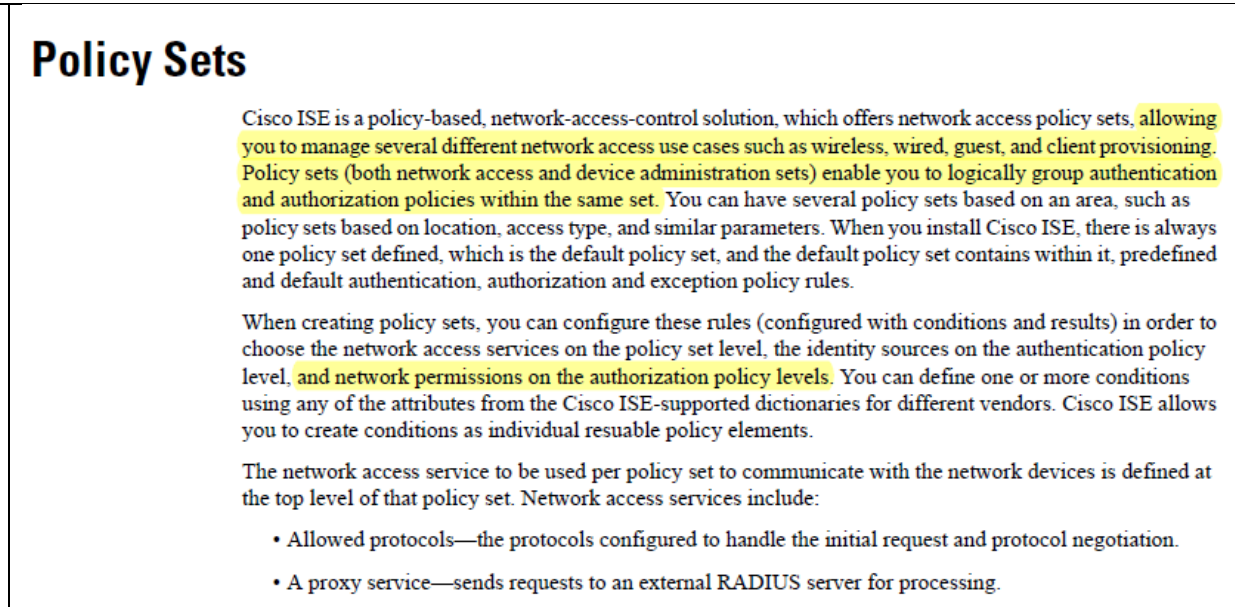
U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	Moreover, Cisco's ISE has a gatekeeper associated with the restricted subset of the protected network. Cisco further explains how ISE collects certain information from the endpoint such as "the MAC address from RADIUS and the IP address" then "issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access[.]"
[1—b] applying a security policy to the access device in response to the request;	Cisco's ISE "appl[ies] a security policy to the access device, responsive to the request [for access,]" or induces others to do so. Cisco explains that the "Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network." • **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods. • **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation. • **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services. ISE 3.0 Admin Guide at 2. Cisco further explains that the ISE "[p]erforms posture assessments to endpoints connected to the network" and "enforces the appropriate compliance policies for [those] endpoints" through different mechanisms. Such "security policies" "include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages . . . antimalware packages .

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	. . patch management . . . rooted or jailbroken status [and] application presence[,]" among others.  **Endpoint posture service** • Performs posture assessments to endpoints connected to the network. • Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM. • Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media. • Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies. • Provides hardware inventory for full network visibility. • Requires the AnyConnect 4.x agent for posture assessment on these OS platforms: ▫ Windows 10 and later ▫ Mac OS X 10.13 and later ▫ Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu) Cisco Identity Services Engine Data Sheet (2023) ("ISE Data Sheet") at 7, available at https://www.cisco.com/c/en/us/products/security/identity-services-engine/ise-ds.pdf (last visited September 22, 2023). Cisco explains how ISE "is a policy-based, network-access-control solution" whose Policy Sets "enable [the user] to logically group authentication and authorization policies within the same set."

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)



Policy Sets

Cisco ISE is a policy-based, network-access-control solution, which offers network access policy sets, allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type, and similar parameters. When you install Cisco ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules.

When creating policy sets, you can configure these rules (configured with conditions and results) in order to choose the network access services on the policy set level, the identity sources on the authentication policy level, and network permissions on the authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE-supported dictionaries for different vendors. Cisco ISE allows you to create conditions as individual resuable policy elements.

The network access service to be used per policy set to communicate with the network devices is defined at the top level of that policy set. Network access services include:

- Allowed protocols—the protocols configured to handle the initial request and protocol negotiation.
- A proxy service—sends requests to an external RADIUS server for processing.

ISE 3.0 Admin Guide at 856; *see also id.* at 858 (Authentication Policies); 874 ("Create Authorization Policies with Endpoint-Analytics Attributes"), 882 ("Cisco ISE uses rule-based policies to provide network access. A policy is a set of rules and results, where the rules are made up of conditions."), 901 ("You can configure authorization profiles and policies in Cisco ISE using the IPv6 attributes in your rule conditions to process such requests from IPv6-enabled endpoints and ensure that the endpoint is compliant."), 940-41 (with Cisco's TrustSec Architecture, "[T]he security group tag (SGT)[] allows Cisco ISE to enforce access control policies by enabling the endpoint device to act upon the SGT to filter traffic."), 1030-31 ("Compliance Module"), 1032 ("Check Posture Compliance"), 1052 (Configure Posture

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

Policies); 1057 ("Client Posture Assessment"), 1057-58 (Posture Assessment Options); *and see generally* 1009-1110 (Chapter 12, Titled "Compliance").

Cisco explains that the ISE can "check" or "view" the "posture compliance" of endpoints through the ISE interface—thereby "applying a security policy to the access device, responsive to the request [for access.]"

Check Posture Compliance

Step 1 Log in to Cisco ISE and access the dashboard.

Step 2 In the **Posture Compliance** dashlet, hover your cursor over a stack bar or sparkline.

A tooltip provides detailed information.

Step 3 Expand the data categories for more information.

Step 4 Expand the **Posture Compliance** dashlet.

A detailed real-time report is displayed.

Note You can view the posture compliance report in the **Context Visibility** window. Navigate **Context Visibility** > **Endpoints** > **Compliance**. This window displays different charts based on **Compliance Status**, **Location**, **Endpoints**, and **Applications by Categories**.

You might see the posture status for endpoints that do not have any active sessions. For example, if the last known posture status for an endpoint is **Compliant**, the status remains **Compliant** in the **Context Visibility** window until the next update is received for the endpoint, even if the endpoint session is terminated. The posture status is retained in the **Context Visibility** window until that endpoint is deleted or purged.

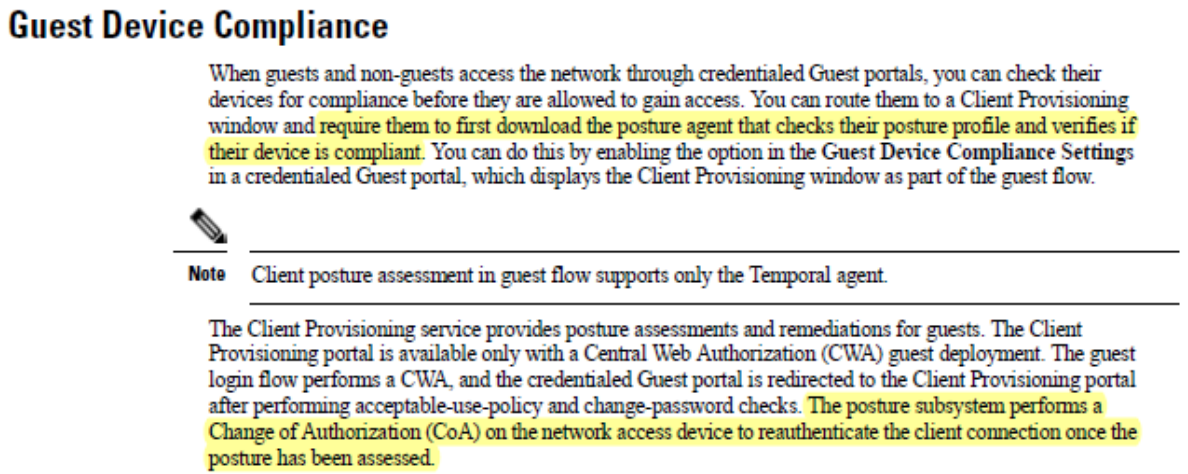
Source: ISE 3.0 Admin Guide at 1032.

As described above (with respect to an MDM server integrated with ISE), ISE "ISE is the enforcement point[, which] obtains data from the MDM server [and] then applies the appropriate access control policies to switches, access routers, wireless access points, and other

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

network access points." Randomized and Changing MAC Deployment Guide at 43. Thus, ISE "appl[ies] a security policy to the access device, responsive to the request [for access.]"

In one example, Cisco explains how ISE "appl[ies] a security policy . . ." with respect to access devices in the form of "guest devices." In particular, Cisco explains how such access devices can be required to "first download [a] posture agent that checks their posture profile and verifies if their device is compliant" with the network security criteria. *Id.* at 401. By "verif[ying] if [a] device is compliant," ISE "applies a security policy" to it.



Guest Device Compliance

When guests and non-guests access the network through credentialed Guest portals, you can check their devices for compliance before they are allowed to gain access. You can route them to a Client Provisioning window and require them to first download the posture agent that checks their posture profile and verifies if their device is compliant. You can do this by enabling the option in the **Guest Device Compliance Settings** in a credentialed Guest portal, which displays the Client Provisioning window as part of the guest flow.

Note Client posture assessment in guest flow supports only the Temporal agent.

The Client Provisioning service provides posture assessments and remediations for guests. The Client Provisioning portal is available only with a Central Web Authorization (CWA) guest deployment. The guest login flow performs a CWA, and the credentialed Guest portal is redirected to the Client Provisioning portal after performing acceptable-use-policy and change-password checks. The posture subsystem performs a Change of Authorization (CoA) on the network access device to reauthenticate the client connection once the posture has been assessed.

Admin Guide at 401. Cisco describes several different posture agents that accomplish this. *See id.* at 1010-11.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	Posture Types The following posture agents monitor and enforce Cisco ISE posture policies: • **AnyConnect**: Deploys the AnyConnect agent to monitor and enforce Cisco ISE posture policies that require interaction with the client. The AnyConnect agent stays on the client. For more information about using AnyConnect in Cisco ISE, see Cisco AnyConnect Secure Mobility, on page 1099. • **AnyConnect Stealth**: Runs posture as a service, with no user interface. The agent stays on the client. When you choose the AnyConnect Stealth posture type in the posture requirement, some of the conditions, remediations, or attributes in a condition are disabled (grayed out). For example, when you enable AnyConnect Stealth requirement, the Manual Remediation Type is disabled (grayed out) because this action requires client-side interaction. When you map the posture profile to the AnyConnect configuration, and then map the AnyConnect configuration to the Client Provisioning window for AnyConnect Stealth mode deployment: • AnyConnect can read the posture profile and set it to the intended mode. • AnyConnect can send information related to the selected mode to Cisco ISE during the initial posture request. • Cisco ISE can match the right policy, based on the mode and other factors, such as identity group, OS, and compliance module.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	• **Temporal Agent**: When a client attempts to access the trusted network, Cisco ISE opens the Client Provisioning portal. The portal instructs the user to download and install the agent, and run the agent. The temporal agent checks the compliance status, and sends the status to Cisco ISE. Cisco ISE acts based on the results. The temporal agent removes itself from the client after compliance processing completes. The temporal agent does not support custom remediation. The default remediation supports only message text. The Temporal Agent does not support the following conditions: • Service Condition MAC—System Daemon check • Service Condition-MAC—Daemon or User Agent check • PM—Up To Date check • PM—Enabled check • DE—Encryption check • For the Temporal Agent, you can only view Patch Management conditions containing the **Installation** check type in the **Requirements** window. • Cisco ISE does not support VLAN-controlled posture with the Temporal Agent for macOS. When you change the network access from an existing VLAN to a new VLAN, the user's IP address is released before the VLAN change. The client gets a new IP address by DHCP when the user connects to the new VLAN. Recognizing the new IP address requires root privileges, but the Temporal Agent runs as a user process. • Cisco ISE supports ACL-controlled posture environment, which does not require the refreshing of endpoint IP addresses. • For more information about configuring the Temporal agent in Cisco ISE, see Configure Cisco Temporal Agent Workflow, on page 1074.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	In another example, the Cisco ISE "appl[ies] a security policy to the access device, responsive to the request [for access]" when it operates with respect to its own or third-party (i.e. non-Cisco) access points. An access device connects to anaccess point (termed a ***network access device*** or ***NAD*** by Cisco). ISE applies a security policy—as described below in step 3 (by "run[ning] the configured authentication and authorization policy") and/or step 11 (by "validat[ing] endpoint compliance").

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

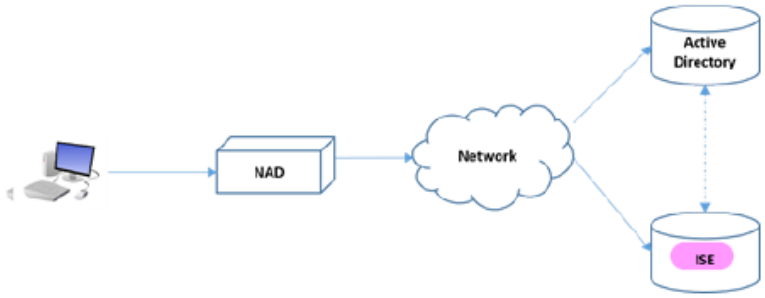
The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

ISE 3.0 Admin Guide at 804; *see also id.* at 805-06 (schematics of same).

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	Finally, in another example—ISE's Easy Connect Enforcement Mode—ISE "collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event. [] After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD ***(based on the appropriate policy managed in the policy service node***), and the user is provided access by the NAD to the network based on ***that policy***." Thus, ISE "applies a security policy." **Easy Connect Enforcement Mode Process Flow** The Easy Connect Enforcement mode process is as follows: 1. The user connects to the NAD from a wired endpoint (such as a PC for example). 2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD. 3. The user logs in to the domain and a security audit event is sent to Cisco ISE. 4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event. 5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy. *Figure 20: Easy Connect Enforcement Mode Basic Flow*  ISE Admin Guide at 581.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

[1—c] using the gatekeeper to determine if requirements of the security policy are satisfied by the access device, and	Cisco's ISE "us[es] the gatekeeper to determine if requirements of the security policy are satisfied by the access device," and induces others to do so. Cisco explains how generally, "ISE allows you to check for compliances, also known as posture, of endpoints, before allowing them to connect to your network." ISE 3.0 Admin Guide at 2. By "check[ing] for compliance" of an endpoint, ISE "uses [its] gatekeeper to determine if requirements of the security policy are satisfied by the access device. *See id.* • **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods. • **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation. • **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services. ISE 3.0 Admin Guide at 2; *see also id.* at 1 ("Cisco Identity Services Engine (ISE) is an identity-based network access control and policy enforcement system. It functions as a common policy engine that enables endpoint access control and network device administration for enterprises. . . You can leverage Cisco ISE to ensure compliance . . .") Cisco also provides various examples of how ISE's gatekeeper "determine[s] if requirements of the security policy are satisfied by the access device[.]" Cisco's ISE can obtain the "***hardware attributes of an endpoint***." ISE 3.0 Admin Guide at 174; *see also id.* at 174-5 (listing attributes), 176 ("Cisco ISE profiles the hardware attributes of a

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	client's system, however, there may be a few hardware attributes Cisco ISE does not profile. . . . The hardware inventory data collection interval can be controlled . . . The default interval is 5 minutes."). Cisco further discloses that one can "check posture compliance" with respect to these hardware attributes—that is, to see if the access device's hardware satisfies requirements that are set in ISE. ISE 3.0 Admin Guide at 1032, 1051; *see also id.* at 2 ("Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network."). "By "check[ing] for compliance," ISE "us[es] the gatekeeper to determine if requirements of the security policy are satisfied by the access device." Cisco's ISE can also obtain "***endpoint attribute data***" which further includes "Profiling attributes: the Multi-Factor Classification attributes—Hardware Manufacturer, Hardware Model, Operating System, and Endpoint Type[;] Trust Score attributes: Attributes related to Random MAC addresses, profiling changes, spoofing detection, and other behaviors that are monitored by Cisco AI Endpoint Analytics to calculate comprehensive Trust Scores for endpoints.[';] . . . Endpoint Trust Score [and] [Configuration Management Database ("CMDB")] attributes" *Id.* at 874-75; *see also* Randomized Changing MAC at 44 (listing six examples of device attributes). Cisco further discloses that "a Cisco ISE administrator can then create specific authorization rules using these values"—which meet the claimed "requirements of a security policy." *See* ISE 3.0 Admin Guide at 874. It follows that Cisco ISE can then determine if the endpoint attribute data complies with the "specific authorization rules"—and thus ISE "us[es] the gatekeeper to determine if requirements of the security policy are satisfied by the access device." Cisco's ISE can also obtain "simple posture conditions," including file conditions, registry conditions, application conditions, service conditions, and USB conditions on the client (the claimed "access device"). *Id.* at 1027. And because it was established that "Cisco ISE allows

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network[,]" (*id.* at 2), by "check[ing] for compliance," ISE "us[es] the gatekeeper to determine if requirements of the security policy are satisfied by the access device." With respect to Cisco's own and third-party (i.e. non-Cisco) access points, ISE "validates endpoint compliance [and] . . . authorizes the endpoint"—that is, it "us[es] the gatekeeper to determine if requirements of the security policy are satisfied by the access device." ISE 3.0 Admin Guide at 804.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

Multiple VLANs may be connected to one network interface card by configuring a VLAN IP helper from the NAD configuration. For more information about configuring an IP helper, see the administration guide for the network device for instructions. For guest access flows that include VLANs with IP helpers, define a guest

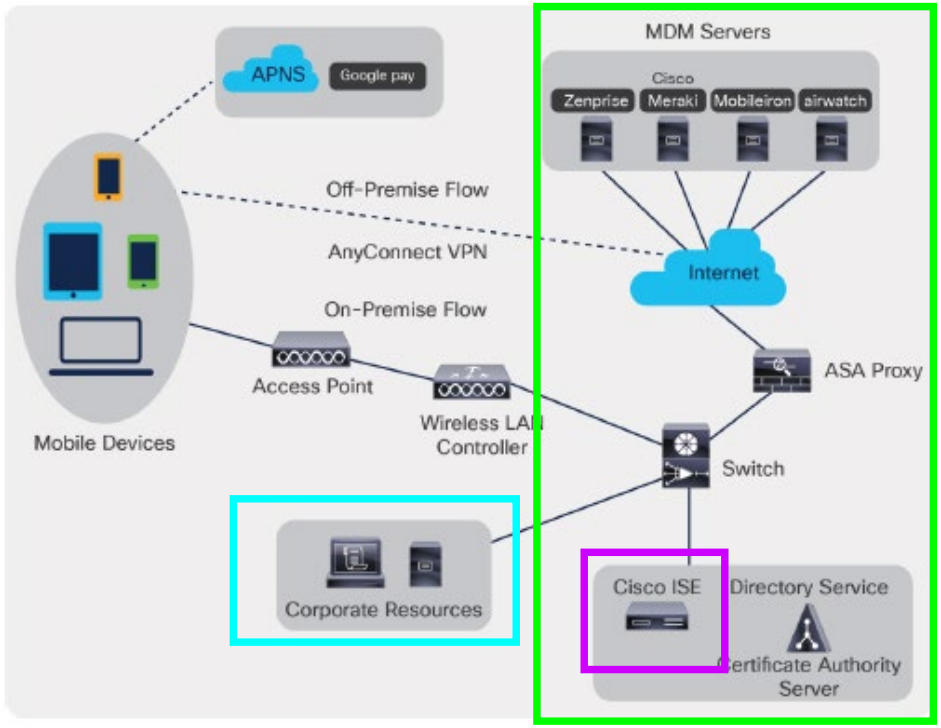
ISE 3.0 Admin Guide at 804.

Also with respect to guest devices, Cisco states that "you can . . . require [guests and non-guests] to first download t***he posture agent that checks their posture profile and verifies if***

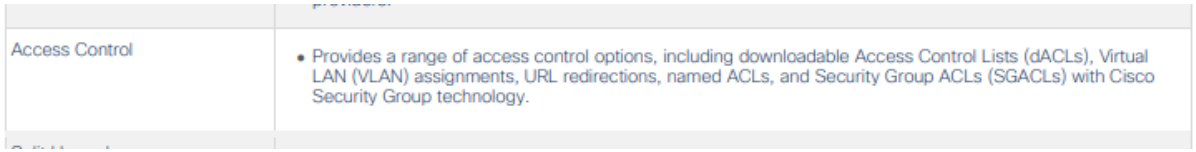
U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	their device is compliant." ISE 3.0 Admin Guide at 401. By "check[ing] their posture profile and verif[ying] if their device is compliant[,]" ISE "us[es] the gatekeeper to determine if requirements of the security policy are satisfied by the access device." **Guest Device Compliance** When guests and non-guests access the network through credentialed Guest portals, you can check their devices for compliance before they are allowed to gain access. You can route them to a Client Provisioning window and require them to first download the posture agent that checks their posture profile and verifies if their device is compliant. You can do this by enabling the option in the **Guest Device Compliance Settings** in a credentialed Guest portal, which displays the Client Provisioning window as part of the guest flow. **Note** Client posture assessment in guest flow supports only the Temporal agent. The Client Provisioning service provides posture assessments and remediations for guests. The Client Provisioning portal is available only with a Central Web Authorization (CWA) guest deployment. The guest login flow performs a CWA, and the credentialed Guest portal is redirected to the Client Provisioning portal after performing acceptable-use-policy and change-password checks. The posture subsystem performs a Change of Authorization (CoA) on the network access device to reauthenticate the client connection once the posture has been assessed. ISE 3.0 Admin Guide at 401.
[1—d] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the	Cisco's ISE "reconfigur[es] the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, when the requirements of the security policy are satisfied," or induces others to do so.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

gatekeeper, when the requirements of the security policy are satisfied.	 As shown, if ISE determines that an access device (e.g. Mobile Devices) satisfies requirements of the security policy, it reconfigures the communication port on the access point to allow the access device to communicate with the less-restricted subset of the protected network (here, "Corporate Resources)." Randomized Changing MAC at 43; *see also id.* at 57 ("If the device is registered with Cisco ISE, is registered with MDM, and is compliant with Cisco ISE and MDM policies, it is ***granted access to the network based on the access control policies configured in Cisco ISE***."). Additionally, as shown in the schematic, if the requirements of the security

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	policy are satisfied, the mobile devices have access through the switch to the corporate resources. Thus, the communication port is "reconfigure[ed] for communicating data . . . without passing the data through the gatekeeper[.]" *Id.* Cisco also describes in its Data Sheet "a range of access control options" for this step, "including downloadable Access Control Lists (dACLs), Virtual LAN (VLAN) assignments, URL redirections, named ACLs, and Security Group ACLs (SGACLs) with Cisco Security Group technology[.]" By using any or all of these methods, ISE "reconfigur[es] the communication port for communicating data between the access device and the less-restricted subset of the protected network"—for example, network resources. Additionally, as show above with respect to MDM servers integrated with ISE, if the requirements of the security policy are satisfied, the communication port is "reconfigure[ed] for communicating data . . . without passing the data through the gatekeeper[.]" *Id.*  Access Control • Provides a range of access control options, including downloadable Access Control Lists (dACLs), Virtual LAN (VLAN) assignments, URL redirections, named ACLs, and Security Group ACLs (SGACLs) with Cisco Security Group technology. ISE Data Sheet at 5. By way of an example previously described—guest device compliance—Cisco states that "the posture agent [] checks their posture profile and verifies if their device is compliant[,]" and further that "the Client Provisioning service provides posture assessments"—that is, ISE determines if "requirements of the security policy are satisfied." ISE 3.0 Admin Guide at 401. Upon such satisfaction, ISE grants the access device access to network resources, thereby

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	"reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network[.]" *See id.* Finally, as show above with respect to MDM servers integrated with ISE, if the requirements of the security policy are satisfied, the communication port is "reconfigure[ed] for communicating data . . . without passing the data through the gatekeeper[.]" *Id.* **Guest Device Compliance** When guests and non-guests access the network through credentialed Guest portals, you can check their devices for compliance before they are allowed to gain access. You can route them to a Client Provisioning window and require them to first download the posture agent that checks their posture profile and verifies if their device is compliant. You can do this by enabling the option in the **Guest Device Compliance Settings** in a credentialed Guest portal, which displays the Client Provisioning window as part of the guest flow. **Note** Client posture assessment in guest flow supports only the Temporal agent. The Client Provisioning service provides posture assessments and remediations for guests. The Client Provisioning portal is available only with a Central Web Authorization (CWA) guest deployment. The guest login flow performs a CWA, and the credentialed Guest portal is redirected to the Client Provisioning portal after performing acceptable-use-policy and change-password checks. The posture subsystem performs a Change of Authorization (CoA) on the network access device to reauthenticate the client connection once the posture has been assessed. ISE 3.0 Admin Guide at 401-02.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	Another example relates to ISE operating with respect to access points (including both Cisco and third-party (i.e. non-Cisco) access points). ISE applies the security policy, as described in the prior step. Once ISE determines that "requirements of the security policy are satisfied," it "sends the [change of authorization ("CoA")], authorizes the endpoint, and bypasses the sink hole[,] and then "the guest user receives the appropriate [network] access based on the CoA." Thus, ISE "reconfigur[es] the communication port for communicating data between the access device and the less-restricted subset of the protected network." Additionally, Cisco describes how ISE "can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication," and shows this in the schematics. As described this way and as further shown in the schematic, if the requirements of the security policy are satisfied, the access devices have network access without passing their data through ISE—that is, "without passing the data through the gatekeeper[.]"

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

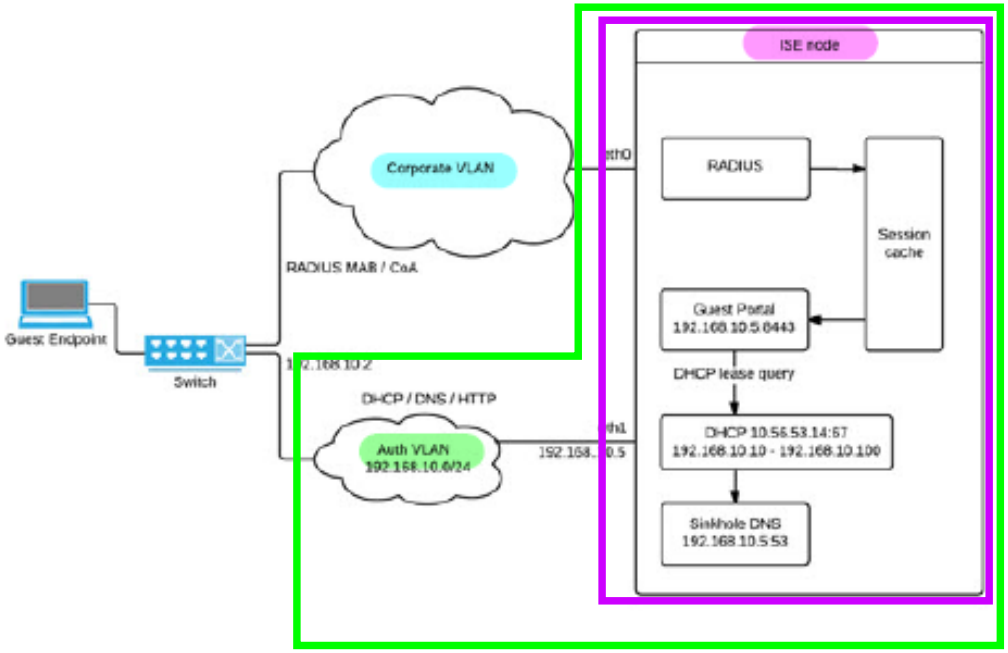
You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

Multiple VLANs may be connected to one network interface card by configuring a VLAN IP helper from the NAD configuration. For more information about configuring an IP helper, see the administration guide for the network device for instructions. For guest access flows that include VLANs with IP helpers, define a guest portal, and select that portal in an authorization profile that is bound to MAB authorization. For more information about guest portals, see the Cisco ISE Guest Services section in *Cisco ISE Admin Guide: Guest and BYOD* .

The following diagram displays a basic network setup when an Auth VLAN is defined (the Auth VLAN is connected directly to a Cisco ISE node).

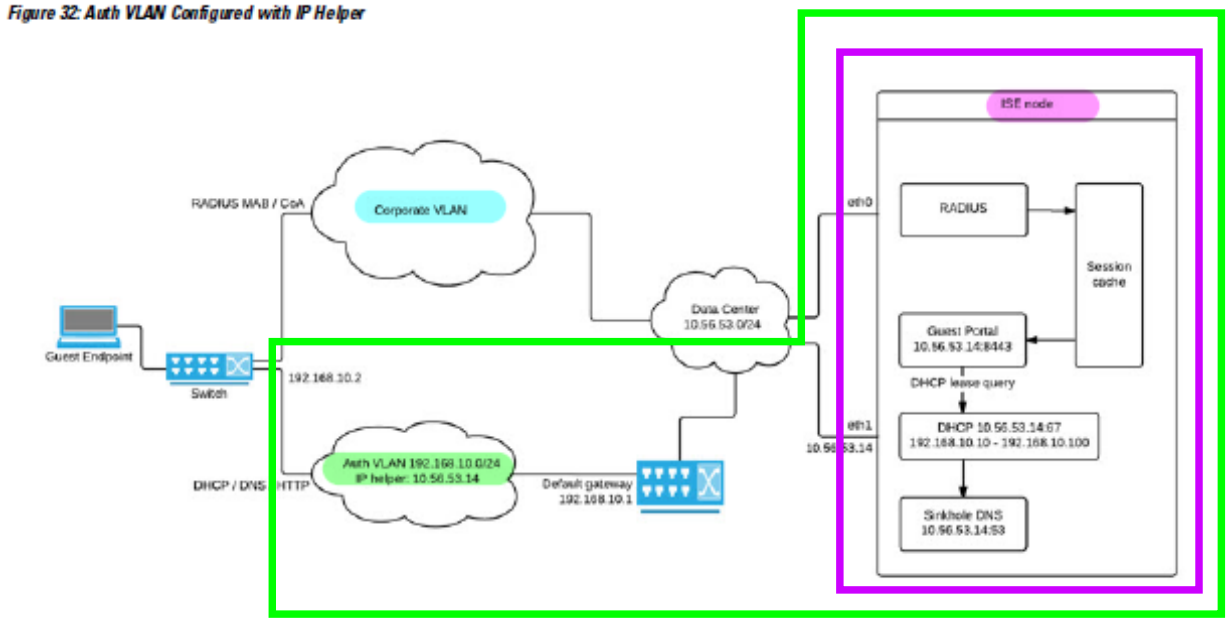
U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

Figure 31: Auth VLAN Connected to Cisco ISE Node



The following diagram displays a network with Auth VLAN and an IP helper.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)



ISE 3.0 Admin Guide at 804-06.

In one further example described above—ISE's Easy Connect Enforcement Mode—ISE collects certain data, after which it "issues a CoA to the [network access device, ("NAD"] (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy." ISE 3.0 Admin Guide at 580-81. By issuing a CoA to the NAD, to provide the user access to the network, ISE "reconfigur[es] the communication port for communicating data between the access device and the less-restricted subset of the

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

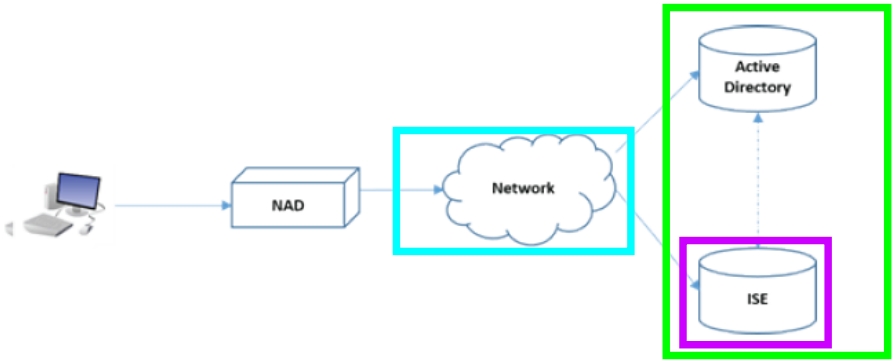
protected network[.]" Additionally, as shown in the schematic, if the requirements of the security policy are satisfied, the access devices have network access without passing their data through ISE—that is, "without passing the data through the gatekeeper[.]"

Easy Connect Enforcement Mode Process Flow

The Easy Connect Enforcement mode process is as follows:

1. The user connects to the NAD from a wired endpoint (such as a PC for example).
2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD.
3. The user logs in to the domain and a security audit event is sent to Cisco ISE.
4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event.
5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy.

Figure 20: Easy Connect Enforcement Mode Basic Flow



U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	In addition to making, using, offering for sale, and selling the ISE, Cisco also induces third-parties to infringe this claim as set forth in InfoExpress's 3-1 disclosures under 35 USC 271(b). For this claim, the underlying direct infringement is caused by the third-parties including Cisco's customers, subscribers, users and developers. And Cisco's acts of induced infringement including the following: as set forth herein, the Release Notes, Admin Guide, Randomized and Changing MAC Deployment Guide and Data Sheets for the ISE are all provided by Cisco to third-parties which provide deliberate and specific instruction and guidance for third-parties to use the ISE in a manner infringed by this claim. In addition, Cisco's Identity Services Engine Administrator Guide ("ISE AG) explains also provide such specific guidance of infringement to third-parties explaining that "[a]dministrators can use the admin portal to: Manage deployments, help desk operations, and network devices, and node monitoring and troubleshooting; Manage Cisco ISE services, policies, administrator accounts, and system configuration and operations." https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/admin_guide/b_ise_admin_3_3/b_ISE_admin_33_overview.html For example, the Admin Guide explains that its audience can be third party administrators ("Cisco ISE administrators can perform various administrative tasks based on the administrative group to which they belong. These administrators are critical. Grant administrative access only to users who are authorized to administer Cisco ISE in your network" ISE 3.0 Admin Guide at 13); developers ("On Facebook, create a Facebook application: a) Log on to http://developers.facebook.com and sign up as a developer," ISE 3.0 Admin Guide at. 397), and it instructs these third-parties on configuring the ISE, for example, with respect to the claimed authentication, compliance, and access point reconfiguration. With respect to this claim, the Admin Guide instructs third-parties how to "Create a Certificate Authentication Profile for TLS-Based Authentication." ISE 3.0 Admin Guide at 269-270. In particular, Cisco instructs these third-parties how to "use certificates for authenticating

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	endpoints that connect to your network" and "defin[ing] a certificate authentication profile in Cisco ISE…" *Id.* In another example, the Cisco's Admin guide instructs third-parties how to apply and/or configure security policies. For example, Cisco explains that the third-parties can "globally configure the Admin portal for posture services." ISE 3.0 Admin Guide at 1015. There, Cisco's Admin guide instructs third-parties how to "download updates automatically to the Cisco ISE through the web from Cisco. *Id*. Further, Cisco explains the various steps for how to "create a posture requirement." Id.. at. 1015-17; *see also id.* at 1066 (Cisco instructing third-parties on "Create[ing] Client Posture Requirements"); *id* at 1067 ("Posture Reassessment Configuration Settings"); *id.* at 1023 ("You can use the Posture Update window to download updates dynamically from the web."); *id.* at 1072 ("Creat[ing] a Posture Condition", "Creat[ing] Posture Remediation."); *id.* at 1073 ("Create Posture Policy"). The ISE AG provides third-parties with an "Administration Portal" which provides third-parties "Policy windows include[ing] tools for managing network security in the areas of authentication, authorization, profiling, posture, and client provisioning." https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/admin_guide/b_ise_admin_3_3/b_ISE_admin_33_basic_setup.html#reference_D93EF6652C8D4EB8B56EC6B857DA6F9A. Further, the ISE AG permits third-parties to create "Posture conditions" by following the following field path at the Administration Portal: "Policy -> Policy Elements -> Conditions -> Posture windows." Id. In another example, Cisco's Admin guide instructs third-parties with respect to "Quarantine [for] a Vulnerable Endpoint." ISE 3.0 Admin Guide at 1127. Specifically, Cisco explains that "You can choose to quarantine the endpoint, provide limited access (redirect to a different portal), or reject the request" and then provides three steps for doing so. *Id*.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	Similarly, the ISE AG explains to third-parties how they can configure the ISE to "perform the following operations to monitor and control network access through ANC: Quarantine: … Setting to the Quarantine state essentially moves an endpoint from its default VLAN to a specified Quarantine VLAN. You must define the Quarantine VLAN previously that is supported on the same NAS as the endpoint." https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/admin_guide/b_ise_admin_3_3/b_ISE_admin_33_maintain_monitor.html.
2. The method of claim 1, further comprising authenticating a user of the access device.	Cisco's ISE performs "[t]he method of claim 1, further comprising authenticating a user of the access device[,]" and induces others to do so. Cisco's ISE "authenticat[es] a user of the access device" of a device (which Cisco terms an "endpoint"). Cisco explains how its ISE "***uses*** a wide range of ***authentication protocols*** to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods."

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	• **Bring Your Own Device (BYOD)**: Cisco ISE allows your employees and guests to securely use their personal devices on your enterprise network. BYOD feature end users can use configured pathways to add their devices, and provision predefined authentications and levels of network access. • **Asset Visibility**: Cisco ISE gives you visibility and control over who and what is on your network consistently, across wireless, wired, and VPN connections. Cisco ISE uses probes and device sensors to listen to the way devices connect to the network. The Cisco ISE profile database, which is extensive, then classifies the device. This gives the visibility and context you need to grant the right level of network access. • **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods. • **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation. Cisco also explains that with respect to authentication policies, Cisco ISE "checks the identity sources and results from the authentication and authorization policy levels." ISE 3.0 Admin Guide at 858. Furthermore, a "single identity database" can include, for example, "internal users" and guest users." *Id.*

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

Authentication Policies

Each policy set can contain multiple authentication rules that together represent the authentication policy for that set. Priority of the authentication policies is determined based on the order to those policies as they appear within the policy set itself (from the Set view page in the Authentication Policy area).

Cisco ISE dynamically chooses the network access service (either an allowed protocol a server sequence) based on the settings configured on the policy set level, and thereafter checks the identity sources and results from the authentication and authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE dictionary. Cisco ISE allows you to create conditions as individual policy elements that can be stored in the Library and then can be reused for other rule-based policies.

The identity method, which is the result of the authentication policy, can be any one of the following:

- Deny access—Access to the user is denied and no authentication is performed.
- Identity database—A single identity database that can be any one of the following:
  - Internal users
  - Guest users
  - Internal endpoints
  - Active Directory
  - Lightweight Directory Access Protocol (LDAP) database
  - RADIUS token server (RSA or SafeWord server)
  - Certificate authentication profile
- Identity source sequences—A sequence of identity databases that is used for authentication.

By way of one example—Cisco explains how the ISE uses the validated Adaptive Security Appliances (ASA) in the context of authentication: "The ASA proceeds to ***primary user authentication (AAA) using the username/password*** and passes the information to the authentication server (ISE)." ISE 3.0 Admin Guide at 280-81. And in a later step, "The ***user can again authenticate*** using the certificate and a normal VPN connection is established." *Id.* By

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	using "primary user authentication (AAA) using the username/password" Cisco "authenticat[es] a user of the access device[.]"

Cisco ISE CA Issues Certificates to ASA VPN Users

ISE CA issues certificates to client machines connecting over ASA VPN. Using this feature, you can automatically provision certificates to end devices that connect over ASA VPN.

Cisco ISE uses the Simple Certificate Enrollment Protocol (SCEP) for enrollment and to provision certificates to the client machines. The AnyConnect client sends the SCEP request to the ASA over an HTTPS connection. The ASA evaluates the request and enforces policies before it relays the request to Cisco ISE over an HTTP connection established between Cisco ISE and ASA. The response from the Cisco ISE CA is relayed back to the client. The ASA cannot read the contents of the SCEP message and functions as a proxy for the Cisco ISE CA. The Cisco ISE CA decrypts the SCEP message from the client and sends the response in an encrypted form.

The ISE CA SCEP URL is http://<*IP Address or FQDN of ISE CA server*>:9090/auth/caservice/pkiclient.exe. If you are using FQDN of the ISE node, the DNS server connected to ASA must be able to resolve the FQDN.

You can configure certificate renewal before expiration in the AnyConnect Client profile. If the certificate has already expired, the renewal flow is similar to a new enrollment.

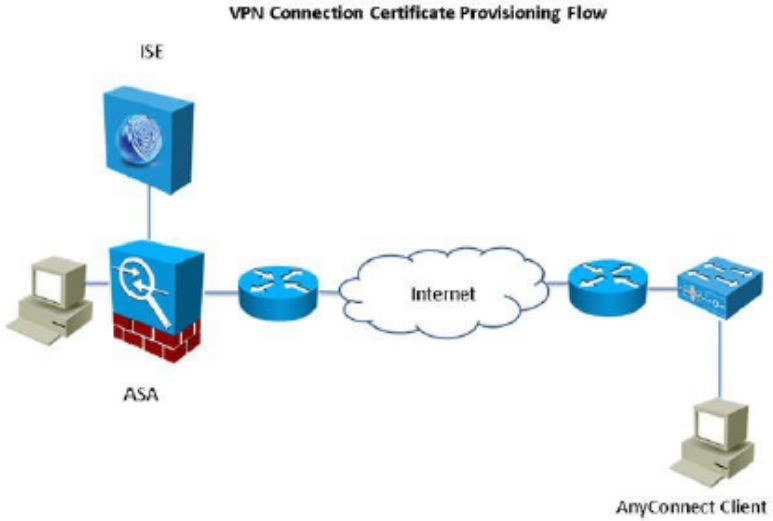
Supported versions include:

- Cisco ASA 5500 Series Adaptive Security Appliances that run software version 8.x
- Cisco AnyConnect VPN version 2.4 or later

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

VPN Connection Certificate-Provisioning Flow

Figure 10: Certificate Provisioning for ASA VPN Users



1. The user initiates a VPN connection.

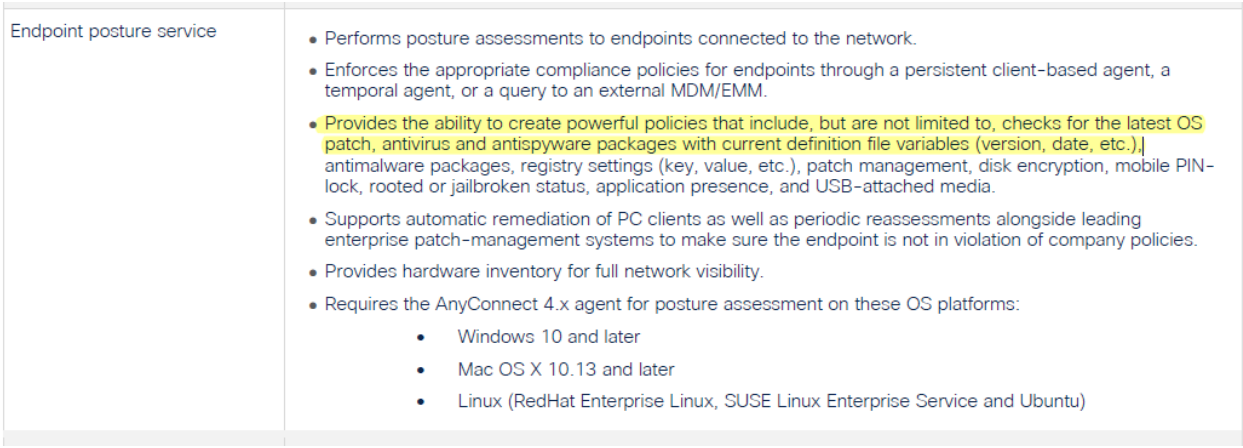
U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	2. The AnyConnect client scans the client machine and sends the attributes such as the unique device identifier (for example, IMEI) to the ASA. 3. The ASA requests certificate-based authentication from the client. The authentication fails because there is no certificate. 4. The ASA proceeds to primary user authentication (AAA) using the username/password and passes the information to the authentication server (ISE). a. If authentication fails, the connection is terminated immediately. b. If authentication passes, limited access is granted. You can configure dynamic access policies (DAP) for client machines that request a certificate using the aaa.cisco.sceprequired attribute. You can set the value for this attribute to "true" and apply ACLs and web ACLs. 5. The VPN connection is established after the relevant policies and ACLs are applied. The client starts key generation for SCEP only after AAA authentication succeeds and the VPN connection is established. 6. The client starts the SCEP enrollment and sends SCEP requests to ASA over HTTP. 7. ASA looks up the session information of the request and relays the request to ISE CA, if the session is allowed for enrollment. 8. ASA relays the response from ISE CA back to the client. 9. If enrollment succeeds, the client presents a configurable message to the user and disconnects the VPN session. 10. The user can again authenticate using the certificate and a normal VPN connection is established. ISE 3.0 Admin Guide at 280-81; *see also id.* at 635 ("Cisco ISE can ***authenticate*** a subject (user or host) against an [Lightweight Directory Access Protocol ('LDAP')] identity source . . ."); 862 (Password-Based Authentication).

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

3. The method of claim 1, further comprising obtaining system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.	Cisco performs "[t]he method of claim 1, further comprising obtaining system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy" and induces others to do so. As explained above with respect to claim element 1-c, Cisco ISE "uses [its] gatekeeper to determine if requirements of the security policy are satisfied by the access device. Furthermore with respect to that same element were provided several examples of how Cisco does so: • By obtaining the "hardware attributes of an endpoint," • By obtaining "endpoint attribute data," • By obtaining "simple posture conditions," • By, with respect to Cisco's own and third-party (i.e. non-Cisco) access points, "validat[ing] endpoint compliance [and] . . . authoriz[ing] the endpoint," and • By, with respect to guest devices, providing "the posture agent that checks their posture profile and verifies if their device is compliant." These examples of attributes, posture conditions and the like also constitute examples of "system data," which Cisco's ISE "obtain[s] . . . from the access device." And furthermore, just as Cisco ISE "use[s] [its] gatekeeper to determine if requirements of the security policy are satisfied by the access device," it so to "appl[ies] [its] security policy [by] using the system data to determine that the access device satisfies the requirements of the security policy."

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

4. The method of claim 3, wherein the system data includes antivirus software status.	Cisco's ISE performs "[t]he method of claim 3, wherein the system data includes antivirus software status." Cisco discloses that ISE can "check[] for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.)[.]" Thus, the "system data" (which is used "to determine that the access device satisfies the requirements of the security policy") includes antivirus software status.  *See also* ISE 3.0 Admin Guide at 1057-58 (posture assessment options include Antivirus Installation and Antivirus Version/ Antivirus Definition Date).

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

5. The method of claim 1, further comprising communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.	Cisco's ISE performs "[t]he method of claim 1, further comprising communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy[,]"and induces others to do so. As disclosed above with respect to claim element 1-b, Cisco's ISE uses "posture agents" (the claimed "agent executing on the access device"). These include: • The ***AnyConnect Agent*** (which can "report[] a complete list of running and installed applications" on the access device, ISE 3.0 Admin Guide at 1102-03; *see also id.* at 1057-58); • The ***AnyConnect Stealth Agent*** (which reports certain information back to ISE, *id.* at 1010-11); and • The ***Cisco Temporal Agent***, (which is a "temporary executable file that is run on the client to check the compliance status" and which "is removed from the client machine after the login session is terminated"). Furthermore, as disclosed above with respect to claim 3, Cisco performs the "method of claim 1, further comprising ***obtaining system data*** from the access device, and wherein applying the security policy includes using the ***system data*** to determine that the access device satisfies the requirements of the security policy[.]" Cisco also discloses several non-limiting examples of "system data." Therefore, these (1) agents (1) "execut[e] on the access device to obtain system data from the access device, and (2) "communicat[e] that system data to ISE's gatekeeper so that (3) ISE can

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	"apply[] the security policy [] using th[at] system data to determine that the access device satisfies the requirements of the security policy," Cisco and/or ISE "communicat[e]between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy."
6. The method of claim 5, wherein the system data includes information regarding devices connected to the access device.	Cisco's ISE performs "[t]he method of claim 5, wherein the system data includes information regarding devices connected to the access device" and induces others to do so. Cisco states, with respect to "hardware attributes," that they include a field for "attached devices." ISE 3.0 Admin Guide at 174-75. Cisco further explains that "You can click the number in the Attached Devices column that corresponds to an endpoint to view the Name, Category, Manufacturer, Type, Product ID, and Vendor ID of the USB devices that are currently attached to the endpoint." *Id.*; *see also id.* 1027 (USB Conditions), 1051 (USB Condition Settings), 1057 (USB_Block "[e]nsures that the endpoint device does not have any USB storage devices connected"). Thus, because Cisco's ISE can determine "attached devices" such as a USB (which are so attached to the endpoint), the system data includes information regarding devices connected to the access device.
10. The method of claim 1, wherein the access point is a network switch.	Cisco's ISE performs "[t]he method of claim 1, wherein the access point is a network switch. and induces others to do so. Cisco explains that with respect to mobile device management (MDM) server integration with ISE, "ISE is the enforcement point . . . [that] then applies the appropriate access control policies to ***switches***, access routers, wireless access points, and other network access points." Randomized and Changing MAC Deployment Guide at 43; *see also* ISE 3.0 Admin Guide at 830

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	(same); *and also* 363 (The device administrator is the user who logs into the network devices such as switches, wireless access points, ***routers***, and gateways, (normally through SSH), to perform the configuration and maintenance of the administered devices."), 787 ("A network device, ***such as a switch or a router***, is an authentication, authorization, and accounting (AAA) client that sends AAA service requests to Cisco ISE. Defining network devices in Cisco ISE enables interactions between Cisco ISE and network devices."). Thus the "access point" includes a "network switch." A list of hardware products that are compatible with its ISE—including switches—is listed in Cisco's Identity Services Engine Network Component Compatibility documents, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014309 to INFOEX-CSCO_0014605. These Cisco documents describe "Cisco Identity Services Engine (ISE) validated compatibility with switches, wireless LAN controllers, and other policy enforcement devices as well as operating systems with which Cisco ISE interoperates." INFOEX-CSCO_0014586 at 14586.
11. The method of claim 1, wherein the access point is a wireless access point.	Cisco's ISE performs "[t]he method of claim 1, wherein the access point is a wireless access point" and induces others to do so. Cisco explains that with respect to mobile device management (MDM) server integration with ISE, "ISE is the enforcement point . . . [that] then applies the appropriate access control policies to switches, access routers, ***wireless access points***, and other network access points." Randomized and Changing MAC Deployment Guide at 43; *see also* ISE 3.0 Admin Guide at 830 (same); *and also* 363 (The device administrator is the user who logs into the network devices such as switches, ***wireless access points***, routers, and gateways, (normally through SSH), to

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	perform the configuration and maintenance of the administered devices.") Thus the "access point" includes a "wireless access point." You can configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type c third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. It then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network. Randomized and Changing MAC Deployment Guide at 43. A list of hardware products that are compatible with its ISE—including access points—is disclosed in Cisco's Identity Services Engine Network Component Compatibility documents, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014309 to INFOEX-CSCO_0014605. These Cisco documents describe "Cisco Identity Services Engine (ISE) validated compatibility with switches, wireless LAN controllers, and other policy enforcement devices as well as operating systems with which Cisco ISE interoperates." INFOEX-CSCO_0014586 at 14586.
12. The method of claim 1, wherein the access point is a remote access virtual private network.	Cisco's ISE performs "[t]he method of claim 1, wherein the access point is a remote access virtual private network" and induces others to do so. Cisco describes how generally, ISE can administer access for VPN connections. ISE 3.0 Admin Guide at 1-2. A Cisco ISE administrator can gather real-time contextual data for a network, including users and user groups (who?), device type (what?), access time (when?), access location (where?), access type (wired, wireless, or VPN) (how?), and network threats and vulnerabilities.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	. . . . • **Asset Visibility**: Cisco ISE gives you visibility and control over who and what is on your network consistently, across wireless, wired, and VPN connections. Cisco ISE uses probes and device sensors to listen to the way devices connect to the network. The Cisco ISE profile database, which is extensive, then classifies the device. This gives the visibility and context you need to grant the right level of network access. ISE 3.0 Admin Guide at 1-2. Cisco further describes how ISE establishes connections over remote access VPNs:

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

Cisco ISE CA Issues Certificates to ASA VPN Users

ISE CA issues certificates to client machines connecting over ASA VPN. Using this feature, you can automatically provision certificates to end devices that connect over ASA VPN.

Cisco ISE uses the Simple Certificate Enrollment Protocol (SCEP) for enrollment and to provision certificates to the client machines. The AnyConnect client sends the SCEP request to the ASA over an HTTPS connection. The ASA evaluates the request and enforces policies before it relays the request to Cisco ISE over an HTTP connection established between Cisco ISE and ASA. The response from the Cisco ISE CA is relayed back to the client. The ASA cannot read the contents of the SCEP message and functions as a proxy for the Cisco ISE CA. The Cisco ISE CA decrypts the SCEP message from the client and sends the response in an encrypted form.

The ISE CA SCEP URL is http://<*IP Address or FQDN of ISE CA server*>:9090/auth/caservice/pkiclient.exe. If you are using FQDN of the ISE node, the DNS server connected to ASA must be able to resolve the FQDN.

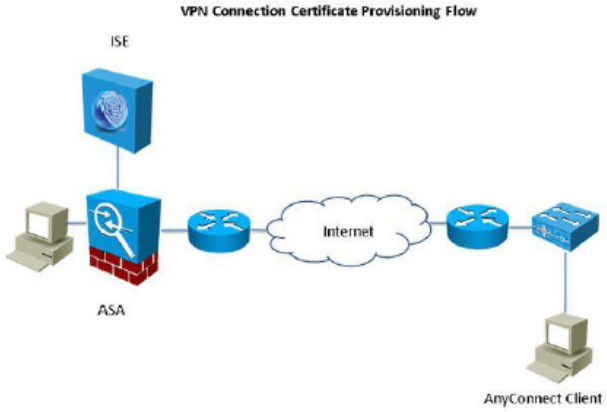
You can configure certificate renewal before expiration in the AnyConnect Client profile. If the certificate has already expired, the renewal flow is similar to a new enrollment.

Supported versions include:

- Cisco ASA 5500 Series Adaptive Security Appliances that run software version 8.x
- Cisco AnyConnect VPN version 2.4 or later

VPN Connection Certificate-Provisioning Flow

Figure 10: Certificate Provisioning for ASA VPN Users



1. The user initiates a VPN connection.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	2. The AnyConnect client scans the client machine and sends the attributes such as the unique device identifier (for example, IMEI) to the ASA. 3. The ASA requests certificate-based authentication from the client. The authentication fails because there is no certificate. 4. The ASA proceeds to primary user authentication (AAA) using the username/password and passes the information to the authentication server (ISE). a. If authentication fails, the connection is terminated immediately. b. If authentication passes, limited access is granted. You can configure dynamic access policies (DAP) for client machines that request a certificate using the aaa.cisco.sceprequired attribute. You can set the value for this attribute to "true" and apply ACLs and web ACLs. 5. The VPN connection is established after the relevant policies and ACLs are applied. The client starts key generation for SCEP only after AAA authentication succeeds and the VPN connection is established. 6. The client starts the SCEP enrollment and sends SCEP requests to ASA over HTTP. 7. ASA looks up the session information of the request and relays the request to ISE CA, if the session is allowed for enrollment. 8. ASA relays the response from ISE CA back to the client. 9. If enrollment succeeds, the client presents a configurable message to the user and disconnects the VPN session. 10. The user can again authenticate using the certificate and a normal VPN connection is established. ISE 3.0 Admin Guide at 280-81, *see also id.* at 281-84 (Configure Cisco ISE CA to Issue Certificates to ASA VPN Users). Finally, Cisco discloses (in its guide for its ASA series firewalls) that (1) Cisco's ASA series firewalls use ISE and (2) they use remote access VPNs. Cisco, ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide, 7.10,

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/asdm710/firewall/asdm-710-firewall-config.pdf, at 2 ("To implement identity control, do any combination of the following: . . . Install Cisco Identity Services Engine (ISE) on a separate server to implement Cisco Trustsec.") *and* 75-78 (including a section on "Register the ASA with the ISE"); *and also, e.g.* 38 ("***Remote access VPNs*** also use extended ACLs for client firewall configurations and dynamic access policies.")

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

Claim 16

[Claim 16—preamble] A non-transitory computer-readable storage medium having stored thereon a program, the program being executable by a processor to perform a method for controlling access to a computer network, the method comprising:	Cisco infringes this claim by making, using, testing, offering for sale, and selling the ISE product and system and through performance of each of the claimed steps and/or providing instructions and data from its servers to third-parties to perform at least one of the claimed steps. Cisco further induces others to infringe as set forth in 1-d above. Further, subsequent to Cisco's making, using, testing, offering for sale, and selling of the ISE, Cisco offers services to third-parties and customers with respect to the ISE. For example, these can include "Technical Services," "Advisory Services," and "Cisco Talos Incidence Response" services. (https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/ise-licensing-guide-og.html). For technical services, for example, Cisco encourages customers to purchase "Cisco Smart Net Total Care" for Cisco ISE physical appliances and Software Support (SWSS) contracts for Cisco ISE virtual machines. For advisory services, Cisco offers Expert Services to address "your business objectives with the technology we offer" (including ISE). *Id*. And for the Talos Incident Response, Cisco provides a full suite of proactive and emergency services to help third-parties prepare, respond, and recover from a cybersecurity breach. Cisco explains that third-parties can "order and transact Cisco Talos Incident Response when ordering Cisco ISE subscriptions." *Id*. To the extent the preamble is limiting, Cisco provides or sells ISE, which includes "[a] non-transitory computer-readable storage medium having stored thereon a program, the program being executable by a processor to perform a method for controlling access to a computer network[.]"

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	Additionally, and as set forth in InfoExpress's 3-1 disclosures, Cisco's ISE also includes Cisco's ISE (NAC) appliance. Specifically, these are Cisco-provided tangible hardware and "virtual appliances" on which ISE can be deployed. A list of accused NAC Appliances (also referred to as "hardware platforms") which ISE supports, are disclosed in InfoExpress's Disclosure of Asserted Claims and Infringement Contentions per Patent L.R. 3-1 and 3-2 at Section II.B.2. These ISE (NAC) Appliances are listed in Cisco's Identity Services Engine Administrator Guides, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0001603 to 0014308, and also their Release Notes for ISE Releases 1.04, 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014606 to 0015185. Cisco's ISE (NAC) appliances are directed to "[g]ranting and denying network access" and using "attributes related to users and their devices" in "determining authorized network access." https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/datasheet-c78-726524.html. Cisco further explains that its NAC appliance (known in one example as "The Cisco Secure Network Server") "supports Cisco's powerful network access and control security applications." *Id*. Further, Cisco explains that the "Cisco Secure Network Server… is configured specifically to support the Cisco Identity Services Engine (ISE) security application." *Id*.
[16-a] receiving a request for access to a less-restricted subset of the protected network from an access device, the request being received through a	As disclosed above with respect to claim element 1-a, Cisco's ISE "receiv[es] a request for access to a less-restricted subset of the protected network from an access device, the request received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper[.]" Thus, Cisco's ISE (including NAC Appliances) comprises "[a] non-transitory computer-readable storage medium having stored thereon a program, the program being executable by a processor to perform a method for controlling

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper;	access to a computer network, the method comprising: . . . receiving a request for access to a less-restricted subset of the protected network from an access device, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper" for the reasons identified in claim element 1-a.
[16-b] applying a security policy to the access device, in response to the request;	As disclosed above with respect to claim element 1-b, Cisco's ISE "appl[ies] a security policy to the access device in response to the request [for access][.]" Thus, Cisco's ISE (including NAC Appliances) comprises "[a] non-transitory computer-readable storage medium having stored thereon a program, the program being executable by a processor to perform a method for controlling access to a computer network, the method comprising: . . . applying a security policy to the access device, in response to the request [for access]" for the reasons identified in claim element 1-b.
[16-c] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network	As disclosed above with respect to claim element 1-d, Cisco's ISE—"reconfigure[es] the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, when the requirements of the security policy are satisfied." Thus, Cisco's ISE (including NAC Appliances) comprises "[a] non-transitory computer-readable storage medium having stored thereon a program, the program being executable by a processor to perform a method for controlling access to a computer network, the method comprising: reconfiguring the communication port for communicating data between the access device and the less-restricted

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

without passing the data through the gatekeeper, when requirements of the security policy are satisfied.	subset of the protected network without passing the data through the gatekeeper, when requirements of the security policy are satisfied" for the reasons identified in claim element 1-d.
17. The non-transitory computer readable storage medium of claim 16, wherein the program is further executable by a processor to authenticate a user of the access device.	Cisco provides or sells "[t]he non-transitory computer readable storage medium of claim 16, wherein the program is further executable by a processor to authenticate a user of the access device." As disclosed above with respect to claim 2, Cisco's ISE "authenticat[es] a user of the access device." Thus, Cisco's ISE (including NAC Appliances) comprises "[a] non-transitory computer readable storage medium of claim 16, wherein the program is further executable by a processor to authenticate a user of the access device" for the reasons identified in claim 2.
18. The non-transitory computer readable storage medium of claim 16, wherein the program is further executable by a processor to obtain system data from the access device, and wherein applying the	Cisco provides or sells "[t]he non-transitory computer readable storage medium of claim 16, wherein the program is further executable by a processor to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy." As disclosed above with respect to claim 3, Cisco's ISE—"obtain[s] system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy." Thus, Cisco's ISE (including NAC Appliances) comprises "[a] non-transitory computer readable storage medium of claim 16, wherein the program is further executable by a processor to obtain

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.	system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy" for the reasons identified in claim 3.

19. The non-transitory computer readable storage medium of claim 18, wherein the system data includes antivirus software version data.	Cisco provides or sells "[t]he non-transitory computer readable storage medium of claim 18, wherein the system data includes antivirus software version data."
	
	As disclosed above with respect to claim 4, Cisco ISE's "system data includes antivirus software status." *See also* ISE Data Sheet at 7 (Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, ***antivirus and antispyware packages*** with current definition file variables (***version***, date, etc.)[.]"
	
	Endpoint posture service
	• Performs posture assessments to endpoints connected to the network.
	• Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM.
	• Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media.
	• Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies.
	• Provides hardware inventory for full network visibility.
	• Requires the AnyConnect 4.x agent for posture assessment on these OS platforms:
	  • Windows 10 and later
	  • Mac OS X 10.13 and later
	  • Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu)

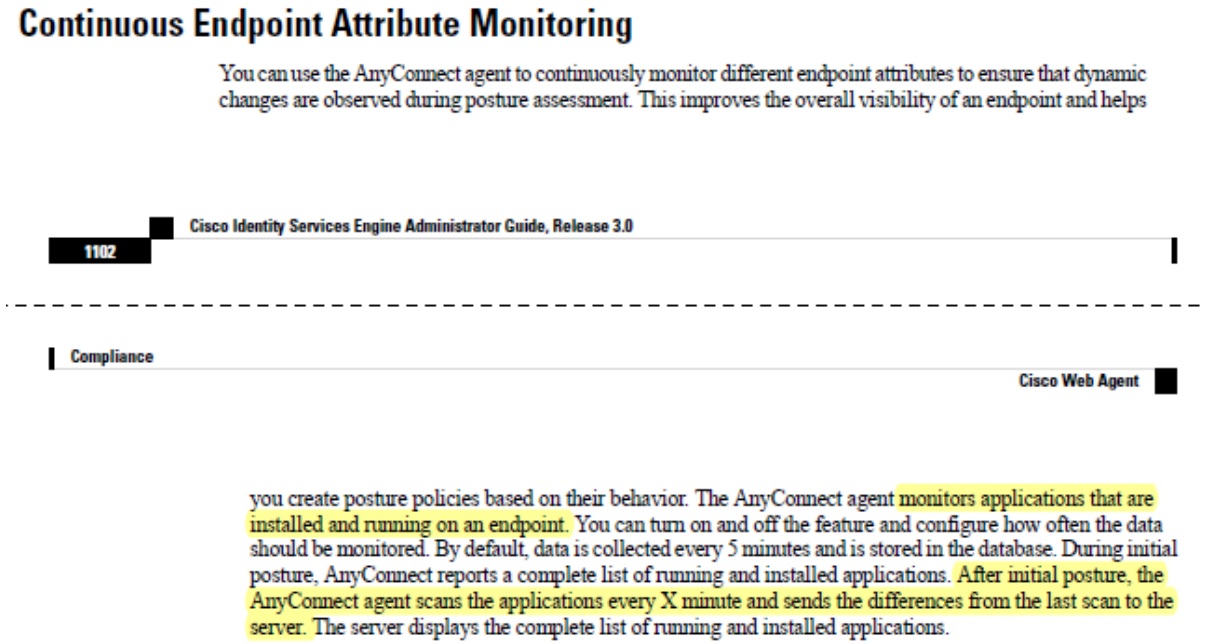
U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	Thus, Cisco's ISE (including NAC Appliances) comprises "[a] non-transitory computer readable storage medium of claim 18, wherein the system data includes antivirus software version data."
20. The non-transitory computer readable storage medium of claim 16, wherein the program is further executable to communicate between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.	Cisco provides or sells "[t]he non-transitory computer readable storage medium of claim 16, wherein the program is further executable to communicate between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy." As disclosed above with respect to claim 5, Cisco's ISE "communicat[es] between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy." Thus, Cisco's ISE (including NAC Appliances) comprises "[a] non-transitory computer readable storage medium of claim 16, wherein the program is further executable to communicate between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy" for the reasons identified in claim 5.
21. The non-transitory computer storage readable medium of	Cisco provides or sells "[t]he non-transitory computer readable storage medium of claim 20, wherein the system data includes information regarding devices connected to the access device."

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

claim 20, wherein the system data includes information regarding devices connected to the access device.	As disclosed above with respect to claim 6, Cisco ISE's "system data includes information regarding devices connected to the access device." Thus, Cisco's ISE (including NAC Appliances) comprises "[a] non-transitory computer storage readable medium of claim 20, wherein the system data includes information regarding devices connected to the access device."
22. The non-transitory computer readable storage medium of claim 16, wherein the program is further executable to communicate between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port for communicating between the access device and the less-restricted subset.	Cisco provides or sells "[t]he non-transitory computer readable storage medium of claim 16, wherein the program is further executable to communicate between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port for communicating between the access device and the less-restricted subset." Cisco states that after an endpoint (the claimed "access device") is granted access to network resources ("after reconfiguring the communication port for communicating between the access device and the less-restricted subset"), ISE can use ***Continuous Endpoint Attribute Monitoring***. ISE 3.0 Admin Guide at 1002-03. With ***Continuous Endpoint Attribute Monitoring***, ISE uses the AnyConnect agent (the claimed "agent executing on the access device") to monitor the endpoint after initial posture ("after reconfiguring . . ."). Cisco further states, "After initial posture, the AnyConnect agent scans the applications every X minute and sends the differences from the last scan to the server." Thus, by sending differences from the last scan to the server, ISE "communicat[es] between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port for communicating between the access device and the less-restricted subset[." Thus, Cisco's ISE (including NAC Appliances) comprises "[a] non-transitory computer readable storage medium of claim 16, wherein the program is further executable to

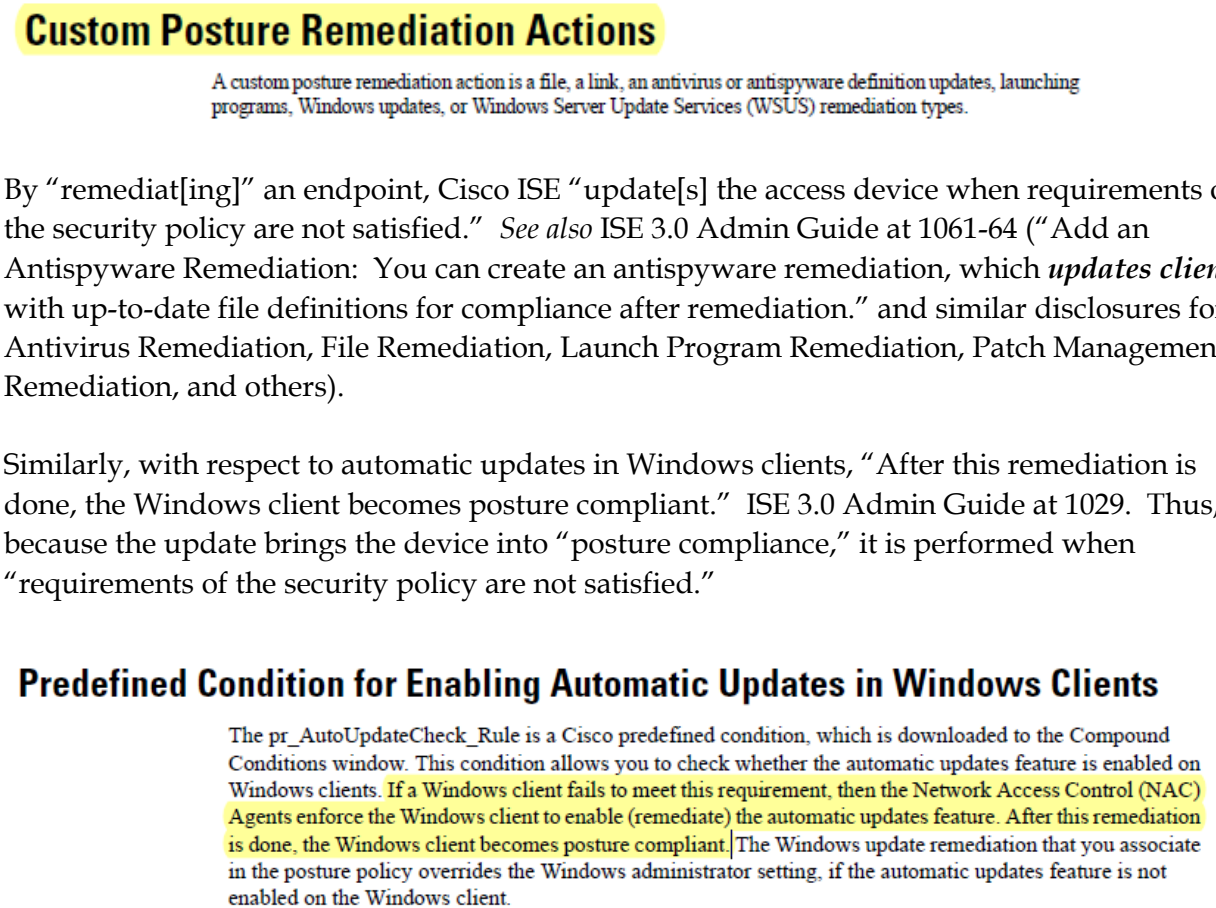
U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	communicate between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port for communicating between the access device and the less-restricted subset."  **Continuous Endpoint Attribute Monitoring** You can use the AnyConnect agent to continuously monitor different endpoint attributes to ensure that dynamic changes are observed during posture assessment. This improves the overall visibility of an endpoint and helps 1102 Cisco Identity Services Engine Administrator Guide, Release 3.0 Compliance Cisco Web Agent you create posture policies based on their behavior. The AnyConnect agent monitors applications that are installed and running on an endpoint. You can turn on and off the feature and configure how often the data should be monitored. By default, data is collected every 5 minutes and is stored in the database. During initial posture, AnyConnect reports a complete list of running and installed applications. After initial posture, the AnyConnect agent scans the applications every X minute and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications. ISE 3.0 Admin Guide at 1102-03.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

27. The non-transitory computer readable storage medium of claim 16, wherein the program is further executable to update the access device when requirements of the security policy are not satisfied.	Cisco provides or sells "[t]he non-transitory computer readable storage medium of claim 16, wherein the program is further executable to update the access device when requirements of the security policy are not satisfied." Cisco ISE contains "Posture Remediation Options," and also "Custom Posture Remediation Actions," which include "a file, a link, an antivirus or antispyware definition ***updates***, launching programs, Windows updates, or Windows Server Update Services (WSUS) remediation types." ISE 3.0 Admin Guide at 1059, 1061. **Posture Remediation Options** The following table provides a list of posture remediation options that are supported by the Cisco ISE Posture Agents for Windows and Macintosh, and the Web Agent for Windows. ***Table 162: Posture Remediation Options*** **ISE Posture Agent for Windows** / **ISE Posture Agent for Macintosh OS X** Message Text (Local Check) / Message Text (Local Check) URL Link (Link Distribution) / URL Link (Link Distribution) File Distribution / — Launch Program / — Antivirus Definition Update / Antivirus Live Update Antispyware Definition Update / Antispyware Live Update Patch Management Remediation (AC 4.1 - and ISE 1.4) / — Windows Update / — WSUS / —

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)



Custom Posture Remediation Actions

A custom posture remediation action is a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) remediation types.

By "remediat[ing]" an endpoint, Cisco ISE "update[s] the access device when requirements of the security policy are not satisfied." *See also* ISE 3.0 Admin Guide at 1061-64 ("Add an Antispyware Remediation: You can create an antispyware remediation, which ***updates clients*** with up-to-date file definitions for compliance after remediation." and similar disclosures for Antivirus Remediation, File Remediation, Launch Program Remediation, Patch Management Remediation, and others).

Similarly, with respect to automatic updates in Windows clients, "After this remediation is done, the Windows client becomes posture compliant." ISE 3.0 Admin Guide at 1029. Thus, because the update brings the device into "posture compliance," it is performed when "requirements of the security policy are not satisfied."

Predefined Condition for Enabling Automatic Updates in Windows Clients

The pr_AutoUpdateCheck_Rule is a Cisco predefined condition, which is downloaded to the Compound Conditions window. This condition allows you to check whether the automatic updates feature is enabled on Windows clients. If a Windows client fails to meet this requirement, then the Network Access Control (NAC) Agents enforce the Windows client to enable (remediate) the automatic updates feature. After this remediation is done, the Windows client becomes posture compliant. The Windows update remediation that you associate in the posture policy overrides the Windows administrator setting, if the automatic updates feature is not enabled on the Windows client.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	See also ISE 3.0 Admin Guide at 1048-50 (Patch Management Condition Settings):

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

Patch Management Condition Settings

The following table describes the fields in the **Patch Management Conditions** window. To view this window, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Patch Management Condition**.

Table 157: Patch Management Condition

Field Name	Usage Guidelines
Name	Enter the name of the patch management condition.
Description	Enter a description for the patch management condition.
Operating System	Choose an operating system to check the installation of a patch management software on the endpoint, or check the latest patch management definition file updates to which the condition is applied. You can select the Windows OS or macOS. You can also select more than one version of an operating system to create the patch management condition.
Vendor Name	Choose a vendor from the **Vendor Name** drop-down list. Based on your selection, the patch management products and their supported versions, check type, and minimum compliant module support details are displayed in the **Products for Selected Vendor** table. The list in the table changes according to the selected operating system.

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

Field Name	Usage Guidelines
Check Patches Installed	(Available only when you select the **Up To Date** check type) You can configure severity levels for missing patches, which are then deployed based on the severity. Choose one of the following options: • **Critical Only**: To check if critical software patches are installed on the endpoints in your deployment. • **Important and Critical**: To check if important and critical software patches are installed on the endpoints in your deployment. • **Moderate, Important, and Critical**: To check if moderate, important, and critical software patches are installed on the endpoints in your deployment. • **Low To Critical**: To check if low, moderate, important, and critical software patches are installed on the endpoints in your deployment. • **All**: To install the missing patches for all severity levels.

and also Randomized Changing MAC at 44 ("Cisco ISE performs the following functions with the external MDM server: . . . Handles device remediation: Endpoints are granted restricted access during remediation."); *and also* ISE Data Sheet at 4 ("Automated device-compliance checks for device-posture and ***remediation*** options using Cisco Secure Client (formerly Anyconnect agent), Temporal and Agentless options . . ." and 7 ("Supports automatic ***remediation*** of PC clients as well as periodic reassessments . . .")

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

Automated device-compliance checks for device-posture and remediation options using Cisco Secure Client (formerly Anyconnect agent), Temporal and Agentless options with custom scripts support. Cisco Secure Client Temporal and Agentless are two different ways to gather posture from endpoints beyond a full agent. Agentless option is supported from ISE 3.0 onwards Io Cisco Secure client also provide advanced VPN services for desktop and laptop checks. ISE also integrates with market-leading Mobile Device Management/Enterprise Mobility Management (MDM/EMM) vendors. MDM integration helps ensure that a mobile device is both secure and policy compliant before it is given access to the network.

. . .

Endpoint posture service	• Performs posture assessments to endpoints connected to the network.
	• Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM.
	• Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media.
	• Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies.
	• Provides hardware inventory for full network visibility.
	• Requires the AnyConnect 4.x agent for posture assessment on these OS platforms:
	  ◦ Windows 10 and later
	  ◦ Mac OS X 10.13 and later
	  ◦ Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu)

ISE Data Sheet at 4, 7.

EXHIBIT F-3

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

U.S. Patent No. 8,677,450	Cisco's Identity Services Engine
[Claim 1—preamble] A method for applying a security policy to network devices, the method comprising:	Cisco infringes this claim by making, using, testing, offering for sale, and selling the Identity Services Engine ("ISE") product and system and through performance of each of the claimed steps and/or providing instructions and data from its servers to third-parties to perform at least one of the claimed steps. Further, subsequent to Cisco's making, using, testing, offering for sale, and selling of the ISE, Cisco offers services to third-parties and customers with respect to the ISE. For example, these can include "Technical Services," "Advisory Services," and "Cisco Talos Incidence Response" services. (https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/ise-licensing-guide-og.html). For technical services, for example, Cisco encourages customers to purchase "Cisco Smart Net Total Care" for Cisco ISE physical appliances and Software Support (SWSS) contracts for Cisco ISE virtual machines. For advisory services, Cisco offers Expert Services to address "your business objectives with the technology we offer" (including ISE). *Id*. And for the Talos Incident Response, Cisco provides a full suite of proactive and emergency services to help third-parties prepare, respond, and recover from a cybersecurity breach. Cisco explains that third-parties can "order and transact Cisco Talos Incident Response when ordering Cisco ISE subscriptions." *Id*. Additionally, and as set forth in InfoExpress's 3-1 disclosures, Cisco's ISE also includes Cisco's ISE (NAC) appliance. Specifically, these are Cisco-provided tangible hardware and "virtual appliances" on which ISE can be deployed. A list of accused ISE (NAC) Appliances (also referred to as "hardware platforms") which ISE supports, are disclosed in InfoExpress's Disclosure of Asserted Claims and Infringement Contentions per Patent L.R. 3-1 and 3-2 at Section II.B.2. These ISE (NAC) Appliances are listed in Cisco's Identity Services Engine Administrator Guides, for

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0001603 to 0014308, and also their Release Notes for ISE Releases 1.04, 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014606 to 0015185. Cisco's ISE (NAC) appliances are directed to "[g]ranting and denying network access" and using "attributes related to users and their devices" in "determining authorized network access." https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/datasheet-c78-726524.html.[1] Cisco further explains that its NAC appliance (known in one example as "The Cisco Secure Network Server") "supports Cisco's powerful network access and control security applications." *Id*. Further, Cisco explains that the "Cisco Secure Network Server… is configured specifically to support the Cisco Identity Services Engine (ISE) security application." *Id*. To the extent the preamble is limiting, Cisco's ISE[2] is "a security policy management platform that provides secure access to network resources" and thereby "appl[ies] a security policy to network devices."

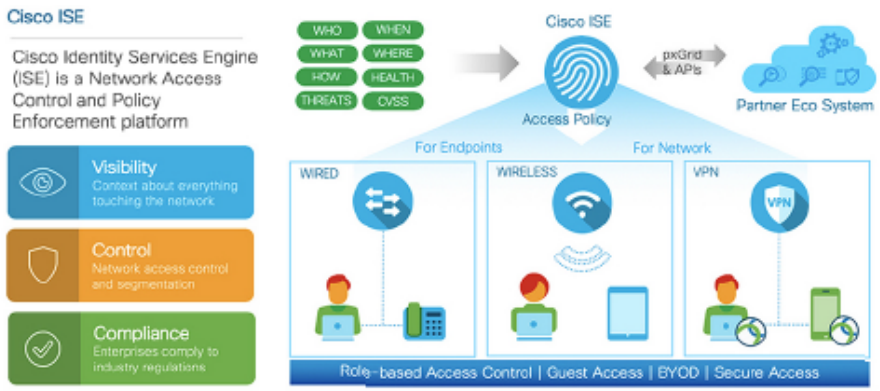
[1] Certain portions of the evidence cited herein identify and relate to the "Cisco Secure Network Server Data Sheet" for Cisco SNS-3715, SNS-3755, and SNS-3795 Secure Network Server. We understand that each other version of the Accused Technology relating to the Cisco ISE (NAC) appliances including ISE-3315-K9, ISE-3355-K9, and ISE-3395-K9; SNS-3415-K9 and SNS-3495-K9; SNS -3515-K9 and SNS-3595-K9; SNS-3615-K9, SNS-3655-K9, and SNS-3695-K9; and ISE Virtual Machine (S/M/L)-K9 are operationally and functionally the same with respect to and for the purposes of identifying infringement for each of the Asserted Claims.

[2] Certain portions of the evidence cited herein identify and relate to the Cisco Identity Services Engine, Release 3.0. We understand that each version of the Accused Technology is operationally and functionally similar with respect to and for infringement of each of the Asserted Claims.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Introduction to Cisco Identity Services Engine Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, wireless controllers, Virtual Private Network (VPN) gateways, 5GaaS networks, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation. Cisco ISE is available on secure network server appliances with different performance characterizations, and also as software that can be run on a virtual machines (VMs). Note that you can add more appliances to a deployment for better performance. Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also enables the configuration and management of distinct personas and services, thereby giving you the ability to create and apply services, where needed, in a network, but operate the Cisco ISE deployment as a complete and coordinated system. For detailed Cisco ISE ordering and licensing information, see the *Cisco Identity Services Engine Ordering Guide*. Release Notes for Cisco Identity Services Engine, Release 3.0 ("ISE 3.0 Release Notes") at 1, *available at* https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/release_notes/b_ise_30_rn.pdf (last visited May 31, 2023) *See also* Cisco Identity Services Engine Administrator Guide, Release 3.0 ("ISE 3.0 Admin Guide"), at 1, available at https://www.cisco.com/c/en/us/ td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Cisco ISE Overview  Cisco Identity Services Engine (ISE) is an identity-based network access control and policy enforcement system. It functions as a common policy engine that enables endpoint access control and network device administration for enterprises. You can leverage Cisco ISE to ensure compliance, enhance infrastructure security, and streamline service operations. A Cisco ISE administrator can gather real-time contextual data for a network, including users and user groups (who?), device type (what?), access time (when?), access location (where?), access type (wired, wireless, or VPN) (how?), and network threats and vulnerabilities.
[1-a] performing an authentication of a device connected to an access point;	Cisco's ISE "perform[s] authentication of a device connected to an access point[,]" and induces others to do so. Cisco's ISE "performs authentication" of a device (which Cisco terms an "endpoint"). Cisco explains how its ISE "***uses*** a wide range of ***authentication protocols*** to provide network devices

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods." By "using [an] authentication protocol" on an endpoint (a "device connected to an access point"), Cisco "perform[s] authentication of a device connected to an access point[.]" • **Bring Your Own Device (BYOD)**: Cisco ISE allows your employees and guests to securely use their personal devices on your enterprise network. BYOD feature end users can use configured pathways to add their devices, and provision predefined authentications and levels of network access. • **Asset Visibility**: Cisco ISE gives you visibility and control over who and what is on your network consistently, across wireless, wired, and VPN connections. Cisco ISE uses probes and device sensors to listen to the way devices connect to the network. The Cisco ISE profile database, which is extensive, then classifies the device. This gives the visibility and context you need to grant the right level of network access. • **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods. • **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation. *See generally* Cisco Identity Services Engine Administrator Guide, Release 3.0 ("ISE 3.0 Admin Guide"), at 2, available at https://www.cisco.com/c/en/us/ td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf (last visited May 31, 2023); *see also id.* (explaining that for the TACACS+ security protocol, "Network devices can be configured to query Cisco ISE for ***authentication and authorization of device administrator actions***."); *id.* (explaining that for ISE's bring-your-own-device (BYOD) feature, "end users can use configured pathways to add their

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	devices, and ***provision predefined authentications and levels of network access***."); *see also id.* at 183 ("UTF-8 Credential ***Authentication***"), 214 ("Wildcard Certificates for HTTPS and ***Extensible Authentication Protocol*** Communication"), 268 (Configure Cisco ISE to Use Certificates for ***Authenticating*** Personal Devices); 269 (Create a Certificate ***Authentication*** Profile for TLS-Based Authentication); 270 (Create an Identity Source Sequence for ***TLS-Based Authentication***); (275 (Configure the ***Dot1X Authentication Policy*** Rule for TLS-Based Authentication); 276 ("Create Authorization Profiles for ***CentralWeb Authentication*** and Supplicant-Provisioning Flows"); 278-79 ("This section lists the authorization profiles that you must create for enabling ***certificate-based authentication*** in Cisco ISE. You must have already created the ACLs (NSP-ACL and NSP-ACL-Google) on the wireless LAN controller (WLC)."); 280 (Cisco ISE CA Issues Certificates to [Adaptive Security Appliance ("ASA")] VPN Users) ("The ASA requests ***certificate-based authentication*** from the client. . . . The ASA proceeds to primary user ***authentication (AAA)*** using the username/ password and passes the information to the ***authentication server (ISE)***."); 354 (discussing exemplary "***authentication method[s]*** that [are] used by the RADIUS protocol"); 428-29 (Guest Access Web Authentication Options); 429-30 (Network Access Devices with Central Web Authentication Process, "In this scenario, the network access device (NAD) makes a new authorization request to the Cisco ISE RADIUS server from an unknown endpoint connection. The endpoint then receives a url-redirect to Cisco ISE. . . . If the guest device is connected to a NAD, the guest service interaction takes the form of a ***MAC Authentication Bypass (MAB) request*** that leads to a Guest portal Central WebAuth login. The following is an outline of the subsequent ***Central Web Authentication (Central WebAuth)*** process, which applies to both wireless and wired network access devices."); 430-31 (Wireless LAN Controller with ***Local Web Authentication*** Process); 431 (Wired Network Access Device with ***Local Web Authentication Process***); 433-34 (Device Registration ***Web Authentication*** Process); 512 ("In Cisco ISE, you can ***authenticate administrators*** via an external identity store such as Active Directory, LDAP, or RSA SecureID."); 513 (***External Authentication*** and Authorization); 635 ("Cisco ISE can ***authenticate*** a subject (user or host) against

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	an [Lightweight Directory Access Protocol ('LDAP')] identity source . . ."); 862 (Password-Based Authentication); 1183 (Enable Your Switch to Support ***StandardWeb Authentication***); 1186 (Enable ***802.1X Port-Based Authentication*** for Switch Ports and Enable EAP for Critical Authentications); 1188-90 (Enable Switch Ports for 802.1X and [***MAC Authentication Bypass ("MAB")***]); 1232-38 ("Live Authentications: "You can monitor recent ***RADIUS authentications*** as they occur . . ."). Cisco also explains that its ISE uses "***policy sets*** [with which] you [] manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group ***authentication and authorization policies*** within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type, and similar parameters." Cisco further explains that "[w]hen creating policy sets, you can configure the rules (configured with condition and results in order to choose . . . the identity sources on the ***authentication policy*** level[.]" Cisco further explains that hierarchically, authentication policy rules are applied first and before local policy exceptions, global policy exceptions and authorization policy rules. ISE 3.0 Admin Guide at 856.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Policy Sets

Cisco ISE is a policy-based, network-access-control solution, which offers network access policy sets, allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type, and similar parameters. When you install Cisco ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules.

When creating policy sets, you can configure these rules (configured with conditions and results) in order to choose the network access services on the policy set level, the identity sources on the authentication policy level, and network permissions on the authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE-supported dictionaries for different vendors. Cisco ISE allows you to create conditions as individual resuable policy elements.

The network access service to be used per policy set to communicate with the network devices is defined at the top level of that policy set. Network access services include:

- Allowed protocols—the protocols configured to handle the initial request and protocol negotiation.
- A proxy service—sends requests to an external RADIUS server for processing.

Note From the **Work Centers** > **Device Administration** , you can also select a relevant TACACS server sequence for your policy set. Use the TACACS server sequence to configure a sequence of TACACS proxy servers for processing.

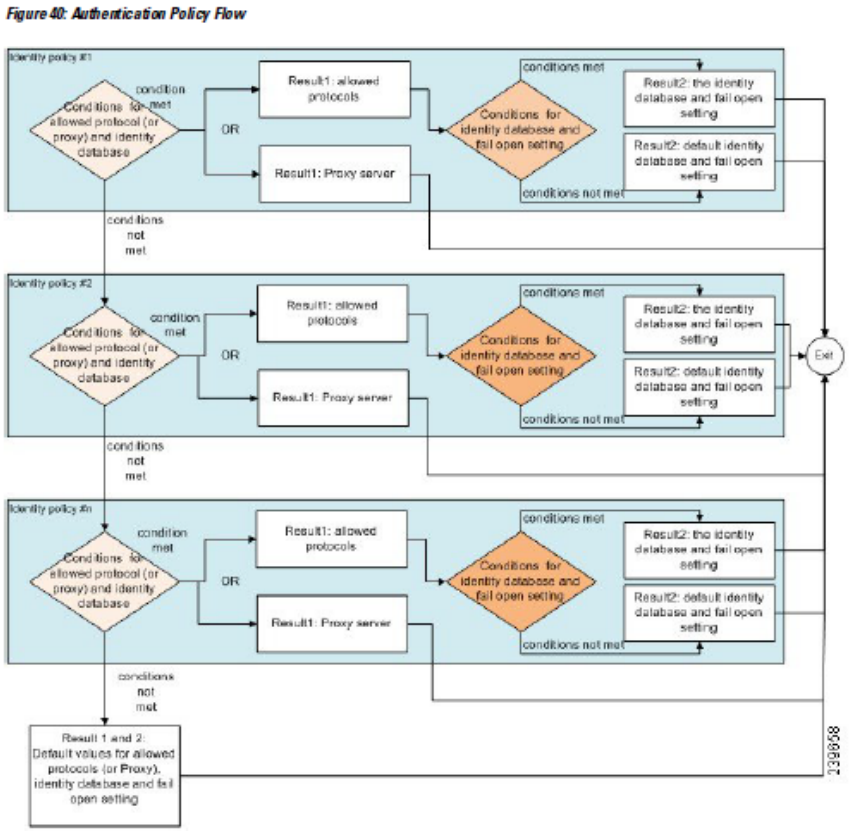
Policy sets are configured hierarchically, where the rule on the top level of the policy set, which can be viewed from the **Policy Set** table, applies to the entire set and is matched before the rules for the rest of the policies and exceptions. Thereafter, rules of the set are applied in this order:

1. Authentication policy rules
2. Local policy exceptions
3. Global policy exceptions
4. Authorization policy rules

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Cisco further explains that "Each policy set can contain ***multiple authentication rules*** that together represent the authentication policy for that set. Priority of the authentication policies is determined based on the order to those policies as they appear within the policy set itself[.]" **Authentication Policies** Each policy set can contain multiple authentication rules that together represent the authentication policy for that set. Priority of the authentication policies is determined based on the order to those policies as they appear within the policy set itself (from the Set view page in the Authentication Policy area). Cisco ISE dynamically chooses the network access service (either an allowed protocol a server sequence) based on the settings configured on the policy set level, and thereafter checks the identity sources and results from the authentication and authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE dictionary. Cisco ISE allows you to create conditions as individual policy elements that can be stored in the Library and then can be reused for other rule-based policies. The identity method, which is the result of the authentication policy, can be any one of the following: . . .

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)



ISE 3.0 Admin Guide at 858-59; *see also id.* at 860 (Configure Authentication Policies: Define an authentication policy per policy set by configuring and maintaining multiple authentication rules, as necessary.").

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Cisco also explains that with its mobile device management (MDM) server integration with ISE, one can "perform authentication" using a Device Unique ID/Global Unique ID (DUID/GUID).

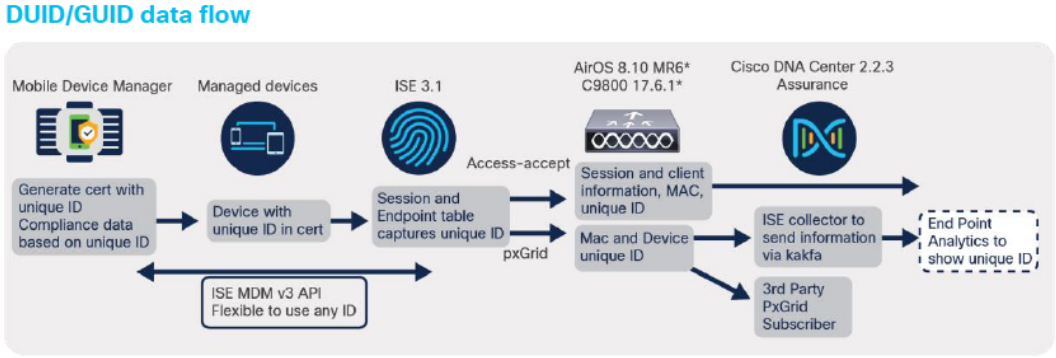


Figure 4.
DUID/GUID data flow

- This solution relies on the mobile device manager, also referred to as a device manager or unified endpoint manager (for example, Cisco Meraki, Airwatch, Intune, MobileIron, etc.), which manage devices in an enterprise infrastructure.
- ISE provides the provisioning of the device with the unique ID-based (DUID) certificates.
- The device presents this certificate during TLS-based authentication. ISE authorizes the devices and also reads the unique ID from the certificate.
- The DUID is used for compliance check with MDM servers and also a unique identifier of the device in the endpoint table.
- The randomized MAC address will not matter, as now the device will have a DUID using the ID in the certificate.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Cisco, Randomized and Changing MAC Deployment Guide (2022) at 42, https://www.cisco.com/c/en/us/products/collateral/wireless/randomized-changing-mac-dg.pdf (last visited June 27, 2023). **Handle random and changing MAC addresses with an MDM server** To avoid issues caused by the use of the MAC address randomization method, configure Cisco ISE to identify endpoints that are connected to an MDM server by a unique device identifier instead of a MAC address. Mobile devices increasingly use random and changing MAC addresses for each SSID. This means that an endpoint presents different MAC addresses to the MDM server and to Cisco ISE. As a result, when the MDM server and Cisco ISE are integrated and an action is initiated for an endpoint, issues arise because the endpoint's identity is different in the two systems. In Cisco ISE, you can now work around this problem by configuring Cisco ISE to use a unique device identifier instead of MAC addresses. When an endpoint enrolls with an MDM server, the MDM server sends a certificate with a GUID value to the endpoint. The endpoint uses this certificate for authentication with Cisco ISE. Cisco ISE receives the GUID for the endpoint from the certificate. All communications between Cisco ISE and the MDM server now use the GUID to identify the endpoint, helping ensure accuracy and consistency between the two systems. Note that GUIDs are available only in certificate-based authentication methods. Basic authentication methods that use only a username and password will not be able to leverage the GUID-based solution. The Cisco ISE MDM APIs have been updated (Cisco ISE MDM APIs Version 3) to facilitate the gathering and management of GUID data. Currently, MobileIron supports Cisco ISE MDM APIs Version 3, and sends GUID information to Cisco ISE. Randomized and Changing MAC Deployment Guide at 48. • **Time Interval for Compliance Device ReAuth Query:** When an endpoint is authenticated or reauthenticated, Cisco ISE uses a cache to get the MDM variables for that endpoint. If the age of the cached value is higher than the value configured in this field, Cisco ISE sends a new device query to the MDM server to get new values. If the compliance status has changed, Cisco ISE triggers the appropriate CoA. Randomized and Changing MAC Deployment Guide at 50. Furthermore, Cisco "perform[s] an authentication of a device connected to an access point[.]"

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	In Cisco's Randomized Changing MAC, it describes generally (in the text and also the schematic) how mobile devices (the claimed "devices") connect to the network through "switches, access routers, wireless access points, and other network access points" (the claimed "access points"). Randomized Changing MAC at 43.

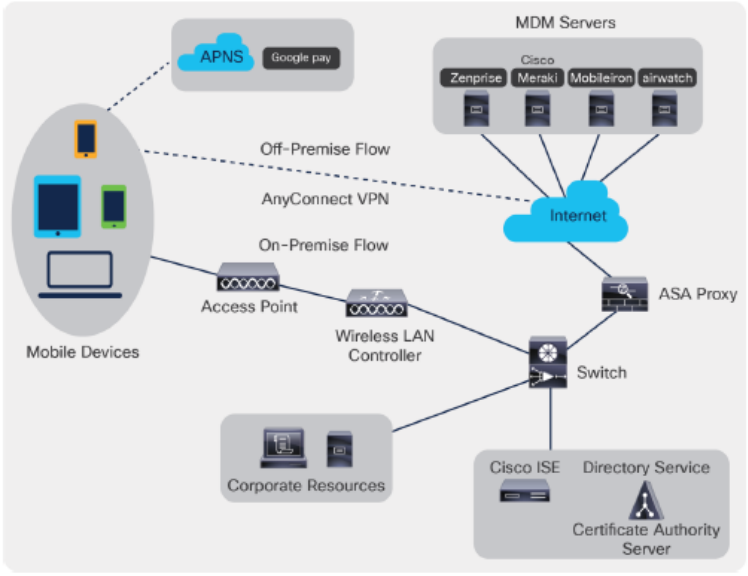


Figure 5.
Cisco ISE and MDM servers

You can configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. It then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Cisco makes, uses, sells, and offers for sale a variety of ISE-validated products which customers oftentimes require with its ISE solutions including wireless access points, switches, LAN controllers, routers, servers, and remote access devices. A list of "access points" that are compatible with its ISE—including switches, routers, and remote access devices (i.e. firewalls)—is listed in Cisco's Identity Services Engine Network Component Compatibility documents, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014309 to INFOEX-CSCO_0014605. These Cisco documents describe "Cisco Identity Services Engine (ISE) validated compatibility with switches, wireless LAN controllers, and other policy enforcement devices as well as operating systems with which Cisco ISE interoperates." INFOEX-CSCO_0014586 at 14586. They further state, with respect to "Validated Network Access Devices," that "Cisco ISE supports interoperability with any Cisco or non-Cisco RADIUS client network access device (NAD) that implements common RADIUS behavior (similar to Cisco IOS 12.x) for standards-based authentication." INFOEX-CSCO_0014586 at 14587. These Cisco documents identify the claimed "access points" including both Cisco-made and third-party access points. Cisco also describes ISE-compatible third-party devices in its ISE 3.0 Admin Guide at 806-07, including those made by Aruba, Motorola, HP, Ruckus, Alcatel, Brocade, and Juniper. *See also* ISE 3.0 Admin Guide at 430 ("The [Wireless LAN Controller ("WLC")] can now log the guest in via the Cisco ISE RADIUS server. When this is complete, the WLC redirects the guest device's browser to the original URL destination. The Wireless LAN Controller (WLC) and the network access devices (NAD) requirements to support the original URL redirect for guest portals are WLC 5760 and ***Cisco Catalyst 3850, 3650, 2000, 3000, and 4000 Series Access Switches*** running releases IOS-XE 3.6.0.E and 15.2(2)E."); 874 (Cisco AI Endpoint Analytics receives endpoint attribute data from multiple sources, such as ***Cisco Catalyst 9000 Series devices***[.]"); 697 ("The following devices support sending [Manufacturer Usage Descriptor ("MUD")] data to Cisco ISE: Cisco Catalyst 3850 Series Switches running Cisco IOS XE Version 16.9.1 & 16.9.2[,] Cisco Catalyst

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Digital Building Series Switches running Cisco IOS Version 15.2(6)E2[, and] Cisco Industrial Ethernet 4000 Series Switches running Cisco IOS Version 15.2(6)E2[.]"); 788 ("Cisco TrustSec-enabled devices use the TrustSec attributes to communicate with Cisco ISE. Cisco TrustSec-enabled devices, such as the Cisco Nexus 7000 Series Switches, Cisco Catalyst 6000 Series Switches, Cisco Catalyst 4000 Series Switches, and Cisco Catalyst 3000 Series Switches are authenticated using the Cisco TrustSec attributes that you define while adding Cisco TrustSec devices.").
[1-b] scanning the device to collect information regarding the device;	Cisco "scan[s] the device to collect information regarding the device[,]" and induces others to do so. By way of one example, ISE can "scan[] the device to collect information regarding the device" by using an agent that resides on the device. For example, the AnyConnect agent "can read the posture profile" (that is, it can "scan the device to collect information regarding the device.") ISE 3.0 Admin Guide at 1010-11. Similarly, the Temporal Agent "checks the compliance status" of a device, thereby "scanning the device to collect information regarding the device."

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Posture Types

The following posture agents monitor and enforce Cisco ISE posture policies:

- **AnyConnect**: Deploys the AnyConnect agent to monitor and enforce Cisco ISE posture policies that require interaction with the client. The AnyConnect agent stays on the client. For more information about using AnyConnect in Cisco ISE, see Cisco AnyConnect Secure Mobility, on page 1099.
- **AnyConnect Stealth**: Runs posture as a service, with no user interface. The agent stays on the client.

  When you choose the AnyConnect Stealth posture type in the posture requirement, some of the conditions, remediations, or attributes in a condition are disabled (grayed out). For example, when you enable AnyConnect Stealth requirement, the Manual Remediation Type is disabled (grayed out) because this action requires client-side interaction.

  When you map the posture profile to the AnyConnect configuration, and then map the AnyConnect configuration to the Client Provisioning window for AnyConnect Stealth mode deployment:

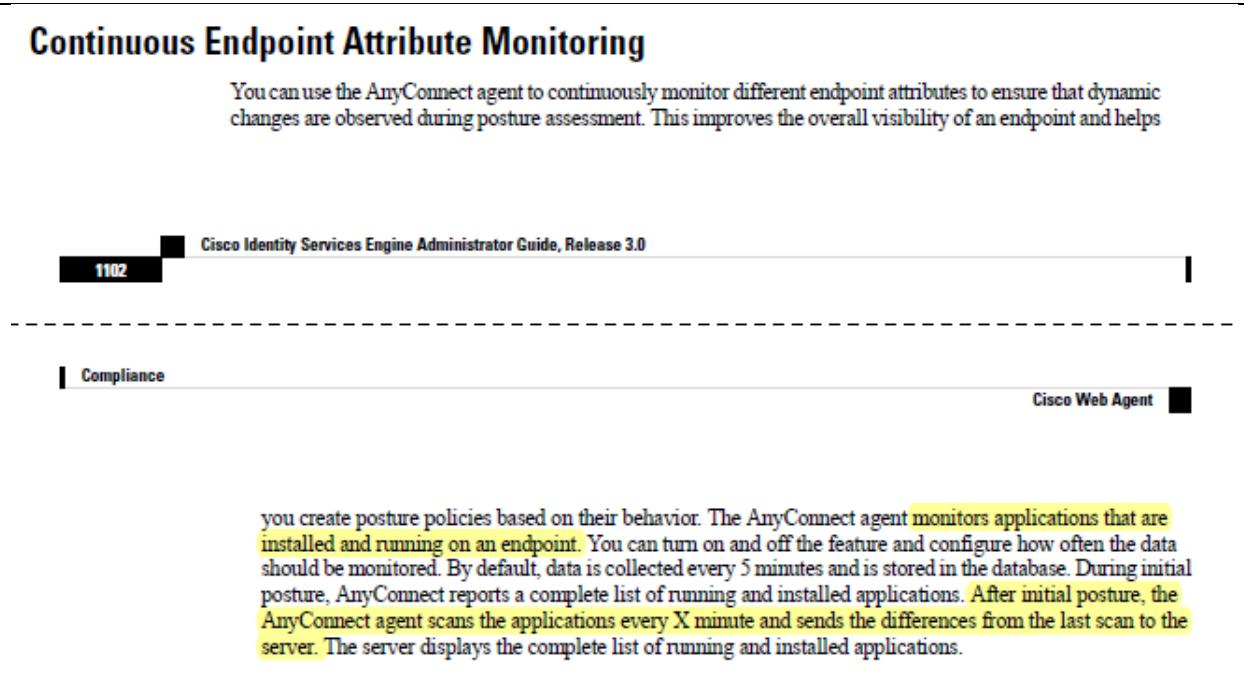
  - AnyConnect can read the posture profile and set it to the intended mode.
  - AnyConnect can send information related to the selected mode to Cisco ISE during the initial posture request.
  - Cisco ISE can match the right policy, based on the mode and other factors, such as identity group, OS, and compliance module.

. . . .

- **Temporal Agent**: When a client attempts to access the trusted network, Cisco ISE opens the Client Provisioning portal. The portal instructs the user to download and install the agent, and run the agent. The temporal agent checks the compliance status, and sends the status to Cisco ISE. Cisco ISE acts based on the results. The temporal agent removes itself from the client after compliance processing completes. The temporal agent does not support custom remediation. The default remediation supports only message text.

ISE 3.0 Admin Guide at 1010-11; *see also id.* at 1102-03 (Continuous Endpoint Attribute Monitoring mode, whereby for initial posture assessment, the AnyConnect Agent "reports a complete list of running and installed applications" on the access device, after which it "***scans*** the applications [on the access device] every X minute and sends the differences from the ***last scan*** to the server").

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)



Continuous Endpoint Attribute Monitoring

You can use the AnyConnect agent to continuously monitor different endpoint attributes to ensure that dynamic changes are observed during posture assessment. This improves the overall visibility of an endpoint and helps

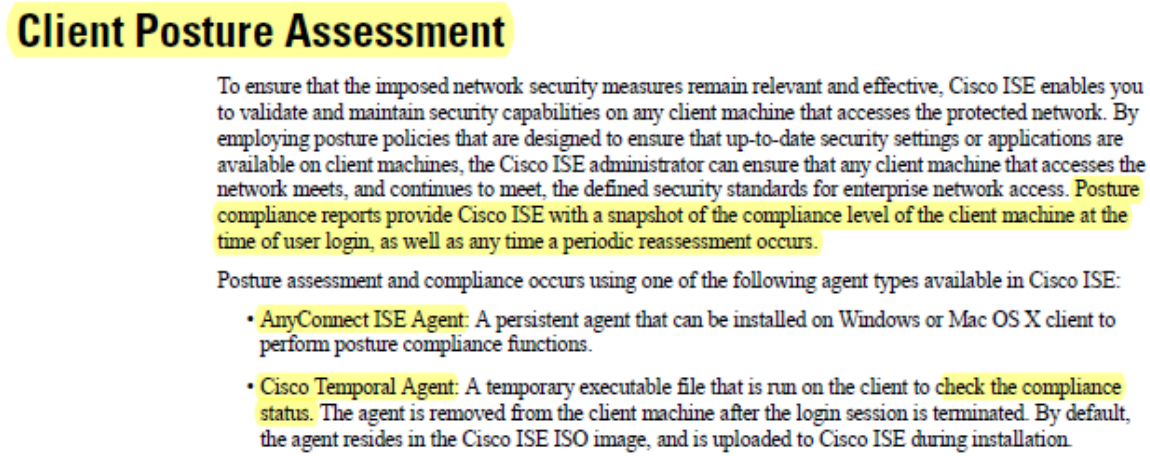
Compliance

Cisco Web Agent

you create posture policies based on their behavior. The AnyConnect agent monitors applications that are installed and running on an endpoint. You can turn on and off the feature and configure how often the data should be monitored. By default, data is collected every 5 minutes and is stored in the database. During initial posture, AnyConnect reports a complete list of running and installed applications. After initial posture, the AnyConnect agent scans the applications every X minute and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications.

ISE 3.0 Admin Guide at 1102-03.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)



Client Posture Assessment

To ensure that the imposed network security measures remain relevant and effective, Cisco ISE enables you to validate and maintain security capabilities on any client machine that accesses the protected network. By employing posture policies that are designed to ensure that up-to-date security settings or applications are available on client machines, the Cisco ISE administrator can ensure that any client machine that accesses the network meets, and continues to meet, the defined security standards for enterprise network access. Posture compliance reports provide Cisco ISE with a snapshot of the compliance level of the client machine at the time of user login, as well as any time a periodic reassessment occurs.

Posture assessment and compliance occurs using one of the following agent types available in Cisco ISE:

- AnyConnect ISE Agent: A persistent agent that can be installed on Windows or Mac OS X client to perform posture compliance functions.
- Cisco Temporal Agent: A temporary executable file that is run on the client to check the compliance status. The agent is removed from the client machine after the login session is terminated. By default, the agent resides in the Cisco ISE ISO image, and is uploaded to Cisco ISE during installation.

See also ISE 3.0 Admin Guide at 1057 ("Cisco Temporal Agent [is] a temporary executable file that is run on the client ***to check the compliance status***."); *id.* at 1057-58 (list of posture assessment options supported by the Cisco ISE Posture Agents).

Another way by which Cisco's ISE can "scan[] the device to collect information regarding the device" is by obtaining the "hardware attributes of an endpoint." ISE 3.0 Admin Guide at 174; *see also id.* at 174-5 (listing attributes), 176 ("Cisco ISE profiles the hardware attributes of a client's system, however, there may be a few hardware attributes Cisco ISE does not profile. . . . The hardware inventory data collection interval can be controlled . . . The default interval is 5 minutes.")

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Yet another way by which Cisco's ISE can "scan[] the device to collect information regarding the device" is by agentless posture[, which] ***provides posture information from clients***, and completely removes itself when finished, until invoked by Cisco ISE again." ISE 3.0 Admin Guide at 1012. Cisco further describes how in agentless posture mode, "Posture evaluation runs on the client, and ***sends the status to Cisco ISE***." *Id.* at 1013. *See also and also* Cisco Community, *How To: Agentless Posture Configuration, Validation & Troubleshooting* (Oct. 15, 2020), *available at* https://community.cisco.com/t5/security-knowledge-base/how-to-agentless-posture-configuration-validation-amp/ta-p/4152763 (last visited May 31, 2023).
	
	Agentless Posture
	
	Agentless posture provides posture information from clients, and completely removes itself when finished, until invoked by Cisco ISE again. No action is required from the end user.
	
	Requirements
	• The client must be reachable by its IP address, and that IP address must be available in RADIUS accounting. IPv6 is not supported.
	• Windows and Mac clients are currently supported.
	  • For Windows clients, port 5985 to access Powershell on the client must be open. Powershell must be version 5.1 or later. The client must have cURL version 7.34 or later.
	  • For macOS clients, port 22 to access SSH must be open to access the client. The client must have cURL version 7.34 or later.
	
	. . . .

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Agentless Posture Process Flow

1. The client connects to the network.
2. Cisco ISE detects if agentless posture is enabled in the authorization profile used by client.
3. If so, Cisco ISE sends an agentless posture job request to the Cisco ISE Messaging queue.
4. Cisco ISE gets the job from the messaging queue, and starts the agentless posture flow.
5. Cisco ISE connects to the client via power shell or SSH.
6. Cisco ISE pushes the certificate, if it's not already in the client's trust certificate authority store.
7. Cisco ISE runs the client provisioning policy.
8. Cisco ISE pushes the agentless plug-in to the client and launches the plug-in.
9. Posture evaluation runs on the client, and sends the status to Cisco ISE.
10. Cisco ISE removes the agentless plug-in from the client. Logs of the posture flow remain on the client for 24 hours, or until the client deletes them.

ISE 3.0 Admin Guide at 1012-13.

By way of one example—Easy Connect Enforcement Mode—Cisco describes how "[t]he user logs in to the domain and a security audit event is sent to Cisco ISE[,]" and then "ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event." ISE 3.0 Admin Guide at 580-82. Because ISE collects certain information about a device seeking to connect, it "scan[s] the device to collect information regarding the device[.]"

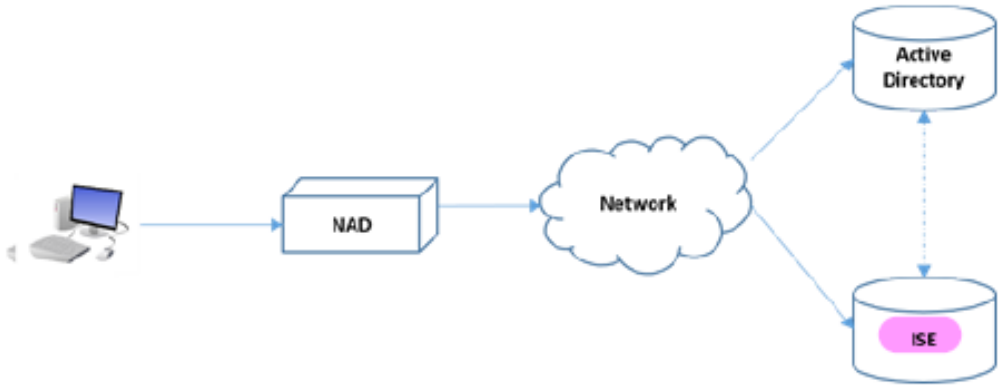
U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Easy Connect Enforcement Mode Process Flow

The Easy Connect Enforcement mode process is as follows:

1. The user connects to the NAD from a wired endpoint (such as a PC for example).
2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD.
3. The user logs in to the domain and a security audit event is sent to Cisco ISE.
4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event.
5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy.

Figure 20: Easy Connect Enforcement Mode Basic Flow



U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	See also ISE 3.0 Admin Guide at 401 (describing how, in Guest Device Compliance, ISE requires guests "to first download the posture agent ***that checks their posture profile*** and verifies if their device is compliant"—and thus "scan[s] the device to collect information regarding the device").

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Guest Device Compliance When guests and non-guests access the network through credentialed Guest portals, you can check their devices for compliance before they are allowed to gain access. You can route them to a Client Provisioning window and require them to first download the posture agent that checks their posture profile and verifies if their device is compliant. You can do this by enabling the option in the **Guest Device Compliance Settings** in a credentialed Guest portal, which displays the Client Provisioning window as part of the guest flow. **Note** Client posture assessment in guest flow supports only the Temporal agent. The Client Provisioning service provides posture assessments and remediations for guests. The Client Provisioning portal is available only with a Central Web Authorization (CWA) guest deployment. The guest login flow performs a CWA, and the credentialed Guest portal is redirected to the Client Provisioning portal after performing acceptable-use-policy and change-password checks. The posture subsystem performs a Change of Authorization (CoA) on the network access device to reauthenticate the client connection once the posture has been assessed. ISE 3.0 Admin Guide at 401.
[1-c] applying a security policy, the security policy including one or more requirements pertaining to the authentication and the information,	Cisco "appl[ies] applying a security policy, the security policy including one or more requirements pertaining to the authentication and the information, the application of the security policy taking place in response to a gatekeeper" and induces others to do so. Cisco explains that "Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods."

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

the application of the security policy taking place in response to a gatekeeper, and	Separate and apart from authentication, Cisco describes how "Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the ***appropriate posture agents*** for posturing services." Thus, Cisco "appl[ies] a security policy" one which includes one or more requirements pertaining to the authentication and also the (posture/compliance) information previously obtained in step 1-b. • **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods. • **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation. • **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services. ISE 3.0 Admin Guide at 2. As described above (with respect to an MDM server integrated with ISE), "ISE is the enforcement point[, which] obtains data from the MDM server [and] then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points." Randomized and Changing MAC Deployment Guide at 43. That same guide separately discusses authentication (via device-unique ID (DUID) and/or global-unique ID (GUID) and posture compliance assessment.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Handle random and changing MAC addresses with an MDM server To avoid issues caused by the use of the MAC address randomization method, configure Cisco ISE to identify endpoints that are connected to an MDM server by a unique device identifier instead of a MAC address. Mobile devices increasingly use random and changing MAC addresses for each SSID. This means that an endpoint presents different MAC addresses to the MDM server and to Cisco ISE. As a result, when the MDM server and Cisco ISE are integrated and an action is initiated for an endpoint, issues arise because the endpoint's identity is different in the two systems. In Cisco ISE, you can now work around this problem by configuring Cisco ISE to use a unique device identifier instead of MAC addresses. When an endpoint enrolls with an MDM server, the MDM server sends a certificate with a GUID value to the endpoint. The endpoint uses this certificate for authentication with Cisco ISE. Cisco ISE receives the GUID for the endpoint from the certificate. All communications between Cisco ISE and the MDM server now use the GUID to identify the endpoint, helping ensure accuracy and consistency between the two systems. Note that GUIDs are available only in certificate-based authentication methods. Basic authentication methods that use only a username and password will not be able to leverage the GUID-based solution. The Cisco ISE MDM APIs have been updated (Cisco ISE MDM APIs Version 3) to facilitate the gathering and management of GUID data. Currently, MobileIron supports Cisco ISE MDM APIs Version 3, and sends GUID information to Cisco ISE. Randomized and Changing MAC Deployment Guide at 48.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Step 6. The user registers the device in the MDM server, and the MDM server redirects the request to Cisco ISE through automatic redirection or manual browser refresh.

Step 7. Cisco ISE queries the MDM server again for the posture status.

© 2022 Cisco and/or its affiliates. All rights reserved.

Step 8. If the user's device is not compliant with the posture (compliance) policies that are configured on the MDM server, the user is notified that the device is out of compliance. The user must take the necessary action to ensure that the device is compliant.

Step 9. When the user's device is compliant, the MDM server updates the device's state in its internal tables.

Step 10. If the user refreshes the browser now, the control is transferred back to Cisco ISE.

Step 11. Cisco ISE polls the MDM server once every four hours to get compliance information and issues the appropriate Change of Authorization (CoA). You can configure the polling interval. Cisco ISE also checks the MDM server every five minutes to make sure that it is available.

Randomized and Changing MAC Deployment Guide at 46-47.

Thus, Cisco "appl[ies] a security policy" one which includes one or more requirements pertaining to the authentication and also the (posture/compliance) information obtained in step 1-b.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	In one example, Cisco explains how ISE "appl[ies] a security policy, the security policy including one or more requirements pertaining to the authentication and the information" when it operates with respect to both Cisco and third-party (i.e. non-Cisco) network access devices (NAD) (the claimed "access points"). A guest endpoint (the claimed "device") connects to the network through a third-party ***network access device*** or ***NAD***. ISE applies a security policy. As described in step 3, "Cisco ISE runs the configured authentication and authorization policy"—which is "pertaining to the authentication." Furthermore in step 11, Cisco ISE "validates endpoint compliance" and/or "authorizes the endpoint—which are "pertaining to the . . . the information."

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

ISE 3.0 Admin Guide at 804; *see also id.* at 805-06 (schematics of same).

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Finally, in another example—ISE's Easy Connect Enforcement Mode—ISE "collects the MAC address from RADIUS and the IP address and domain name" ("pertaining to the authentication") and also collects "accounting information (login information) about the user, from the security audit event" ("pertaining to the . . . information"). ISE 3.0 Admin Guide at 581. Furthermore, "[a]fter all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (***based on the appropriate policy managed in the policy service node***), and the user is provided access by the NAD to the network based on that policy." Thus, Cisco "appl[ies] a security policy, the security policy including one or more requirements pertaining to the authentication and the information"

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 770 of 1144
INFOEXPRESS, INC. - EX2572

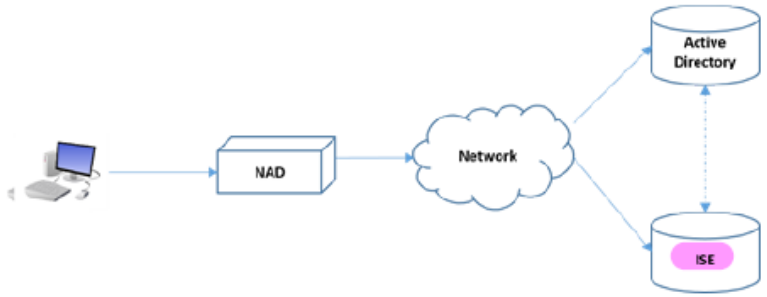
U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Easy Connect Enforcement Mode Process Flow

The Easy Connect Enforcement mode process is as follows:

1. The user connects to the NAD from a wired endpoint (such as a PC for example).
2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD.
3. The user logs in to the domain and a security audit event is sent to Cisco ISE.
4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event.
5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy.

Figure 20: Easy Connect Enforcement Mode Basic Flow



Admin Guide at 580-81.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Finally, "the application of the security policy tak[es] place in response to a gatekeeper[.]" Cisco describes ISE as "a security policy management platform that provides secure access to network resources[.]" ISE gathers certain information from the network, which an administrator can use "to make proactive governance decisions by creating ***access control policies*** for the various network elements, including access switches, wireless controllers, Virtual Private Network (VPN) gateways, 5GaaS networks, and data center switches." Furthermore, "ISE acts as the ***policy manager*** in the Cisco TrustSec solution and supports TrustSec software-defined segmentation[.]" Therefore, because ISE contains a gatekeeper, which "creates" and "manages" security policies, "application of the security policy tak[es] place in response to a gatekeeper[.]"

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Introduction to Cisco Identity Services Engine

Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, wireless controllers, Virtual Private Network (VPN) gateways, 5GaaS networks, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation.

Cisco ISE is available on secure network server appliances with different performance characterizations, and also as software that can be run on a virtual machines (VMs). Note that you can add more appliances to a deployment for better performance.

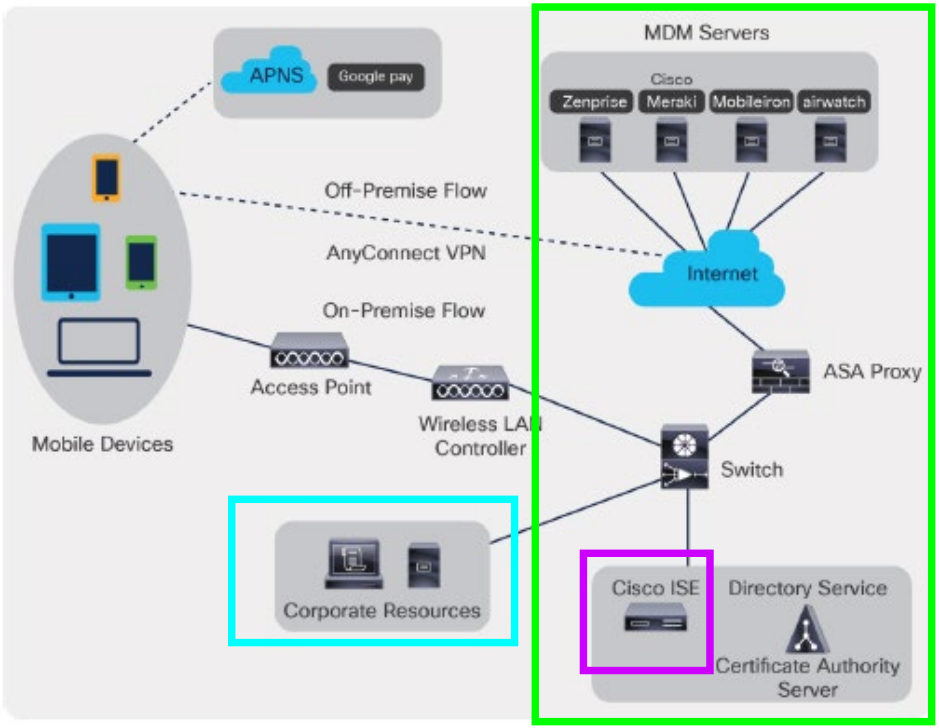
Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also enables the configuration and management of distinct personas and services, thereby giving you the ability to create and apply services, where needed, in a network, but operate the Cisco ISE deployment as a complete and coordinated system.

For detailed Cisco ISE ordering and licensing information, see the *Cisco Identity Services Engine Ordering Guide*.

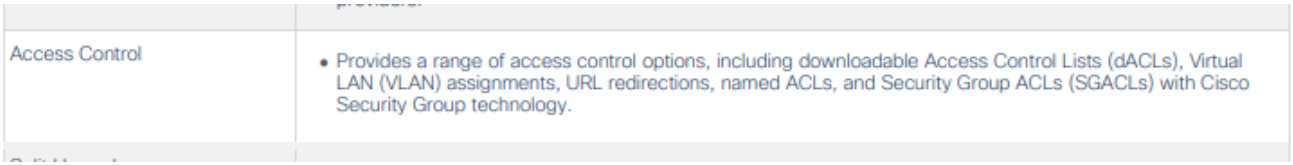
For information on monitoring and troubleshooting the system, see the "Monitoring and Troubleshooting Cisco ISE" section in the *Cisco Identity Services Engine Administrator Guide*.

ISE 3.0 Release Notes at 1, *see also* ISE 3.0 Admin Guide at 1, (further describing ISE as "an identity-based network access control and ***policy enforcement system*** [that] functions as a common policy engine that enables endpoint access control and network device administration[.]")

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

[1-d] configuring the access point in response to a result of applying the security policy.	Cisco "configur[es] the access point in response to a result of applying the security policy[,]" and induces others to do so.  As shown, once ISE applies a security policy, it configures the access point to allow the device access to the network (here, "Corporate Resources)." Randomized Changing MAC at 43; *see also id.* at 57 ("If the device is registered with Cisco ISE, is registered with MDM, and is compliant with

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Cisco ISE and MDM policies, it is ***granted access to the network based on the access control policies configured in Cisco ISE***."). Cisco also describes in its Data Sheet "a range of access control options" for this step, "including downloadable Access Control Lists (dACLs), Virtual LAN (VLAN) assignments, URL redirections, named ACLs, and Security Group ACLs (SGACLs) with Cisco Security Group technology[.]" By using any or all of these methods, ISE "configur[es] the access point in response to a result of applying the security policy[,]"  Cisco Identity Services Engine Data Sheet (2023) ("ISE Data Sheet") at 5, available at https://www.cisco.com/c/en/us/products/security/identity-services-engine/ise-ds.pdf (last visited September 22, 2023). With respect to the example above—involving access points (which included both Cisco and third-party (i.e. non-Cisco) access points)—once ISE determines that "requirements of the security policy are satisfied," it "sends the [change of authorization ("CoA")], authorizes the endpoint, and bypasses the sink hole[,] and then the "the guest user receives the appropriate [network] access based on the CoA." Thus, by sending CoA commands, Cisco ISE "configur[es] the access point in response to a result of applying the security policy."

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

Multiple VLANs may be connected to one network interface card by configuring a VLAN IP helper from the NAD configuration. For more information about configuring an IP helper, see the administration guide for the network device for instructions. For guest access flows that include VLANs with IP helpers, define a guest portal, and select that portal in an authorization profile that is bound to MAB authorization. For more information about guest portals, see the Cisco ISE Guest Services section in *Cisco ISE Admin Guide: Guest and BYOD* .

The following diagram displays a basic network setup when an Auth VLAN is defined (the Auth VLAN is connected directly to a Cisco ISE node).

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	In one further example described above—ISE's Easy Connect Enforcement Mode—ISE collects certain data, after which it "issues a CoA to the [network access device, ("NAD"] (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy." ISE 3.0 Admin Guide at 580-81. By issuing a CoA to the NAD, to provide the user access to the network, Cisco ISE "configur[es] the access point in response to a result of applying the security policy."

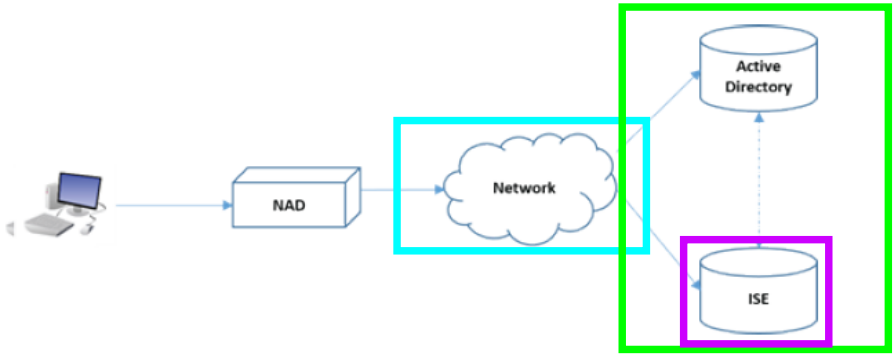
U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Easy Connect Enforcement Mode Process Flow

The Easy Connect Enforcement mode process is as follows:

1. The user connects to the NAD from a wired endpoint (such as a PC for example).
2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD.
3. The user logs in to the domain and a security audit event is sent to Cisco ISE.
4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event.
5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy.

Figure 20: Easy Connect Enforcement Mode Basic Flow



ISE 3.0 Admin Guide at 581.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	In addition to making, using, offering for sale, and selling the ISE, Cisco also induces third-parties to infringe this claim as set forth in InfoExpress's 3-1 disclosures under 35 USC 271(b). For this claim, the underlying direct infringement is caused by the third-parties including Cisco's customers, subscribers, users and developers. And Cisco's acts of induced infringement including the following: as set forth herein, the Release Notes, Admin Guide, Randomized and Changing MAC Deployment Guide and Data Sheets for the ISE are all provided by Cisco to third-parties which provide deliberate and specific instruction and guidance for third-parties to use the ISE in a manner infringed by this claim. In addition, Cisco's Identity Services Engine Administrator Guide ("ISE AG) explains also provide such specific guidance of infringement to third-parties explaining that "[a]dministrators can use the admin portal to: Manage deployments, help desk operations, and network devices, and node monitoring and troubleshooting; Manage Cisco ISE services, policies, administrator accounts, and system configuration and operations." https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/admin_guide/b_ise_admin_3_3/b_ISE_admin_33_overview.html For example, the Admin Guide explains that it's audience can be third party administrators ("Cisco ISE administrators can perform various administrative tasks based on the administrative group to which they belong. These administrators are critical. Grant administrative access only to users who are authorized to administer Cisco ISE in your network" Admin Guide, pg. 13); developers ("On Facebook, create a Facebook application: a) Log on to http://developers.facebook.com and sign up as a developer," Admin Guide, pg. 398), and it instructs these third-parties on configuring the ISE, for example, with respect to the claimed authentication, compliance, and access point reconfiguration. With respect to this claim, the Admin Guide instructs third-parties how to "Create a Certificate Authentication Profile for TLS-Based Authentication." Admin Guide, pp. 269-270. In particular, Cisco instructs these third-parties how to "use certificates for authenticating endpoints that connect to your network" and "defin[ing] a certificate authentication profile in Cisco ISE…" Id.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	In another example, the Cisco's Admin guide instructs third-parties how to apply and/or configure security policies. For example, Cisco explains that the third-parties can "globally configure the Admin portal for posture services." Admin Guide, pg. 1015. There, Cisco's Admin guide instructs third-parties how to "download updates automatically to the Cisco ISE through the web from Cisco. Id. Further, Cisco explains the various steps for how to "create a posture requirement." Id., pp. 1015-17; See also Admin, p. 1066 (Cisco instructing third-parties on "Create[ing] Client Posture Requirements"); Admin, p. 1067 ("Posture Reassessment Configuration Settings"); Admin p. 1023 ("You can use the Posture Update window to download updates dynamically from the web."); Admin, p. 1072 ("Creat[ing] a Posture Condition", "Creat[ing] Posture Remediation."); Admin, p. 1073 ("Create Posture Policy"). The ISE AG provides third-parties with an "Administration Portal" which provides third-parties "Policy windows include[ing] tools for managing network security in the areas of authentication, authorization, profiling, posture, and client provisioning." https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/admin_guide/b_ise_admin_3_3/b_ISE_admin_33_basic_setup.html#reference_D93EF6652C8D4EB8B56EC6B857DA6F9A. Further, the ISE AG permits third-parties to create "Posture conditions" by following the following field path at the Administration Portal: "Policy -> Policy Elements -> Conditions -> Posture windows." Id. In another example, Cisco's Admin guide instructs third-parties with respect to "Quarantine [for] a Vulnerable Endpoint." Admin, p. 1127. Specifically, Cisco explains that "You can choose to quarantine the endpoint, provide limited access (redirect to a different portal), or reject the request" and then provides three steps for doing so. Id. Similarly, the ISE AG explains to third-parties how they can configure the ISE to "perform the following operations to monitor and control network access through ANC: Quarantine: … Setting to the Quarantine state essentially moves an endpoint from its default VLAN to a specified

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Quarantine VLAN. You must define the Quarantine VLAN previously that is supported on the same NAS as the endpoint." https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/admin_guide/b_ise_admin_3_3/b_ISE_admin_33_maintain_monitor.html.
2. The method of claim 1, further comprising facilitating updates to software on the device in response to applying the security policy, using the gatekeeper.	Cisco performs "[t]he method of claim 1, further comprising facilitating updates to software on the device in response to applying the security policy, using the gatekeeper" and induces others to do so. Cisco describes "facilitating updates to software on the device" as "remediating" it. Cisco describes "Posture Remediation Options," and also "Custom Posture Remediation Actions," which include "a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) remediation types." ISE 3.0 Admin Guide at 1059, 1061.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Posture Remediation Options

The following table provides a list of posture remediation options that are supported by the Cisco ISE Posture Agents for Windows and Macintosh, and the Web Agent for Windows.

Table 162: Posture Remediation Options

ISE Posture Agent for Windows	ISE Posture Agent for Macintosh OS X
Message Text (Local Check)	Message Text (Local Check)
URL Link (Link Distribution)	URL Link (Link Distribution)
File Distribution	—
Launch Program	—
Antivirus Definition Update	Antivirus Live Update
Antispyware Definition Update	Antispyware Live Update
Patch Management Remediation (AC 4.1 - and ISE 1.4)	—
Windows Update	—
WSUS	—

Custom Posture Remediation Actions

A custom posture remediation action is a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) remediation types.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	By "remediat[ing]" an endpoint, Cisco "facilitate[es] updates to software on the device." *See also* ISE 3.0 Admin Guide at 1061-64 ("Add an Antispyware Remediation: You can create an antispyware remediation, which ***updates clients*** with up-to-date file definitions for compliance after remediation." and similar disclosures for Antivirus Remediation, File Remediation, Launch Program Remediation, Patch Management Remediation, and others). *See also* ISE 3.0 Admin Guide at 1029 (automatic updates in Windows clients): **Predefined Condition for Enabling Automatic Updates in Windows Clients** The pr_AutoUpdateCheck_Rule is a Cisco predefined condition, which is downloaded to the Compound Conditions window. This condition allows you to check whether the automatic updates feature is enabled on Windows clients. If a Windows client fails to meet this requirement, then the Network Access Control (NAC) Agents enforce the Windows client to enable (remediate) the automatic updates feature. After this remediation is done, the Windows client becomes posture compliant. The Windows update remediation that you associate in the posture policy overrides the Windows administrator setting, if the automatic updates feature is not enabled on the Windows client.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

and at 1048-50 (Patch Management Condition Settings):

Patch Management Condition Settings

The following table describes the fields in the **Patch Management Conditions** window. To view this window, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Patch Management Condition**.

Table 157: Patch Management Condition

Field Name	Usage Guidelines
Name	Enter the name of the patch management condition.
Description	Enter a description for the patch management condition.
Operating System	Choose an operating system to check the installation of a patch management software on the endpoint, or check the latest patch management definition file updates to which the condition is applied. You can select the Windows OS or macOS. You can also select more than one version of an operating system to create the patch management condition.
Vendor Name	Choose a vendor from the **Vendor Name** drop-down list. Based on your selection, the patch management products and their supported versions, check type, and minimum compliant module support details are displayed in the **Products for Selected Vendor** table. The list in the table changes according to the selected operating system.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Field Name	Usage Guidelines
Check Patches Installed	(Available only when you select the **Up To Date** check type) You can configure severity levels for missing patches, which are then deployed based on the severity. Choose one of the following options: • **Critical Only**: To check if critical software patches are installed on the endpoints in your deployment. • **Important and Critical**: To check if important and critical software patches are installed on the endpoints in your deployment. • **Moderate, Important, and Critical**: To check if moderate, important, and critical software patches are installed on the endpoints in your deployment. • **Low To Critical**: To check if low, moderate, important, and critical software patches are installed on the endpoints in your deployment. • **All**: To install the missing patches for all severity levels.

and also Randomized Changing MAC at 44 ("Cisco ISE performs the following functions with the external MDM server: . . . Handles device remediation: Endpoints are granted restricted access during remediation."); *and also* Identity Services Engine Data Sheet at 4 ("Automated device-compliance checks for device-posture and ***remediation*** options using Cisco Secure Client (formerly Anyconnect agent), Temporal and Agentless options . . ." and 7 ("Supports automatic ***remediation*** of PC clients as well as periodic reassessments . . .")

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

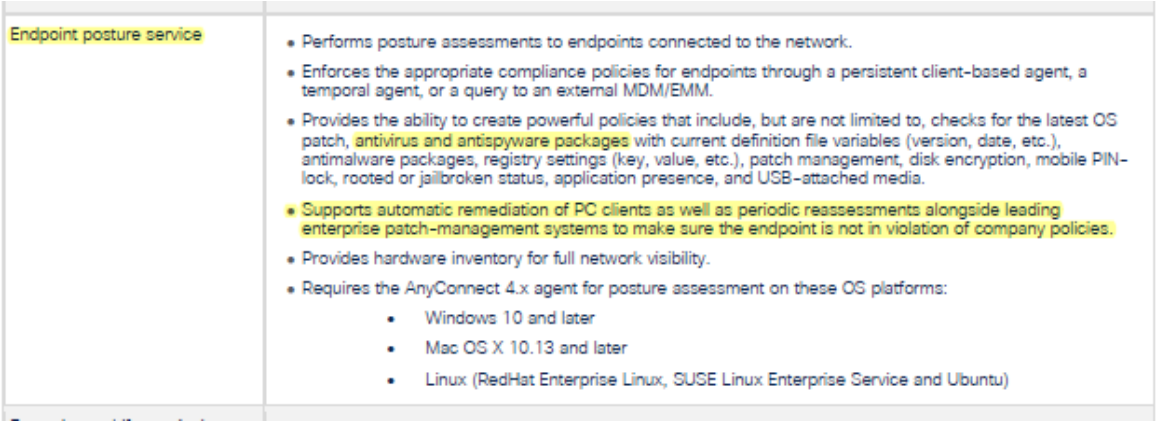
Automated device-compliance checks for device-posture and remediation options using Cisco Secure Client (formerly Anyconnect agent), Temporal and Agentless options with custom scripts support. Cisco Secure Client Temporal and Agentless are two different ways to gather posture from endpoints beyond a full agent. Agentless option is supported from ISE 3.0 onwards lo Cisco Secure client also provide advanced VPN services for desktop and laptop checks. ISE also integrates with market-leading Mobile Device Management/Enterprise Mobility Management (MDM/EMM) vendors. MDM integration helps ensure that a mobile device is both secure and policy compliant before it is given access to the network.

. . .

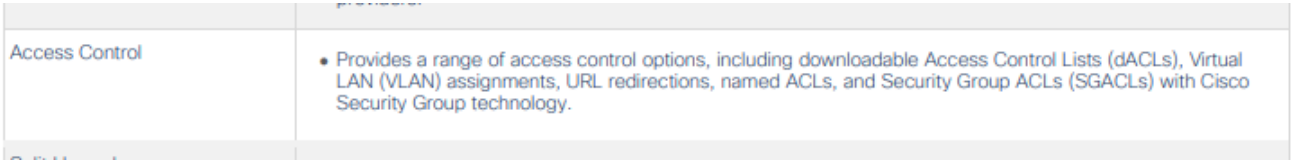
Endpoint posture service	• Performs posture assessments to endpoints connected to the network.
	• Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM.
	• Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media.
	• Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies.
	• Provides hardware inventory for full network visibility.
	• Requires the AnyConnect 4.x agent for posture assessment on these OS platforms:
	  ◦ Windows 10 and later
	  ◦ Mac OS X 10.13 and later
	  ◦ Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu)

Identity Services Engine Data Sheet at 4, 7.

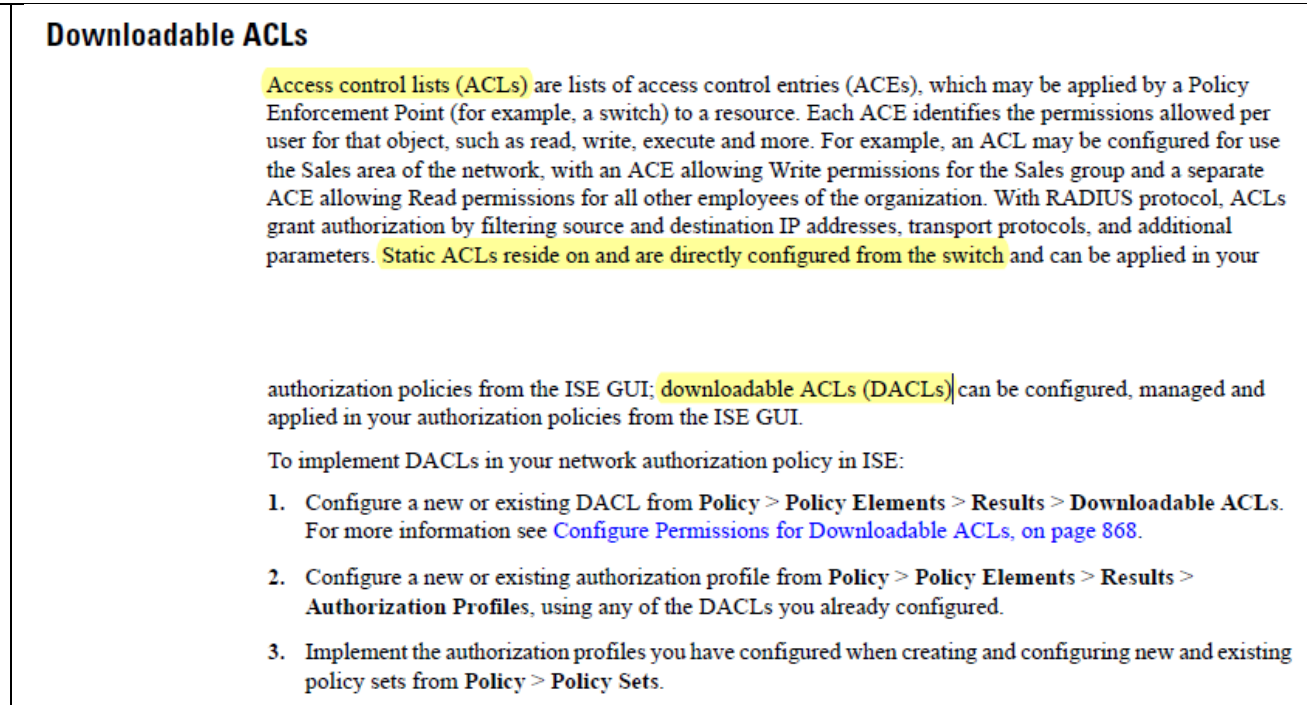
U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Finally, Cisco "facilitat[es] updates . . . in response to applying the security policy, using the gatekeeper. Cisco describes how ISE "Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies." ISE Data Sheet at 7.  Endpoint posture service • Performs posture assessments to endpoints connected to the network. • Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM. • Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media. • Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies. • Provides hardware inventory for full network visibility. • Requires the AnyConnect 4.x agent for posture assessment on these OS platforms: – Windows 10 and later – Mac OS X 10.13 and later – Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu) Because ISE remediates an endpoint (the "device") "to make sure the endpoint is not in violation of company policies[,]" this means that such remediation is "in response to applying the security policy" and further that it uses ISE's policy-management apparatus (the "gatekeeper").

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

3. The method of claim 1, wherein configuring the access point includes setting an access control list on the access point.	Cisco's ISE performs "[t]he method of claim 1, wherein configuring the access point includes setting an access control list on the access point" and induces others to do so. First, Cisco discloses that ISE uses Access Control Lists, or ACLs. ISE Data Sheet at 5 ("[ISE] [P]rovides a range of access control options, including ***downloadable Access Control Lists (dACLs)***, Virtual LAN (VLAN) assignments, URL redirections, ***named ACLs***, and ***Security Group ACLs (SGACLs)*** with Cisco Security Group technology."  Cisco further describes how "[w]ith the RADIUS protocol, ACLs ***grant authorization*** by filtering source and destination IP addresses, transport protocols, and additional parameters." ISE 3.0 Admin Guide at 867-68. By the ACL "grant[ing] authorization," ISE "configure[es] the access point [by] setting an access control list on the access point." *See id.*

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)



Downloadable ACLs

Access control lists (ACLs) are lists of access control entries (ACEs), which may be applied by a Policy Enforcement Point (for example, a switch) to a resource. Each ACE identifies the permissions allowed per user for that object, such as read, write, execute and more. For example, an ACL may be configured for use the Sales area of the network, with an ACE allowing Write permissions for the Sales group and a separate ACE allowing Read permissions for all other employees of the organization. With RADIUS protocol, ACLs grant authorization by filtering source and destination IP addresses, transport protocols, and additional parameters. Static ACLs reside on and are directly configured from the switch and can be applied in your

authorization policies from the ISE GUI; downloadable ACLs (DACLs) can be configured, managed and applied in your authorization policies from the ISE GUI.

To implement DACLs in your network authorization policy in ISE:

1. Configure a new or existing DACL from **Policy** > **Policy Elements** > **Results** > **Downloadable ACLs**. For more information see Configure Permissions for Downloadable ACLs, on page 868.
2. Configure a new or existing authorization profile from **Policy** > **Policy Elements** > **Results** > **Authorization Profiles**, using any of the DACLs you already configured.
3. Implement the authorization profiles you have configured when creating and configuring new and existing policy sets from **Policy** > **Policy Sets**.

Cisco further describes how ACLs are "set" on different access points within ISE. The "ISE is the enforcement point . . . [that] then applies the appropriate access control policies to ***switches, access routers, wireless access points, and other network access points***."

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

In the following illustration, Cisco ISE is the enforcement point and the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution.

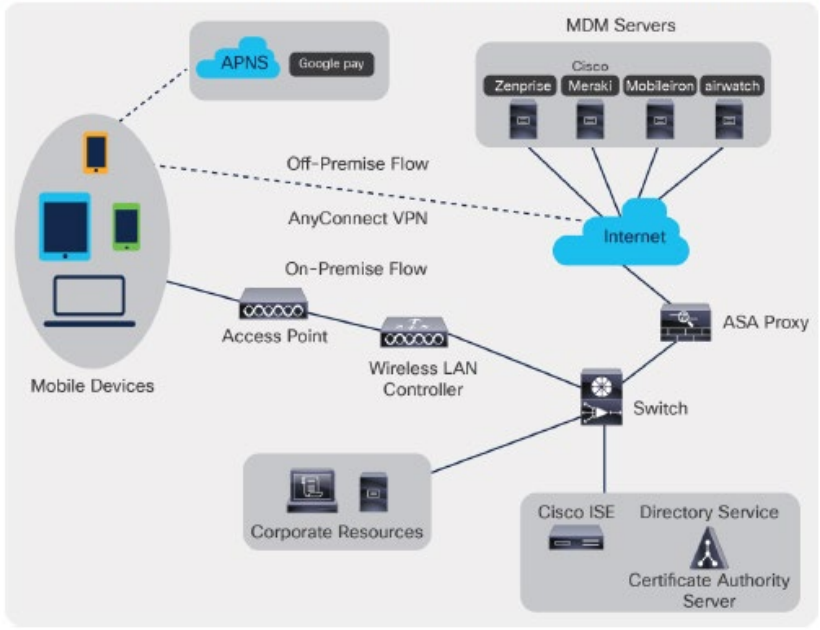


Figure 5.
Cisco ISE and MDM servers

You can configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. It then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network.

Randomized and Changing MAC at 43.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Cisco describes how ACLs are "set" on four kinds of access points: switches, routers, wireless access points, and firewalls (in conjunction with remote access VPNs). With respect to switches, Cisco states that static ACLs "reside on and are directly configured from the switch" while downloadable ACLs "can be configured, managed and applied in your authorization policies from the ISE GUI." ISE 3.0 Admin Guide at 867-68. Thus, "configuring the access point" (here, the switch) "includes setting an access control list" on it. **Downloadable ACLs** Access control lists (ACLs) are lists of access control entries (ACEs), which may be applied by a Policy Enforcement Point (for example, a switch) to a resource. Each ACE identifies the permissions allowed per user for that object, such as read, write, execute and more. For example, an ACL may be configured for use the Sales area of the network, with an ACE allowing Write permissions for the Sales group and a separate ACE allowing Read permissions for all other employees of the organization. With RADIUS protocol, ACLs grant authorization by filtering source and destination IP addresses, transport protocols, and additional parameters. Static ACLs reside on and are directly configured from the switch and can be applied in your authorization policies from the ISE GUI; downloadable ACLs (DACLs) can be configured, managed and applied in your authorization policies from the ISE GUI. To implement DACLs in your network authorization policy in ISE: 1. Configure a new or existing DACL from **Policy** > **Policy Elements** > **Results** > **Downloadable ACLs**. For more information see Configure Permissions for Downloadable ACLs, on page 868. 2. Configure a new or existing authorization profile from **Policy** > **Policy Elements** > **Results** > **Authorization Profiles**, using any of the DACLs you already configured. 3. Implement the authorization profiles you have configured when creating and configuring new and existing policy sets from **Policy** > **Policy Sets**.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Cisco also discloses that its switches can be configured by the ISE to run an IPv4-based Access Control List. Cisco, Configure IPv4-based Access Control List (ACL) and Access Control Entry (ACE) on a Switch, https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-350-series-managed-switches/smb3025-configure-ipv4-based-access-control-list-acl-and-access-cont.pdf (last visited September 27, 2023).

Configure IPv4-based Access Control List (ACL) and Access Control Entry (ACE) on a Switch

Objective

An Access Control List (ACL) is a list of network traffic filters and correlated actions used to improve security. It blocks or allows users to access specific resources. An ACL contains the hosts that are permitted or denied access to the network device.

The IPv4-based ACL is a list of source IPv4 addresses that use Layer 3 information to permit or deny access to traffic. IPv4 ACLs restrict IP-related traffic based on the configured IP filters. A filter contains the rules to match an IP packet, and if the packet matches, the rule also stipulates if the packet should be permitted or denied.

An Access Control Entry (ACE) contains the actual access rule criteria. Once the ACE is created, it is applied to an ACL.

You should use access lists to provide a basic level of security for accessing your network. If you do not configure access lists on your network devices, all packets passing through the switch or router could be allowed onto all parts of your network.

This article provides instructions on how to configure IPv4-based ACL and ACE on your managed switch.

Applicable Devices

- Sx350 Series
- SG350X Series
- Sx500 Series
- Sx550X Series

Thus, "configuring the access point" "includes setting an access control list" on it.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Cisco also states that "ACLs are applied at the interface of the router." Cisco, Configure and Filter IP Access Lists at 6-7, https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.pdf (last accessed September 26, 2023).

Apply ACLs

You can define ACLs and still not apply them. But, the ACLs have no effect until they are applied to the interface of the router. It is a good practice to apply the ACL on the interface closest to the source of the traffic. As shown in this example, when you try to block traffic from source to destination, you can apply an inbound ACL to E0 on router A instead of an outbound list to E1 on router C. An access-list has a **deny ip any any** implicitly at the end of any access-list. If traffic is related to a DHCP request and if it is not explicitly permitted, the traffic is dropped because when you look at DHCP request in IP, the source address is s=0.0.0.0 (Ethernet1/0), d=255.255.255.255, len 604, rcvd 2 UDP src=68, dst=67. Notice that the source IP address is 0.0.0.0 and destination address is 255.255.255.255. Source port is 68 and destination 67. Therefore, you must permit this kind of traffic in your access-list or else the traffic is dropped due to implicit deny at the end of the statement.

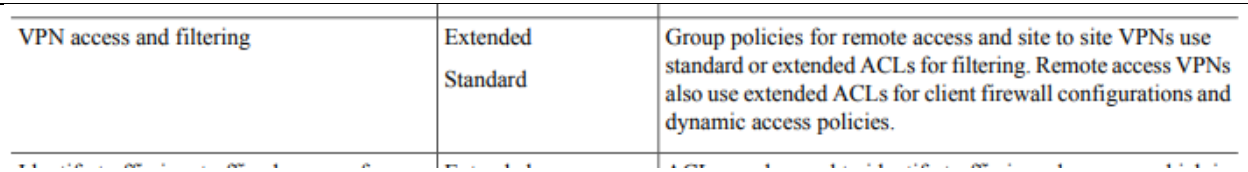
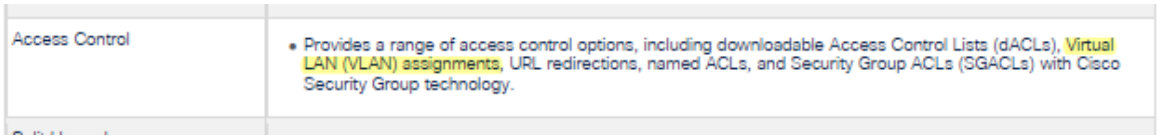
Note: For UDP traffic to pass through, UDP traffic must also be permitted explicitly by the ACL.

Thus, "configuring the access point" "includes setting an access control list" on it.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Cisco further discloses that its wireless access points can be configured to run a ***Management ACL***. Cisco, Configure Management Access Control List (ACL) on a Wireless Access Point, https://www.cisco.com/c/en/us/support/docs/smb/wireless/cisco-small-business-100-series-wireless-access-points/smb5282-configure-management-access-control-list-acl-on-a-wireless-a.pdf (last visited September 27, 2023). **Configure Management Access Control List (ACL) on a Wireless Access Point** **Objective** Management Access Control List (ACL) is a feature of the Wireless Access Point (WAP) that can permit hosts to access the web-based utility through web, Telnet, or SNMP. You can authorize up to five IPv4 hosts and five IPv6 hosts to have access to the web-based utility. This article aims to guide you through the configuration, and authorize hosts according to their IPv4 and IPv6 addresses. Thus, "configuring the access point" "includes setting an access control list" on it. In conjunction with remote access VPNs, Cisco states that "Remote access VPNs also use extended ACLs for client firewall configurations and dynamic access points."

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	 Cisco, ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide, 7.10, at 38, https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/asdm710/firewall/asdm-710-firewall-config.pdf; *see generally id.* at 59-74 (chapter 4 on access control lists); *and* 2 ("To implement identity control, do any combination of the following: . . . Install Cisco Identity Services Engine (ISE) on a separate server to implement Cisco Trustsec.") Thus, "configuring the access point" (here, the remote access VPN/firewall) "includes setting an access control list" on it.
4. The method of claim 1, wherein configuring the access point includes assigning a VLAN.	Cisco performs "[t]he method of claim 1, wherein configuring the access point includes assigning a VLAN." Cisco discloses that generally, ISE "provides a range of access control options, including . . . Virtual LAN (VLAN) assignments. ISE Data Sheet at 5. Disclosing "VLAN assignment[]" as an "access control option" shows that "configuring the access point includes assigning a VLAN." 

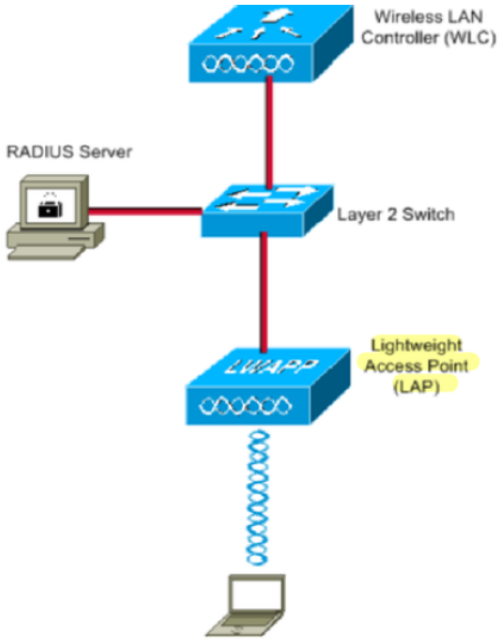
U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Cisco provides two examples of "configuring the access point [by] assigning a VLAN." First, Cisco describes how one can perform ***dynamic VLAN assignment*** by using ISE and a Catalyst 9800 wireless LAN controller (WLC). Cisco, Configure Dynamic VLAN Assignment with ISE and Catalyst 9800 Wireless LAN Controller at 3, 25 (June 2022), https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/217043-configure-dynamic-vlan-assignment-with-c.pdf (last visited May 22, 2023). **Introduction** This document describes the concept of dynamic VLAN assignment and how to configure the Catalyst 9800 wireless LAN controller (WLC) and Cisco Identity Service Engine (ISE) to assign wireless LAN (WLAN) in order to accomplish this for the wireless clients. **Requirements** Cisco recommends that you have knowledge of these topics: • Have basic knowledge of the WLC and Lightweight Access Points (LAPs). • Have functional knowledge of the AAA server such as ISE. • Have a thorough knowledge of wireless networks and wireless security issues. Configure Dynamic VLAN Assignment with ISE at 1.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Network Diagram

This document uses this network setup:



These are the configuration details of the components used in this diagram:

- The IP address of Cisco ISE (RADIUS) server is 10.10.1.24.
- The Management Interface address of the WLC is 10.10.1.17.
- The internal DHCP server on the controller is used to assign the IP address to wireless clients.
- This document uses 802.1x with PEAP as the security mechanism.

Cisco, Configure Dynamic VLAN Assignment at 3. Thus, through dynamic VLAN assignment, Cisco "configure[es] the access point [by] assigning a VLAN."

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	By way of a second example—Adaptive Network Control—Cisco describes how ISE can "quarantine" a user "essentially" by "mov[ing] an endpoint ***from its default VLAN*** to a ***specified Quarantine VLAN***." ISE 3.0 Admin Guide at 300. Similarly, ISE can "unquarantined" a user by "returning the endpoint to its original VLAN" and thus "permit[ting] full access to the network for an endpoint." By changing VLANs (from quarantine to original), Cisco "configure[es] the access point [by] assigning a VLAN." **Adaptive Network Control** Adaptive Network Control (ANC) is a service that runs on the Administration node. This service monitors and controls network access of endpoints. ANC is invoked by the ISE administrator on the admin GUI, and also can be invoked through pxGrid from third-party systems. ANC supports wired and wireless deployments and requires an Advantage License. You can use ANC to change the authorization state without having to modify the overall authorization policy of the system. ANC allows you to set the authorization state when you quarantine an endpoint. As a result, the established authorization policies where authorization policies are defined to check for ANCPolicy to limit or deny network access. You can unquarantine an endpoint for full network access. You can also shut down the port on the network attached system (NAS) that disconnects the endpoint from the network. There are no limits to the number of users that can be quarantined at one time. Also, there are no time constraints on the quarantine period length. You can perform the following operations to monitor and control network access through ANC: • Quarantine: Allows you to use Exception policies (authorization policies) to limit or deny an endpoint access to the network. You must create Exception policies to assign different authorization profiles (permissions) depending on the ANCPolicy. Setting to the Quarantine state essentially moves an endpoint from its default VLAN to a specified Quarantine VLAN. You must define the Quarantine VLAN previously that is supported on the same NAS as the endpoint. • Unquarantine: Allows you to reverse the quarantine status that permits full access to the network for an endpoint. This happens by returning the endpoint to its original VLAN. • Shutdown: Allows you to deactivate a port on the NAS and disconnect the endpoint from the network. Once the port is shut down on the NAS to which an endpoint is connected, manually reset the port on the NAS again. This allows an endpoint to connect to the network, which is not available for wireless deployments.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

7. The method of claim 1, wherein the authentication includes using an EAP protocol.	Cisco performs "[t]he method of claim 1, wherein the authentication includes using an EAP protocol" and induces others to do so. Cisco describes how ISE uses several different EAP protocols, including Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), and Protected Extensible Authentication Protocol (PEAP). ISE 3.0 Admin Guide at 903. By using ISE's EAP-based authentication methods, Cisco (and third parties) perform "[t]he method of claim 1, wherein the authentication includes using an EAP protocol." **Policy Set Protocol Settings** You must define global protocol settings in Cisco ISE before you can use these protocols to create, save and implement a policy set. You can use the Protocol Settings page to define global options for the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), and Protected Extensible Authentication Protocol (PEAP) protocols, which communicate with the other devices in your network. **Supported Network Access Policy Set Protocols** The following is a list of protocols that you can choose while defining your Network Access Policy Set policy: • Password Authentication Protocol (PAP) • Protected Extensible Authentication Protocol (PEAP) • Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2) • Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) • Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) • Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) • Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) • Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS) ISE 3.0 Admin Guide at 903.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Cisco goes on to describe the guidelines for each of these EAP types. ISE 3.0 Admin Guide at 903-06 (EAP-FAST); 906-07 (EAP-TTLS); 907-08 (EAP-TLS); 908-09 (PEAP); 919-25 (allowed protocols in ISE include EAP-MD5, EAP-TLS, LEAP, PEAP, EAP-FAST, EAP-TTLS, Tunnel Extensible Authentication Protocol (TEAP). Cisco also describes several RADIUS-based EAP protocols in ISE: **RADIUS-Based EAP Protocols** EAP provides an extensible framework that supports various authentication types. This section describes the EAP methods supported by Cisco ISE and contains the following topics: **Simple EAP Methods** • EAP-Message Digest 5 • Lightweight EAP **EAP Methods That Use Cisco ISE Server Certificate for Authentication** • PEAP/EAP-MS-CHAPv2 • PEAP/EAP-GTC • EAP-FAST/EAP-MS-CHAPv2 • EAP-FAST/EAP-GTC Apart from the methods listed above, there are EAP methods that use certificates for both server and client authentication. ISE 3.0 Admin Guide at 934.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

RADIUS-Based EAP Authentication Flow

Whenever EAP is involved in the authentication process, the process is preceded by an EAP negotiation phase to determine which specific EAP method (and inner method, if applicable) should be used. EAP-based authentication occurs in the following process:

1. A host connects to a network device.
2. The network device sends an EAP Request to the host.
3. The host replies with an EAP Response to the network device.
4. The network device encapsulates the EAP Response that it received from the host into a RADIUS Access-Request (using the EAP-Message RADIUS attribute) and sends the RADIUS Access-Request to Cisco ISE.
5. Cisco ISE extracts the EAP Response from the RADIUS packet and creates a new EAP Request, encapsulates it into a RADIUS Access-Challenge (again, using the EAP-Message RADIUS attribute), and sends it to the network device.
6. The network device extracts the EAP Request and sends it to the host.

In this way, the host and Cisco ISE indirectly exchange EAP messages (transported over RADIUS and passed through the network device). The initial set of EAP messages that are exchanged in this manner negotiate the specific EAP method that will subsequently be used to perform the authentication.

The EAP messages that are subsequently exchanged are then used to carry the data that is needed to perform the actual authentication. If it is required by the specific EAP authentication method that is negotiated, Cisco ISE uses an identity store to validate user credentials.

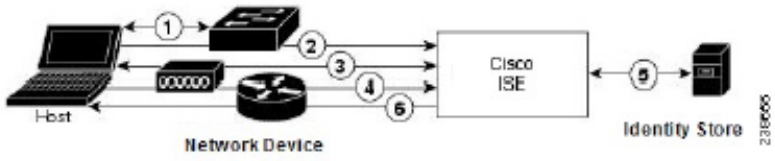
After Cisco ISE determines whether the authentication should pass or fail, it sends either an EAP-Success or EAP-Failure message, encapsulated into a RADIUS Access-Accept or Access-Reject message to the network device (and ultimately also to the host).

ISE 3.0 Admin Guide at 934.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

The following figure shows a RADIUS-based authentication with EAP.

Figure 47: RADIUS-Based Authentication with EAP



ISE 3.0 Admin Guide at 935; *see also id.* at 935-37 (EAP-MD5, LEAP, PEAP advantages and protocol flow, EAP-FAST benefits and protocol flow); 940-41 (EAP-FAST is used within Cisco's TrustSec architecture).

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

8. The method of claim 1, wherein the authentication includes using a RADIUS protocol.	Cisco performs "[t]he method of claim 1, wherein the authentication includes using a RADIUS protocol" and induces others to do so. Cisco states that generally "Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, . . ." ISE 3.0 Admin Guide at 2. • **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods. Cisco further describes how "Cisco ISE supports RADIUS protocol flow according to RFC 2865 and generic support for all general RADIUS attributes as described in RFC 2865 and its extension. Cisco ISE supports parsing of vendor-specific attributes only for vendors that are defined in the Cisco ISE dictionary. ISE 3.0 Admin Guide at 918. **RADIUS Protocol Support in Cisco ISE** RADIUS is a client/server protocol through which remote-access servers communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. You can use RADIUS to maintain user profiles in a central database that all remote servers can share. This protocol provides better security, and you can use it to set up a policy that is applied at a single administered network point. RADIUS also functions as a RADIUS client in Cisco ISE to proxy requests to a remote RADIUS server, and it provides Change of Authorization (CoA) activities during an active session. Cisco ISE supports RADIUS protocol flow according to RFC 2865 and generic support for all general RADIUS attributes as described in RFC 2865 and its extension. Cisco ISE supports parsing of vendor-specific attributes only for vendors that are defined in the Cisco ISE dictionary.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	See also id. at 925 ("Allowed Protocols" within ISE include "Require Message Authenticator for all RADIUS Requests"); *and also e.g., id.* at 909-12 (Configure RADIUS Settings); 820 (Configure RADIUS IPSec on Cisco ISE); 888 (RADIUS-Vendor Dictionaries); 1185 ("Configure the switch to interact with Cisco ISE as the RADIUS source server by entering the following commands: . . ."); 1185 ("Specify the settings to ensure the switch can appropriately handle RADIUS CoA behavior and related posture functions on Cisco ISE by entering the following commands: . . ."); 580-82 (in Easy Connect Enforcement Mode, "ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event); 354 (the field for "Auth Method" "show[s] the authentication method that is used by the RADIUS protocol . . ."); 429-30 (Network Access Devices with Central Web Authentication Process, "In this scenario, the network access device (NAD) makes a new authorization request to the Cisco ISE RADIUS server from an unknown endpoint connection. Cisco also describes several RADIUS-based EAP protocols in ISE:

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

RADIUS-Based EAP Protocols

EAP provides an extensible framework that supports various authentication types. This section describes the EAP methods supported by Cisco ISE and contains the following topics:

Simple EAP Methods

- EAP-Message Digest 5
- Lightweight EAP

EAP Methods That Use Cisco ISE Server Certificate for Authentication

- PEAP/EAP-MS-CHAPv2
- PEAP/EAP-GTC
- EAP-FAST/EAP-MS-CHAPv2
- EAP-FAST/EAP-GTC

Apart from the methods listed above, there are EAP methods that use certificates for both server and client authentication.

ISE 3.0 Admin Guide at 934.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

RADIUS-Based EAP Authentication Flow

Whenever EAP is involved in the authentication process, the process is preceded by an EAP negotiation phase to determine which specific EAP method (and inner method, if applicable) should be used. EAP-based authentication occurs in the following process:

1. A host connects to a network device.
2. The network device sends an EAP Request to the host.
3. The host replies with an EAP Response to the network device.
4. The network device encapsulates the EAP Response that it received from the host into a RADIUS Access-Request (using the EAP-Message RADIUS attribute) and sends the RADIUS Access-Request to Cisco ISE.
5. Cisco ISE extracts the EAP Response from the RADIUS packet and creates a new EAP Request, encapsulates it into a RADIUS Access-Challenge (again, using the EAP-Message RADIUS attribute), and sends it to the network device.
6. The network device extracts the EAP Request and sends it to the host.

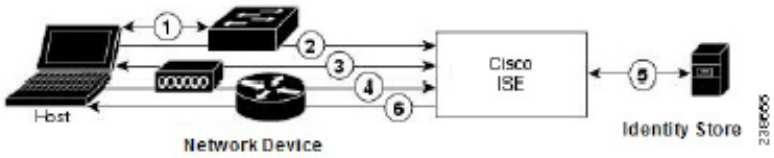
In this way, the host and Cisco ISE indirectly exchange EAP messages (transported over RADIUS and passed through the network device). The initial set of EAP messages that are exchanged in this manner negotiate the specific EAP method that will subsequently be used to perform the authentication.

The EAP messages that are subsequently exchanged are then used to carry the data that is needed to perform the actual authentication. If it is required by the specific EAP authentication method that is negotiated, Cisco ISE uses an identity store to validate user credentials.

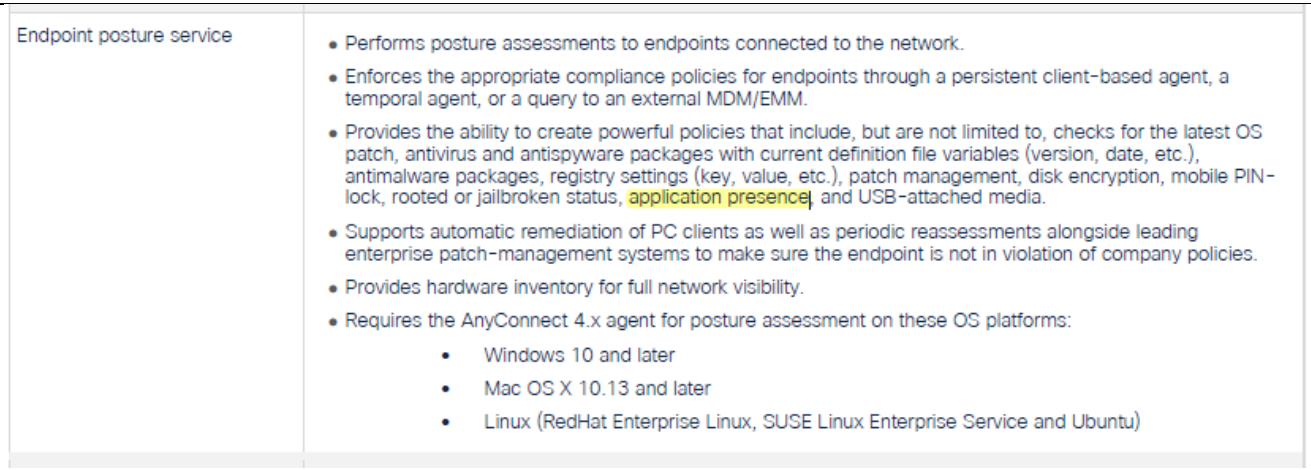
After Cisco ISE determines whether the authentication should pass or fail, it sends either an EAP-Success or EAP-Failure message, encapsulated into a RADIUS Access-Accept or Access-Reject message to the network device (and ultimately also to the host).

ISE 3.0 Admin Guide at 934.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	The following figure shows a RADIUS-based authentication with EAP. *Figure 47: RADIUS-Based Authentication with EAP*  ISE 3.0 Admin Guide at 935; *see also id.* at 935-37 ("PEAP is compatible with the IEEE 802.1X standard and RADIUS protocol. Cisco ISE supports PEAP version 0 (PEAPv0) and PEAP version 1 (PEAPv1)).")
9. The method of claim 1, wherein one of the requirements pertains to a status of an application on the device.	Cisco performs "[t]he method of claim 1, wherein one of the requirements pertains to a status of an application on the device" and induces others to do so. Cisco states that it "[p]erforms posture assessments to endpoints connected to the network" and "enforces the appropriate compliance policies for [those] endpoints" through different mechanisms. Such "security policies" "include, but are not limited to, checks for . . . application presence[,]" among other criteria. Thus one of the "requirements" (of "the appropriate compliance policies") pertains to a status of an application on the device.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)



Endpoint posture service	• Performs posture assessments to endpoints connected to the network.
	• Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM.
	• Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media.
	• Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies.
	• Provides hardware inventory for full network visibility.
	• Requires the AnyConnect 4.x agent for posture assessment on these OS platforms:
	  ◦ Windows 10 and later
	  ◦ Mac OS X 10.13 and later
	  ◦ Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu)

ISE Data Sheet at 7.

Cisco also describes "simple posture conditions," including "application conditions" on the client (the claimed "device"). ISE 3.0 Admin Guide at 1027. Thus one of the conditions ("requirements") pertains to a status of an application on the device.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Simple Posture Conditions

You can use the **Posture Navigation** pane to manage the following simple conditions:

- File Conditions: A condition that checks the existence of a file, the date of a file, and the versions of a file on the client.
- Registry Conditions: A condition that checks for the existence of a registry key or the value of the registry key on the client.
- Application Conditions: A condition that checks if an application or process is running or not running on the client.

Note If a process is installed and running, user is compliant. However, the Application condition works in reverse logic; If an application is not installed and not running, the end user is complaint. If an application is installed and running, the end user is non-complaint.

- Service Conditions: A condition that checks if a service is running or not running on the client.
- Dictionary Conditions: A condition that checks a dictionary attribute with a value.
- USB Conditions: A condition that checks for the presence of USB mass storage device.

Cisco also states—with respect to continuous endpoint attribute monitoring— "After initial posture [assessment], the AnyConnect agent scans ***the applications*** [on the endpoint, i.e. the "device"] every X minute and sends the differences from the last scan to the server. The server displays the ***complete list of running and installed applications***." ISE 3.0 Admin Guide at 1102-03. Thus one of the "requirements" pertains to a status of an application on the device.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Continuous Endpoint Attribute Monitoring You can use the AnyConnect agent to continuously monitor different endpoint attributes to ensure that dynamic changes are observed during posture assessment. This improves the overall visibility of an endpoint and helps you create posture policies based on their behavior. The AnyConnect agent monitors applications that are installed and running on an endpoint. You can turn on and off the feature and configure how often the data should be monitored. By default, data is collected every 5 minutes and is stored in the database. During initial posture, AnyConnect reports a complete list of running and installed applications. After initial posture, the AnyConnect agent scans the applications every X minute and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications. ISE 3.0 Admin Guide at 1102-03.
11. The method of claim 1, wherein one of the requirements pertains to other devices coupled to the device.	Cisco performs "[t]he method of claim 1, wherein one of the requirements pertains to other devices coupled to the device" and induces others to do so. Cisco states, with respect to "hardware attributes," that they include a field for "attached devices." ISE 3.0 Admin Guide at 174-75. Cisco further explains that "You can click the number in the ***Attached Devices*** column that corresponds to an endpoint to view the Name, Category, Manufacturer, Type, Product ID, and Vendor ID of the USB devices that are currently attached to the endpoint." *Id.*; *see also id.* at 1027 (USB Conditions), 1051 (USB Condition Settings), 1057 (USB_Block "[e]nsures that the endpoint device does not have any USB storage devices connected"). Thus, because Cisco's ISE can determine "attached devices" such as a USB (which are

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	so attached to the endpoint), one of the requirements pertains to other devices coupled to the device.
14. The method of claim 1, wherein the scanning is performed using an agent on the device.	Cisco performs "[t]he method of claim 1, wherein the scanning is performed using an agent on the device" and induces others to do so. As described above with respect to claim element 1-b, Cisco ISE "scan[s] the device to collect information regarding the device" by using agents. Thus, Cisco performs "[t]he method of claim 1, wherein the scanning is performed using an agent on the device" and induces others to do so.

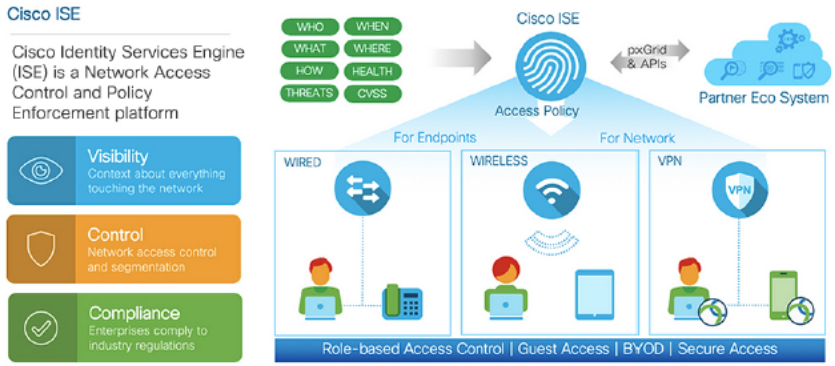
U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

[16-preamble] A method of providing access over a communication network, the method comprising:	Cisco infringes this claim by making, using, testing, offering for sale, and selling the ISE product and system and through performance of each of the claimed steps and/or providing instructions and data from its servers to third-parties to perform at least one of the claimed steps, and as further described in claim 1. To the extent the preamble is limiting, Cisco ISE is "a security policy management platform that provides secure access to network resources" and thereby "provid[es] access over a communication network." **Introduction to Cisco Identity Services Engine** Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, wireless controllers, Virtual Private Network (VPN) gateways, 5GaaS networks, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation. Cisco ISE is available on secure network server appliances with different performance characterizations, and also as software that can be run on a virtual machines (VMs). Note that you can add more appliances to a deployment for better performance. Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also enables the configuration and management of distinct personas and services, thereby giving you the ability to create and apply services, where needed, in a network, but operate the Cisco ISE deployment as a complete and coordinated system. For detailed Cisco ISE ordering and licensing information, see the *Cisco Identity Services Engine Ordering Guide*. For information on monitoring and troubleshooting the system, see the "Monitoring and Troubleshooting Cisco ISE" section in the *Cisco Identity Services Engine Administrator Guide*. ISE 3.0 Release Notes at 1.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Cisco further describes ISE as a "Network Access Control and Policy enforcement system . . . that enables endpoint access control" and which thereby "provid[es] access over a communication network."

Cisco ISE Overview



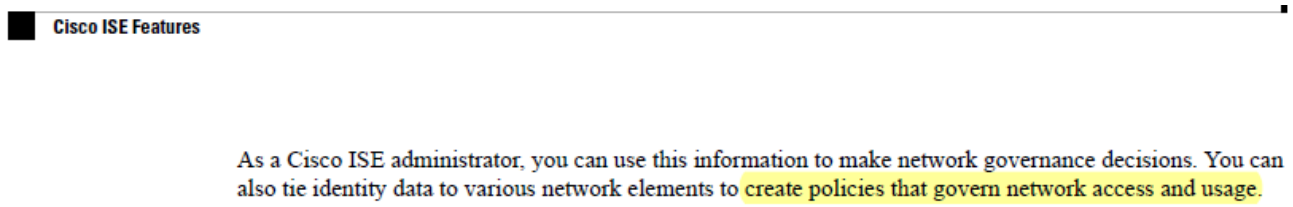
Cisco Identity Services Engine (ISE) is an identity-based network access control and policy enforcement system. It functions as a common policy engine that enables endpoint access control and network device administration for enterprises.

You can leverage Cisco ISE to ensure compliance, enhance infrastructure security, and streamline service operations.

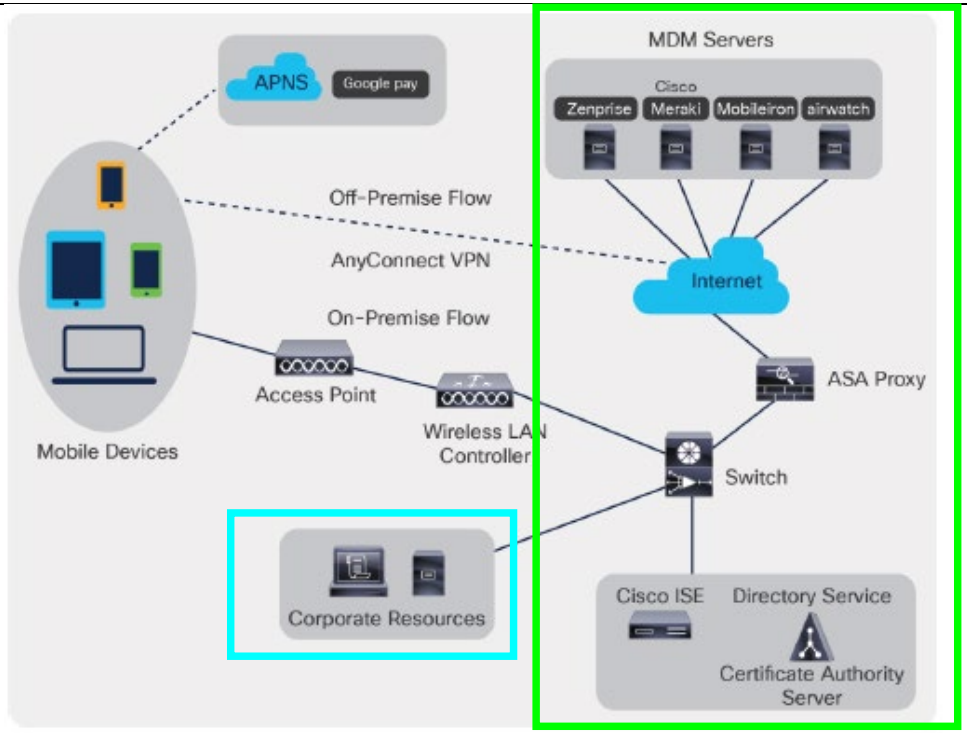
A Cisco ISE administrator can gather real-time contextual data for a network, including users and user groups (who?), device type (what?), access time (when?), access location (where?), access type (wired, wireless, or VPN) (how?), and network threats and vulnerabilities.

ISE 3.0 Admin Guide at 1.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Cisco further describes its ISE as allowing a an administrator to "tie identity data to various network elements to create policies that govern network access and usage" which is thereby a "method of providing access over a communication network."  ISE 3.0 Admin Guide at 2.
[16-a] receiving at an access point a request for access to a less-restricted network, the request coming from an access device;	Cisco ISE "receiv[es] at an access point a request for access to a less-restricted network, the request coming from an access device," or induces others to do so as set forth in claim element 1-d. In this step, the Cisco ISE receives a request for a less restricted subset of the protected network (blue) from a user access device—for example, a mobile phone, tablet, or laptop computer (e.g. Mobile Devices).

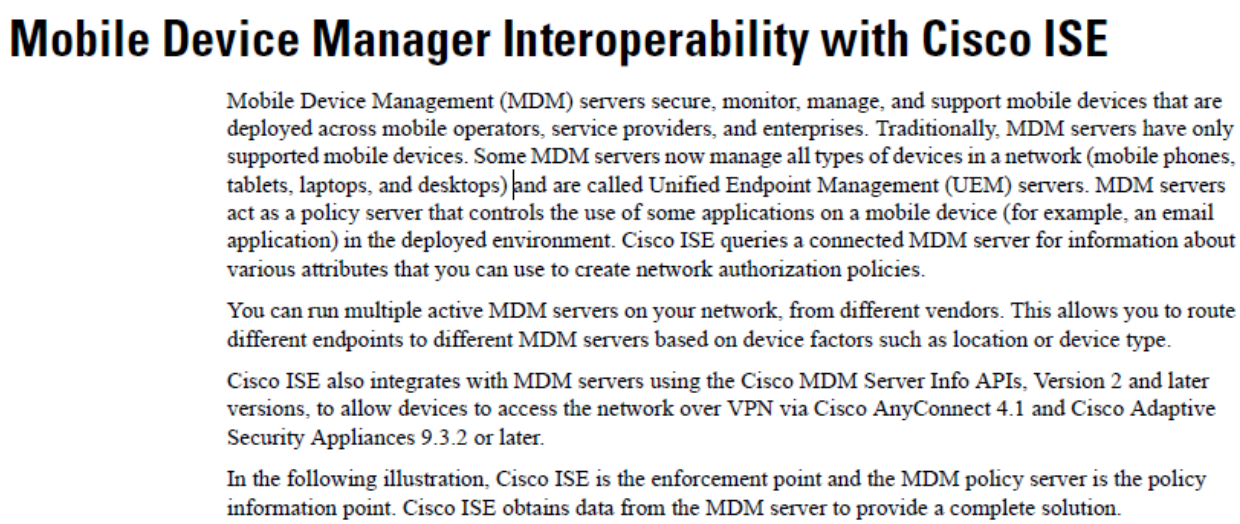
U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)



Randomized and Changing MAC Deployment Guide at 43.

Cisco also describes in its ISE 3.0 Admin Guide how Mobile Device Management (MDM) servers "secure, monitor, manage, and support mobile devices that are deployed across mobile operators, service providers, and enterprises. Traditionally, MDM servers have only supported mobile devices. Some MDM servers now manage ***all types of devices in a network (mobile phones, tablets, laptops, and desktops)***[.]"

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)



Mobile Device Manager Interoperability with Cisco ISE

Mobile Device Management (MDM) servers secure, monitor, manage, and support mobile devices that are deployed across mobile operators, service providers, and enterprises. Traditionally, MDM servers have only supported mobile devices. Some MDM servers now manage all types of devices in a network (mobile phones, tablets, laptops, and desktops) and are called Unified Endpoint Management (UEM) servers. MDM servers act as a policy server that controls the use of some applications on a mobile device (for example, an email application) in the deployed environment. Cisco ISE queries a connected MDM server for information about various attributes that you can use to create network authorization policies.

You can run multiple active MDM servers on your network, from different vendors. This allows you to route different endpoints to different MDM servers based on device factors such as location or device type.

Cisco ISE also integrates with MDM servers using the Cisco MDM Server Info APIs, Version 2 and later versions, to allow devices to access the network over VPN via Cisco AnyConnect 4.1 and Cisco Adaptive Security Appliances 9.3.2 or later.

In the following illustration, Cisco ISE is the enforcement point and the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution.

ISE 3.0 Admin Guide at 830.

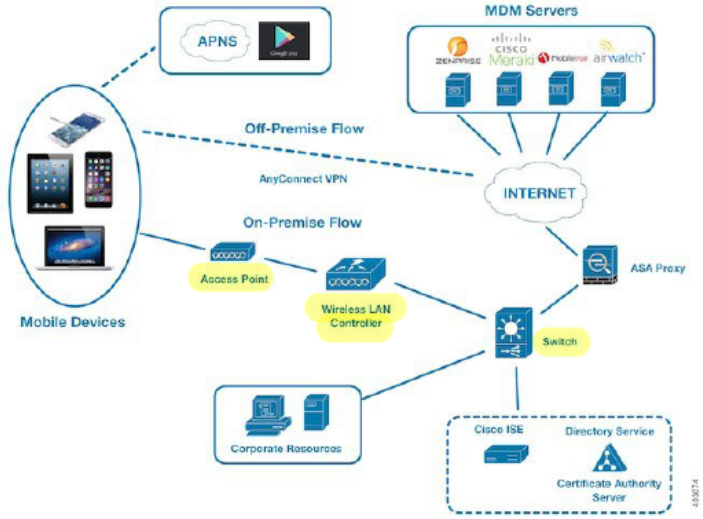
The "access devices" from which Cisco ISE "receiv[es] at an access point a request for access" are termed "endpoints" in Cisco's language. An endpoint is "typically a network-capable device that connect[s] to your network through wired and wireless network access devices and VPN. Endpoints can be personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, and so on." ISE 3.0 Admin Guide at 730; *see also id.* at 101 ("Here, an endpoint could mean users, PCs, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, or

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

other types of network devices."); 765 ("For example, a user registers a laptop with wired and wireless addresses.").

Cisco further describes how the request for access is "receiv[ed] at an access point[.]" Cisco's "access points" include its "switches, access routers, wireless access points, and other network access points." ISE 3.0 Admin Guide at 830.

Figure 33: MDM Interoperability with Cisco ISE



Configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. Cisco ISE applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network.

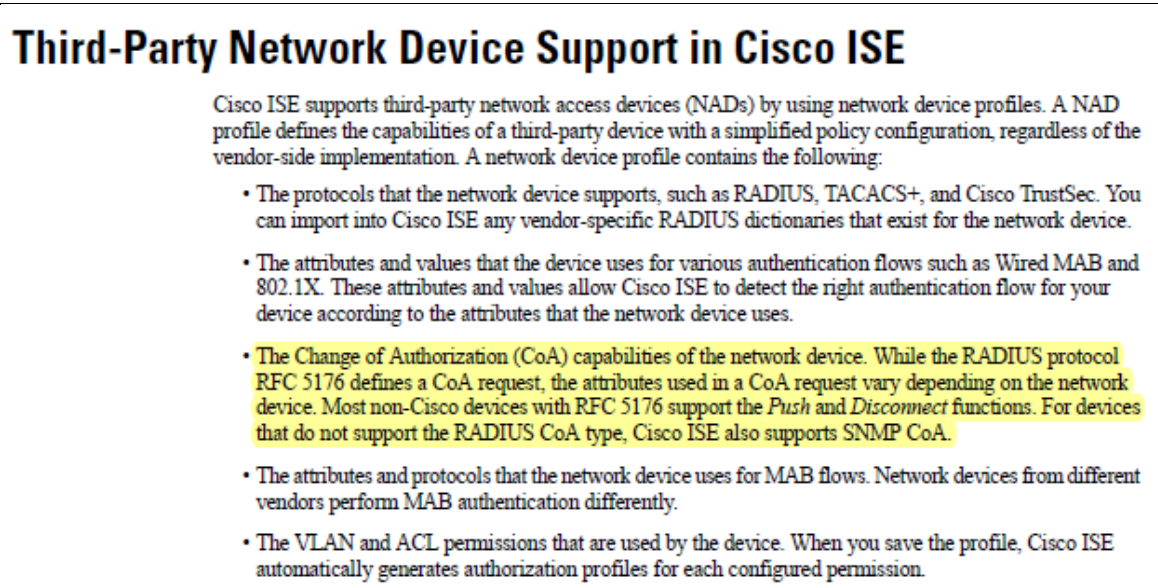
U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	See also Randomized and Changing MAC Deployment Guide at 43 (same); *see also* ISE 3.0 Admin Guide at 363 ("The device administrator is the user who logs into the network devices such as ***switches, wireless access points, routers, and gateways***, (normally through SSH), to perform the configuration and maintenance of the administered devices."). Cisco makes, uses, sells, and offers for sale a variety of ISE-validated products which customers oftentimes require with its ISE solutions including wireless access points, switches, LAN controllers, routers, servers, and remote access devices. A list of "access points" that are compatible with its ISE—including switches, routers, and remote access devices (i.e. firewalls)—is listed in Cisco's Identity Services Engine Network Component Compatibility documents, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014309 to INFOEX-CSCO_0014605. These Cisco documents describe "Cisco Identity Services Engine (ISE) validated compatibility with switches, wireless LAN controllers, and other policy enforcement devices as well as operating systems with which Cisco ISE interoperates." INFOEX-CSCO_0014586 at 14586. They further state, with respect to "Validated Network Access Devices," that "Cisco ISE supports interoperability with any Cisco or non-Cisco RADIUS client network access device (NAD) that implements common RADIUS behavior (similar to Cisco IOS 12.x) for standards-based authentication." INFOEX-CSCO_0014586 at 14587. These Cisco documents identify the claimed "access points" including both Cisco-made and third-party access points. Cisco also describes ISE-compatible third-party devices in its ISE 3.0 Admin Guide at 806-07, including those made by Aruba, Motorola, HP, Ruckus, Alcatel, Brocade, and Juniper. *See also* ISE 3.0 Admin Guide at 430 ("The [Wireless LAN Controller ("WLC")] can now log the guest in via the Cisco ISE RADIUS server. When this is complete, the WLC redirects the guest device's browser to the original URL destination. The Wireless LAN Controller (WLC) and the network access devices (NAD) requirements to support the original URL redirect for guest portals

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	are WLC 5760 and ***Cisco Catalyst 3850, 3650, 2000, 3000, and 4000 Series Access Switches*** running releases IOS-XE 3.6.0.E and 15.2(2)E."); 874 (Cisco AI Endpoint Analytics receives endpoint attribute data from multiple sources, such as ***Cisco Catalyst 9000 Series devices***[.]"); 697 ("The following devices support sending [Manufacturer Usage Descriptor ("MUD")] data to Cisco ISE: Cisco Catalyst 3850 Series Switches running Cisco IOS XE Version 16.9.1 & 16.9.2[,] Cisco Catalyst Digital Building Series Switches running Cisco IOS Version 15.2(6)E2[, and] Cisco Industrial Ethernet 4000 Series Switches running Cisco IOS Version 15.2(6)E2[.]"); 788 ("Cisco TrustSec-enabled devices use the TrustSec attributes to communicate with Cisco ISE. Cisco TrustSec-enabled devices, such as the Cisco Nexus 7000 Series Switches, Cisco Catalyst 6000 Series Switches, Cisco Catalyst 4000 Series Switches, and Cisco Catalyst 3000 Series Switches are authenticated using the Cisco TrustSec attributes that you define while adding Cisco TrustSec devices."). These hardware devices include those made by both Cisco and also third-parties. Cisco also describes ISE-compatible third-party devices in its ISE 3.0 Admin Guide at 806-07, including those made by Aruba, Motorola, HP, Ruckus, Alcatel, Brocade, and Juniper. Cisco describes in its ISE 3.0 Admin Guide an example where the request for access is received through a Cisco or third-party (that is, a non-Cisco) access device (termed a "network access device") in Cisco's literature. ISE 3.0 Admin Guide at 803-06.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	 ISE 3.0 Admin Guide at 803.
[16-b] applying a security policy to the access device in response to the request, application of the security policy including performing an	Cisco ISE "appl[ies] a security policy to the access device in response to the request, application of the security policy including performing an audit of the access device[,]" and induces others to do so. Cisco explains that "Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the ***appropriate posture agents*** for posturing services." Thus, Cisco "appl[ies] a security policy to the access device[,]" the application of which "include[es] performing an audit of the access device."

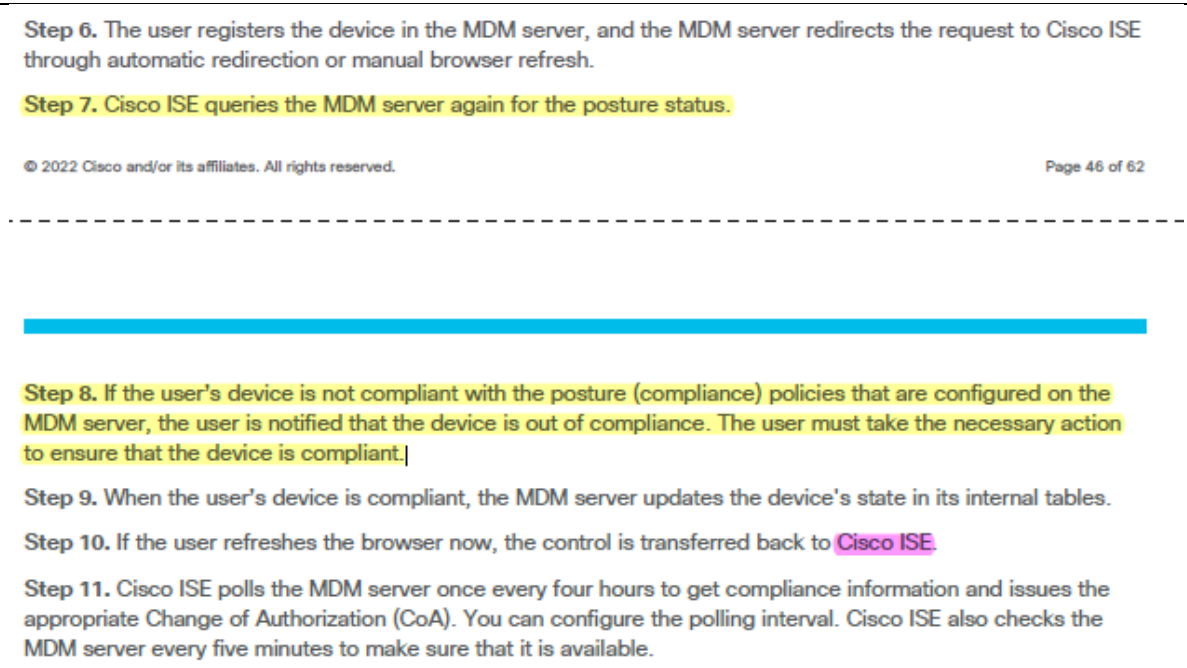
U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

audit of the access device;	• **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods. • **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation. • **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services. ISE 3.0 Admin Guide at 2. As described above (with respect to an MDM server integrated with ISE), "ISE is the enforcement point[, which] obtains data from the MDM server [and] then ***applies the appropriate access control policies*** to switches, access routers, wireless access points, and other network access points." Randomized and Changing MAC Deployment Guide at 43.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Handle random and changing MAC addresses with an MDM server To avoid issues caused by the use of the MAC address randomization method, configure Cisco ISE to identify endpoints that are connected to an MDM server by a unique device identifier instead of a MAC address. Mobile devices increasingly use random and changing MAC addresses for each SSID. This means that an endpoint presents different MAC addresses to the MDM server and to Cisco ISE. As a result, when the MDM server and Cisco ISE are integrated and an action is initiated for an endpoint, issues arise because the endpoint's identity is different in the two systems. In Cisco ISE, you can now work around this problem by configuring Cisco ISE to use a unique device identifier instead of MAC addresses. When an endpoint enrolls with an MDM server, the MDM server sends a certificate with a GUID value to the endpoint. The endpoint uses this certificate for authentication with Cisco ISE. Cisco ISE receives the GUID for the endpoint from the certificate. All communications between Cisco ISE and the MDM server now use the GUID to identify the endpoint, helping ensure accuracy and consistency between the two systems. Note that GUIDs are available only in certificate-based authentication methods. Basic authentication methods that use only a username and password will not be able to leverage the GUID-based solution. The Cisco ISE MDM APIs have been updated (Cisco ISE MDM APIs Version 3) to facilitate the gathering and management of GUID data. Currently, MobileIron supports Cisco ISE MDM APIs Version 3, and sends GUID information to Cisco ISE. Randomized and Changing MAC Deployment Guide at 48.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)



Step 6. The user registers the device in the MDM server, and the MDM server redirects the request to Cisco ISE through automatic redirection or manual browser refresh.

Step 7. Cisco ISE queries the MDM server again for the posture status.

© 2022 Cisco and/or its affiliates. All rights reserved.

Step 8. If the user's device is not compliant with the posture (compliance) policies that are configured on the MDM server, the user is notified that the device is out of compliance. The user must take the necessary action to ensure that the device is compliant.

Step 9. When the user's device is compliant, the MDM server updates the device's state in its internal tables.

Step 10. If the user refreshes the browser now, the control is transferred back to Cisco ISE.

Step 11. Cisco ISE polls the MDM server once every four hours to get compliance information and issues the appropriate Change of Authorization (CoA). You can configure the polling interval. Cisco ISE also checks the MDM server every five minutes to make sure that it is available.

Randomized and Changing MAC Deployment Guide at 46-47.

Thus, Cisco "appl[ies] a security policy to the access device[,]" the application of which "include[es] performing an audit of the access device."

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	In one example, Cisco explains how ISE "appl[ies] a security policy to the access device[,]" the application of which "include[es] performing an audit of the access device" when it operates with respect to both Cisco and third-party (i.e. non-Cisco) network access devices (NAD) (the claimed "access points"). A guest endpoint (the claimed "device") connects to the network through a Cisco or third-party ***network access device*** or ***NAD***. ISE applies a security policy. As described in step 11 below, Cisco ISE "validates endpoint compliance" and/or "authorizes the endpoint"—which show "performing an audit of the access device."

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

ISE 3.0 Admin Guide at 804; *see also id.* at 805-06 (schematics of same).

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

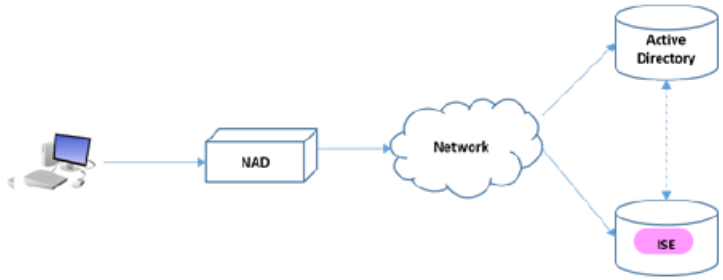
Finally, in another example—ISE's Easy Connect Enforcement Mode—ISE collects "accounting information (login information) about the user, from the security audit event." ISE 3.0 Admin Guide at 581. Furthermore, "[a]fter all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD ***(based on the appropriate policy managed in the policy service node***), and the user is provided access by the NAD to the network based on that policy." Thus, Cisco "appl[ies] a security policy to the access device[,]" the application of which "include[es] performing an audit of the access device."

Easy Connect Enforcement Mode Process Flow

The Easy Connect Enforcement mode process is as follows:

1. The user connects to the NAD from a wired endpoint (such as a PC for example).
2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD.
3. The user logs in to the domain and a security audit event is sent to Cisco ISE.
4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event.
5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy.

Figure 20: Easy Connect Enforcement Mode Basic Flow



Admin Guide at 580-81.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	See also above, claim elements 1-b & c, describing (1) several types of "information regarding the device" per those claims (for example, "hardware attributes" of the device), (2) several techniques within ISE for collecting such "information," including agents, and (3) the application of a security policy, the requirements of which "pertain[] to" such "information."
[16-c] providing information to the access device to improve compliance of the access device to the security policy, in response to the audit;	Cisco ISE "provid[es] information to the access device to improve compliance of the access device to the security policy, in response to the audit" and induces others to do so. Cisco describes "providing information to the access device to improve compliance of the access device to the security policy" as "remediating" that access device. Cisco describes "Posture Remediation Options," and also "Custom Posture Remediation Actions," which include "a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) remediation types." ISE 3.0 Admin Guide at 1059, 1061.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Posture Remediation Options

The following table provides a list of posture remediation options that are supported by the Cisco ISE Posture Agents for Windows and Macintosh, and the Web Agent for Windows.

Table 162: Posture Remediation Options

ISE Posture Agent for Windows	ISE Posture Agent for Macintosh OS X
Message Text (Local Check)	Message Text (Local Check)
URL Link (Link Distribution)	URL Link (Link Distribution)
File Distribution	—
Launch Program	—
Antivirus Definition Update	Antivirus Live Update
Antispyware Definition Update	Antispyware Live Update
Patch Management Remediation (AC 4.1 - and ISE 1.4)	—
Windows Update	—
WSUS	—

Custom Posture Remediation Actions

A custom posture remediation action is a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) remediation types.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	By "remediat[ing]" an endpoint, Cisco ISE "provid[es] information to [that endpoint] to improve compliance of the [that endpoint] to the security policy." Cisco also describes this in its ISE 3.0 Admin Guide at 1061, where, with respect to Antispyware remediation, it states, "You can create an antispyware remediation, which updates clients ***with up-to-date file definitions for compliance*** after remediation." The "up-to-date file definitions ***for compliance***" are the "information . . . to ***improve compliance***" with respect to an ISE security policy. *See also*, ISE 3.0 Admin Guide at 1062-64 (similar disclosures of Antivirus remediation, Patch Management Remediation, and Windows Server Update Services (WSUS) remediations, and remediation mechanisms including downloading files, launching programs/applications, or accessing remediation resources through a URL link). *See also* ISE 3.0 Admin Guide at 1029 (automatic updates in Windows clients): **Predefined Condition for Enabling Automatic Updates in Windows Clients** The pr_AutoUpdateCheck_Rule is a Cisco predefined condition, which is downloaded to the Compound Conditions window. This condition allows you to check whether the automatic updates feature is enabled on Windows clients. If a Windows client fails to meet this requirement, then the Network Access Control (NAC) Agents enforce the Windows client to enable (remediate) the automatic updates feature. After this remediation is done, the Windows client becomes posture compliant. The Windows update remediation that you associate in the posture policy overrides the Windows administrator setting, if the automatic updates feature is not enabled on the Windows client.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

and at 1048-50 (Patch Management Condition Settings):

Patch Management Condition Settings

The following table describes the fields in the **Patch Management Conditions** window. To view this window, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Patch Management Condition**.

Table 157: Patch Management Condition

Field Name	Usage Guidelines
Name	Enter the name of the patch management condition.
Description	Enter a description for the patch management condition.
Operating System	Choose an operating system to check the installation of a patch management software on the endpoint, or check the latest patch management definition file updates to which the condition is applied. You can select the Windows OS or macOS. You can also select more than one version of an operating system to create the patch management condition.
Vendor Name	Choose a vendor from the **Vendor Name** drop-down list. Based on your selection, the patch management products and their supported versions, check type, and minimum compliant module support details are displayed in the **Products for Selected Vendor** table. The list in the table changes according to the selected operating system.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Field Name	Usage Guidelines
Check Patches Installed	(Available only when you select the **Up To Date** check type) You can configure severity levels for missing patches, which are then deployed based on the severity. Choose one of the following options: • **Critical Only**: To check if critical software patches are installed on the endpoints in your deployment. • **Important and Critical**: To check if important and critical software patches are installed on the endpoints in your deployment. • **Moderate, Important, and Critical**: To check if moderate, important, and critical software patches are installed on the endpoints in your deployment. • **Low To Critical**: To check if low, moderate, important, and critical software patches are installed on the endpoints in your deployment. • **All**: To install the missing patches for all severity levels.

and also Randomized Changing MAC at 44 ("Cisco ISE performs the following functions with the external MDM server: . . . Handles device remediation: Endpoints are granted restricted access during remediation."); *and also* Identity Services Engine Data Sheet at 4 ("Automated device-compliance checks for device-posture and ***remediation*** options using Cisco Secure Client (formerly Anyconnect agent), Temporal and Agentless options . . ." and 7 ("Supports automatic ***remediation*** of PC clients as well as periodic reassessments . . .")

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Automated device-compliance checks for device-posture and remediation options using Cisco Secure Client (formerly Anyconnect agent), Temporal and Agentless options with custom scripts support. Cisco Secure Client Temporal and Agentless are two different ways to gather posture from endpoints beyond a full agent. Agentless option is supported from ISE 3.0 onwards lo Cisco Secure client also provide advanced VPN services for desktop and laptop checks. ISE also integrates with market-leading Mobile Device Management/Enterprise Mobility Management (MDM/EMM) vendors. MDM integration helps ensure that a mobile device is both secure and policy compliant before it is given access to the network.

. . .

Endpoint posture service	• Performs posture assessments to endpoints connected to the network.
	• Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM.
	• Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media.
	• Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies.
	• Provides hardware inventory for full network visibility.
	• Requires the AnyConnect 4.x agent for posture assessment on these OS platforms:
	  ◦ Windows 10 and later
	  ◦ Mac OS X 10.13 and later
	  ◦ Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu)

Identity Services Engine Data Sheet at 4, 7.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

[16-d] granting access to the less-restricted network based on satisfaction of the security policy by the updated access device; and	Cisco ISE "grant[s] access to the less-restricted network based on satisfaction of the security policy by the updated access device" and induces others to do so. Cisco describes "posture assessment requirements," premised on remediation action(s), and further that "All the clients connecting to your network ***must meet mandatory requirements*** during posture evaluation to become compliant on the network." ISE 3.0 Admin Guide at 1064. Because the access devices (which Cisco terms "clients") "***must meet mandatory requirements*** during posture evaluation to become compliant on the network"—and thus to have network access, Cisco ISE can thus "grant[] access' based on whether that device has been remediated (i.e., "based on satisfaction of the security policy by the updated access device"). **Posture Assessment Requirements** A posture requirement is a set of compound conditions with an associated remediation action that can be linked with a role and an operating system. All the clients connecting to your network must meet mandatory requirements during posture evaluation to become compliant on the network. Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies. If requirements are optional and clients fail these requirements, then the clients have an option to continue during posture evaluation of endpoints. ISE 3.0 Admin Guide at 1064; *see also id.* at 1065: **Mandatory Requirements** During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings. For example, you have specified a mandatory requirement with a user-defined condition to check the existence of C:\temp\text.file in the absolute path. If the file does not exist, the mandatory requirement fails and the user will be moved to Non-Compliant state.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	By way of another example—Windows Clients—Cisco states that if a Windows client fails to enable the automatic update feature, "then the Network Access Control (NAC) Agents enforce the Windows client to enable (remediate) the automatic updates feature. After this remediation is done, the Windows client becomes posture compliant." ISE 3.0 Admin Guide at 1029. So because the Windows client becomes posture-compliant once remediation is done, (*id.*), and because network access is premised on compliance (*see, e.g., id.* at 2), here again Cisco ISE "grant[s] access to the less-restricted network based on satisfaction of the security policy by the updated access device[.] **Predefined Condition for Enabling Automatic Updates in Windows Clients** The pr_AutoUpdateCheck_Rule is a Cisco predefined condition, which is downloaded to the Compound Conditions window. This condition allows you to check whether the automatic updates feature is enabled on Windows clients. If a Windows client fails to meet this requirement, then the Network Access Control (NAC) Agents enforce the Windows client to enable (remediate) the automatic updates feature. After this remediation is done, the Windows client becomes posture compliant. The Windows update remediation that you associate in the posture policy overrides the Windows administrator setting, if the automatic updates feature is not enabled on the Windows client. ISE 3.0 Admin Guide at 1029. *See also* Identity Services Engine Data Sheet at 4 ("***Automated*** device-compliance checks for device-posture and ***remediation*** options . . .), 7 ("Supports ***automatic remediation*** of PC clients as well as periodic reassessments . . .")

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Automated device-compliance checks for device-posture and remediation options using Cisco Secure Client (formerly Anyconnect agent), Temporal and Agentless options with custom scripts support. Cisco Secure Client Temporal and Agentless are two different ways to gather posture from endpoints beyond a full agent. Agentless option is supported from ISE 3.0 onwards Io Cisco Secure client also provide advanced VPN services for desktop and laptop checks. ISE also integrates with market-leading Mobile Device Management/Enterprise Mobility Management (MDM/EMM) vendors. MDM integration helps ensure that a mobile device is both secure and policy compliant before it is given access to the network.

. . .

Endpoint posture service	• Performs posture assessments to endpoints connected to the network.
	• Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM.
	• Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media.
	• Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies.
	• Provides hardware inventory for full network visibility.
	• Requires the AnyConnect 4.x agent for posture assessment on these OS platforms:
	  ◦ Windows 10 and later
	  ◦ Mac OS X 10.13 and later
	  ◦ Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu)

Identity Services Engine Data Sheet at 4, 7; *and also* ISE 3.0 Admin Guide at 1069 ("An endpoint that is postured noncompliant matches a posture requirement with a remediation action, and it should be granted limited network access to remediation resources in order to remediate itself.")

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Noncompliant Profile The posture compliance status of an endpoint is set to noncompliant when a matching posture policy is defined for that endpoint but it fails to meet all the mandatory requirements during posture assessment. An endpoint that is postured noncompliant matches a posture requirement with a remediation action, and it should be granted limited network access to remediation resources in order to remediate itself. ISE 3.0 Admin Guide at 1069.
[16-e] authenticating a user of the access device, wherein granting access is further based on the authentication.	Cisco ISE "authenticat[es] a user of the access device, wherein granting access is further based on the authentication" and induces others to do so. Cisco ISE "uses a wide range of ***authentication protocols*** to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods." By "using [an] authentication protocol to provide . . . [an] endpoint[] with a secure network access[,]" Cisco ISE "grant[s] access further based on the authentication."

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

- **Bring Your Own Device (BYOD)**: Cisco ISE allows your employees and guests to securely use their personal devices on your enterprise network. BYOD feature end users can use configured pathways to add their devices, and provision predefined authentications and levels of network access.
- **Asset Visibility**: Cisco ISE gives you visibility and control over who and what is on your network consistently, across wireless, wired, and VPN connections. Cisco ISE uses probes and device sensors to listen to the way devices connect to the network. The Cisco ISE profile database, which is extensive, then classifies the device. This gives the visibility and context you need to grant the right level of network access.
- **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods.
- **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation.

See ISE 3.0 Admin Guide at 2; *see also id.* (explaining that for the TACACS+ security protocol, "Network devices can be configured to query Cisco ISE for ***authentication and authorization of device administrator actions***."); *id.* (explaining that for ISE's bring-your-own-device (BYOD) feature, "end users can use configured pathways to add their devices, and ***provision predefined authentications and levels of network access***."); *see also id.* at 183 ("UTF-8 Credential ***Authentication***"), 214 ("Wildcard Certificates for HTTPS and ***Extensible Authentication Protocol*** Communication"), 268 (Configure Cisco ISE to Use Certificates for ***Authenticating*** Personal Devices); 269 (Create a Certificate ***Authentication*** Profile for TLS-Based Authentication); 270 (Create an Identity Source Sequence for ***TLS-Based Authentication***); (275 (Configure the ***Dot1X Authentication Policy*** Rule for TLS-Based Authentication); 276 ("Create Authorization Profiles for ***CentralWeb Authentication*** and Supplicant-Provisioning Flows"); 278-79 ("This section lists the

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	authorization profiles that you must create for enabling ***certificate-based authentication*** in Cisco ISE. You must have already created the ACLs (NSP-ACL and NSP-ACL-Google) on the wireless LAN controller (WLC)."); 280 (Cisco ISE CA Issues Certificates to [Adaptive Security Appliance ("ASA")] VPN Users) ("The ASA requests ***certificate-based authentication*** from the client. . . . The ASA proceeds to primary user ***authentication (AAA)*** using the username/ password and passes the information to the ***authentication server (ISE)***."); 354 (discussing exemplary "***authentication method[s]*** that [are] used by the RADIUS protocol"); 428-29 (Guest Access Web Authentication Options); 429-30 (Network Access Devices with Central Web Authentication Process, "In this scenario, the network access device (NAD) makes a new authorization request to the Cisco ISE RADIUS server from an unknown endpoint connection. The endpoint then receives a url-redirect to Cisco ISE. . . . If the guest device is connected to a NAD, the guest service interaction takes the form of a ***MAC Authentication Bypass (MAB) request*** that leads to a Guest portal Central WebAuth login. The following is an outline of the subsequent ***Central Web Authentication (Central WebAuth)*** process, which applies to both wireless and wired network access devices."); 430-31 (Wireless LAN Controller with ***Local Web Authentication*** Process); 431 (Wired Network Access Device with ***Local Web Authentication Process***); 433-34 (Device Registration ***Web Authentication*** Process); 512 ("In Cisco ISE, you can ***authenticate administrators*** via an external identity store such as Active Directory, LDAP, or RSA SecureID."); 513 (***External Authentication*** and Authorization); 635 ("Cisco ISE can ***authenticate*** a subject (user or host) against an [Lightweight Directory Access Protocol ('LDAP')] identity source . . ."); 862 (Password-Based Authentication); 1183 (Enable Your Switch to Support ***StandardWeb Authentication***); 1186 (Enable ***802.1X Port-Based Authentication*** for Switch Ports and Enable EAP for Critical Authentications); 1188-90 (Enable Switch Ports for 802.1X and [***MAC Authentication Bypass ("MAB")***]); 1232-38 ("Live Authentications: "You can monitor recent ***RADIUS authentications*** as they occur . . .").

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Cisco also explains that its ISE uses "***policy sets*** [with which] you [] manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group ***authentication and authorization policies*** within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type, and similar parameters." Cisco further explains that "[w]hen creating policy sets, you can configure the rules (configured with condition and results in order to choose . . . the identity sources on the ***authentication policy*** level[.]" Cisco further explains that hierarchically, authentication policy rules are applied first and before local policy exceptions, global policy exceptions and authorization policy rules. ISE 3.0 Admin Guide at 856.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Policy Sets

Cisco ISE is a policy-based, network-access-control solution, which offers network access policy sets, allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type, and similar parameters. When you install Cisco ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules.

When creating policy sets, you can configure these rules (configured with conditions and results) in order to choose the network access services on the policy set level, the identity sources on the authentication policy level, and network permissions on the authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE-supported dictionaries for different vendors. Cisco ISE allows you to create conditions as individual resuable policy elements.

The network access service to be used per policy set to communicate with the network devices is defined at the top level of that policy set. Network access services include:

- Allowed protocols—the protocols configured to handle the initial request and protocol negotiation.
- A proxy service—sends requests to an external RADIUS server for processing.

Note From the **Work Centers** > **Device Administration** , you can also select a relevant TACACS server sequence for your policy set. Use the TACACS server sequence to configure a sequence of TACACS proxy servers for processing.

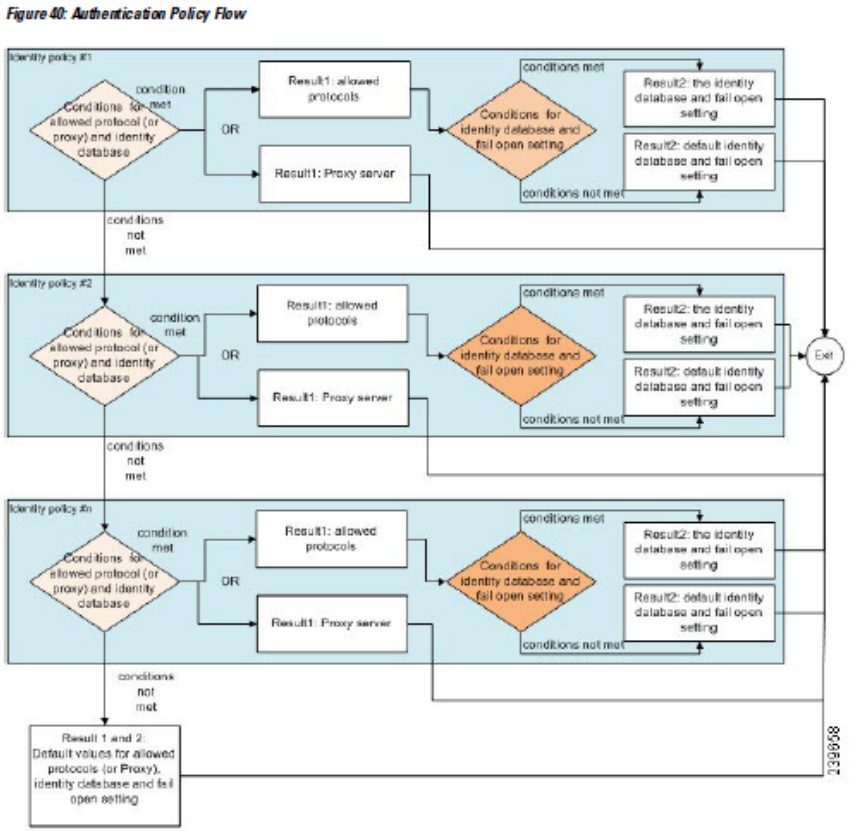
Policy sets are configured hierarchically, where the rule on the top level of the policy set, which can be viewed from the **Policy Set** table, applies to the entire set and is matched before the rules for the rest of the policies and exceptions. Thereafter, rules of the set are applied in this order:

1. Authentication policy rules
2. Local policy exceptions
3. Global policy exceptions
4. Authorization policy rules

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Cisco goes on to explain that "Each policy set can contain ***multiple authentication rules*** that together represent the authentication policy for that set. Priority of the authentication policies is determined based on the order to those policies as they appear within the policy set itself[.]" **Authentication Policies** Each policy set can contain multiple authentication rules that together represent the authentication policy for that set. Priority of the authentication policies is determined based on the order to those policies as they appear within the policy set itself (from the Set view page in the Authentication Policy area). Cisco ISE dynamically chooses the network access service (either an allowed protocol a server sequence) based on the settings configured on the policy set level, and thereafter checks the identity sources and results from the authentication and authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE dictionary. Cisco ISE allows you to create conditions as individual policy elements that can be stored in the Library and then can be reused for other rule-based policies. The identity method, which is the result of the authentication policy, can be any one of the following: . . .

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)



ISE 3.0 Admin Guide at 858-59; *see also id.* at 860 (Configure Authentication Policies: Define an authentication policy per policy set by configuring and maintaining multiple authentication rules, as necessary.").

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Cisco also explains that with its mobile device management (MDM) server integration with ISE, one can "perform authentication" using a Device Unique ID/Global Unique ID (DUID/GUID).

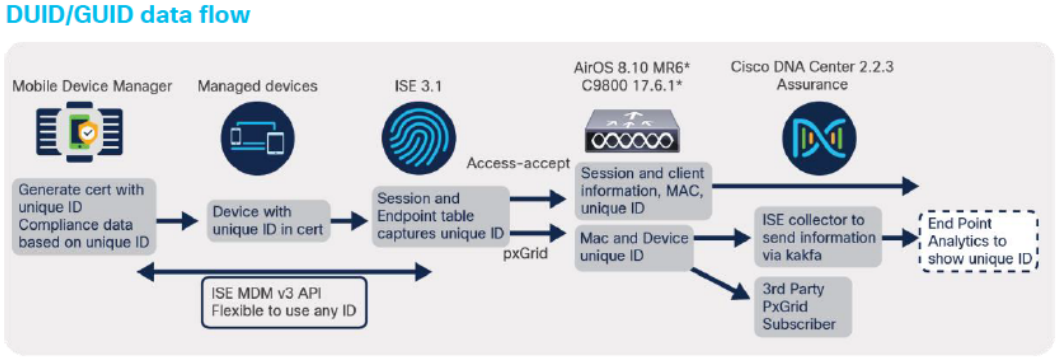


Figure 4.
DUID/GUID data flow

- This solution relies on the mobile device manager, also referred to as a device manager or unified endpoint manager (for example, Cisco Meraki, Airwatch, Intune, MobileIron, etc.), which manage devices in an enterprise infrastructure.
- ISE provides the provisioning of the device with the unique ID-based (DUID) certificates.
- The device presents this certificate during TLS-based authentication. ISE authorizes the devices and also reads the unique ID from the certificate.
- The DUID is used for compliance check with MDM servers and also a unique identifier of the device in the endpoint table.
- The randomized MAC address will not matter, as now the device will have a DUID using the ID in the certificate.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Randomized and Changing MAC Deployment Guide at 42.

Handle random and changing MAC addresses with an MDM server

To avoid issues caused by the use of the MAC address randomization method, configure Cisco ISE to identify endpoints that are connected to an MDM server by a unique device identifier instead of a MAC address. Mobile devices increasingly use random and changing MAC addresses for each SSID. This means that an endpoint presents different MAC addresses to the MDM server and to Cisco ISE. As a result, when the MDM server and Cisco ISE are integrated and an action is initiated for an endpoint, issues arise because the endpoint's identity is different in the two systems.

In Cisco ISE, you can now work around this problem by configuring Cisco ISE to use a unique device identifier instead of MAC addresses. When an endpoint enrolls with an MDM server, the MDM server sends a certificate with a GUID value to the endpoint. The endpoint uses this certificate for authentication with Cisco ISE. Cisco ISE receives the GUID for the endpoint from the certificate. All communications between Cisco ISE and the MDM server now use the GUID to identify the endpoint, helping ensure accuracy and consistency between the two systems.

Note that GUIDs are available only in certificate-based authentication methods. Basic authentication methods that use only a username and password will not be able to leverage the GUID-based solution.

The Cisco ISE MDM APIs have been updated (Cisco ISE MDM APIs Version 3) to facilitate the gathering and management of GUID data. Currently, MobileIron supports Cisco ISE MDM APIs Version 3, and sends GUID information to Cisco ISE.

Randomized and Changing MAC Deployment Guide at 48.

- **Time Interval for Compliance Device ReAuth Query:** When an endpoint is authenticated or reauthenticated, Cisco ISE uses a cache to get the MDM variables for that endpoint. If the age of the cached value is higher than the value configured in this field, Cisco ISE sends a new device query to the MDM server to get new values. If the compliance status has changed, Cisco ISE triggers the appropriate CoA.

Randomized and Changing MAC Deployment Guide at 50.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	In addition to making, using, offering for sale, and selling the ISE, Cisco also induces third-parties to infringe this claim as set forth in InfoExpress's 3-1 disclosures under 35 USC 271(b). For this claim, the underlying direct infringement is caused by the third-parties including Cisco's customers, subscribers, users and developers. And Cisco's acts of induced infringement including the following: as set forth herein, the Release Notes, Admin Guide, Randomized and Changing MAC Deployment Guide and Data Sheets for the ISE are all provided by Cisco to third-parties which provide deliberate and specific instruction and guidance for third-parties to use the ISE in a manner infringed by this claim. In addition, Cisco's Identity Services Engine Administrator Guide ("ISE AG) explains also provide such specific guidance of infringement to third-parties explaining that "[a]dministrators can use the admin portal to: Manage deployments, help desk operations, and network devices, and node monitoring and troubleshooting; Manage Cisco ISE services, policies, administrator accounts, and system configuration and operations." https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/admin_guide/b_ise_admin_3_3/b_ISE_admin_33_overview.html For example, the Admin Guide explains that its audience can be third party administrators ("Cisco ISE administrators can perform various administrative tasks based on the administrative group to which they belong. These administrators are critical. Grant administrative access only to users who are authorized to administer Cisco ISE in your network" ISE 3.0 Admin Guide at 13); developers ("On Facebook, create a Facebook application: a) Log on to http://developers.facebook.com and sign up as a developer," ISE 3.0 Admin Guide at. 397), and it instructs these third-parties on configuring the ISE, for example, with respect to the claimed authentication, compliance, and access point reconfiguration. With respect to this claim, the Admin Guide instructs third-parties how to "Create a Certificate Authentication Profile for TLS-Based Authentication." ISE 3.0 Admin Guide at 269-270. In particular, Cisco instructs these third-parties how to "use certificates for authenticating endpoints that connect to your network" and "defin[ing] a certificate authentication profile in Cisco ISE…" *Id.*

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	In another example, the Cisco's Admin guide instructs third-parties how to apply and/or configure security policies. For example, Cisco explains that the third-parties can "globally configure the Admin portal for posture services." ISE 3.0 Admin Guide at 1015. There, Cisco's Admin guide instructs third-parties how to "download updates automatically to the Cisco ISE through the web from Cisco. *Id*. Further, Cisco explains the various steps for how to "create a posture requirement." Id.. at. 1015-17; *see also id.* at 1066 (Cisco instructing third-parties on "Create[ing] Client Posture Requirements"); *id* at 1067 ("Posture Reassessment Configuration Settings"); *id*. at 1023 ("You can use the Posture Update window to download updates dynamically from the web."); *id.* at 1072 ("Creat[ing] a Posture Condition", "Creat[ing] Posture Remediation."); *id.* at 1073 ("Create Posture Policy"). The ISE AG provides third-parties with an "Administration Portal" which provides third-parties "Policy windows include[ing] tools for managing network security in the areas of authentication, authorization, profiling, posture, and client provisioning." https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/admin_guide/b_ise_admin_3_3/b_ISE_admin_33_basic_setup.html#reference_D93EF6652C8D4EB8B56EC6B857DA6F9A. Further, the ISE AG permits third-parties to create "Posture conditions" by following the following field path at the Administration Portal: "Policy -> Policy Elements -> Conditions -> Posture windows." Id. In another example, Cisco's Admin guide instructs third-parties with respect to "Quarantine [for] a Vulnerable Endpoint." ISE 3.0 Admin Guide at 1127. Specifically, Cisco explains that "You can choose to quarantine the endpoint, provide limited access (redirect to a different portal), or reject the request" and then provides three steps for doing so. *Id*. Similarly, the ISE AG explains to third-parties how they can configure the ISE to "perform the following operations to monitor and control network access through ANC: Quarantine: … Setting to the Quarantine state essentially moves an endpoint from its default VLAN to a specified

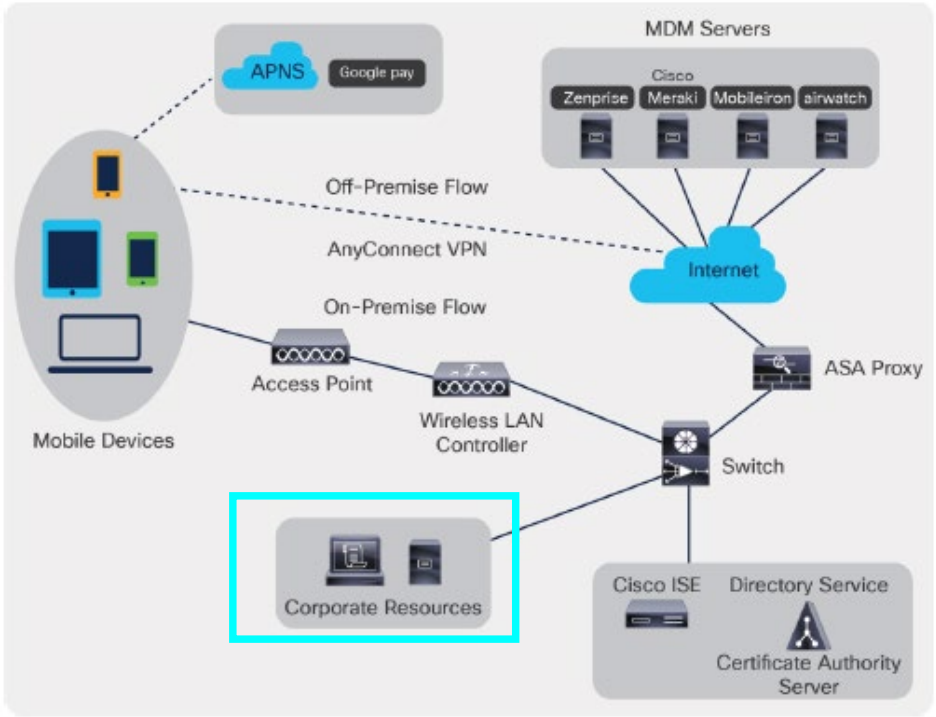
U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	Quarantine VLAN. You must define the Quarantine VLAN previously that is supported on the same NAS as the endpoint." https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/admin_guide/b_ise_admin_3_3/b_ISE_admin_33_maintain_monitor.html.
[22-preamble] A method of providing access over a communication network, the method comprising:	Cisco infringes this claim by making, using, testing, offering for sale, and selling the ISE product and system and through performance of each of the claimed steps and/or providing instructions and data from its servers to third-parties to perform at least one of the claimed steps, and as further described in claim 1. To the extent the preamble is limiting, Cisco ISE "provid[es] access over a communication network," as was explained above with respect to claim 16's preamble.
[22-a] receiving at an access point a request for access via a less-restricted network, the request coming from an access device;	Cisco ISE "receiv[es] at an access point a request for access via a less-restricted network, the request coming from an access device[,]" and induces others to do so, as was explained above with respect to claim element 16-a and 1-d.
[22-b] applying a security policy to the access device in response to the request, application of the	Cisco ISE "appl[ies] a security policy to the access device in response to the request, application of the security policy including performing an audit of the access device[,]" and induces others to do so, as was explained above with respect to claim element 16-b.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

security policy including performing an audit of the access device;	
[22-c] providing information to the access device to improve compliance of the access device to the security policy, in response to the audit; and	Cisco ISE "provid[es] information to the access device to improve compliance of the access device to the security policy, in response to the audit[,]" and induces others to do so, as was explained above with respect to claim element 16-c.
[22-d] granting access to the less-restricted network based on satisfaction of the security policy by the updated access device, the granting of access includes configuring the access point to allow the access.	Cisco ISE "grant[s] access to the less-restricted network based on satisfaction of the security policy by the updated access device, the granting of access includes configuring the access point to allow the access[,]" and induces others to do so. As was explained above with respect to claim element 16-d, Cisco ISE "grant[s] access to the less-restricted network based on satisfaction of the security policy by the updated access device[.]" Moreover, "granting of access includes configuring the access point to allow the access."

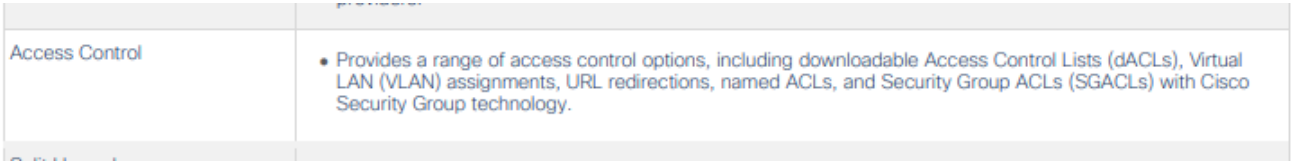
U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)



As shown, once ISE applies a security policy, it configures the access point to allow access (here, to "Corporate Resources)." Randomized Changing MAC at 43; *see also id.* at 57 ("If the device is registered with Cisco ISE, is registered with MDM, and is compliant with Cisco ISE and MDM policies, it is ***granted access to the network based on the access control policies configured in Cisco ISE***.").

Cisco also describes in its Data Sheet "a range of access control options" for this step, "including downloadable Access Control Lists (dACLs), Virtual LAN (VLAN) assignments, URL redirections,

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	named ACLs, and Security Group ACLs (SGACLs) with Cisco Security Group technology[.]" By using any or all of these methods, ISE "configur[es] the access point to allow the access[.]"  ISE Data Sheet at 5. With respect to the example above—involving both Cisco and third-party (i.e. non-Cisco) access points—once ISE determines that "requirements of the security policy are satisfied," it "sends the [change of authorization ("CoA")], authorizes the endpoint, and bypasses the sink hole[,] and then the "the guest user receives the appropriate [network] access based on the CoA." Thus, by sending CoA commands, Cisco ISE "configur[es] the access point to allow the access[.]"

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

Multiple VLANs may be connected to one network interface card by configuring a VLAN IP helper from the NAD configuration. For more information about configuring an IP helper, see the administration guide for the network device for instructions. For guest access flows that include VLANs with IP helpers, define a guest portal, and select that portal in an authorization profile that is bound to MAB authorization. For more information about guest portals, see the Cisco ISE Guest Services section in *Cisco ISE Admin Guide: Guest and BYOD* .

The following diagram displays a basic network setup when an Auth VLAN is defined (the Auth VLAN is connected directly to a Cisco ISE node).

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	In one further example described above—ISE's Easy Connect Enforcement Mode—ISE collects certain data, after which it "issues a CoA to the [network access device, ("NAD"] (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy." ISE 3.0 Admin Guide at 580-81. By issuing a CoA to the NAD, to provide the user access to the network, Cisco ISE "configur[es] the access point to allow the access[.]"

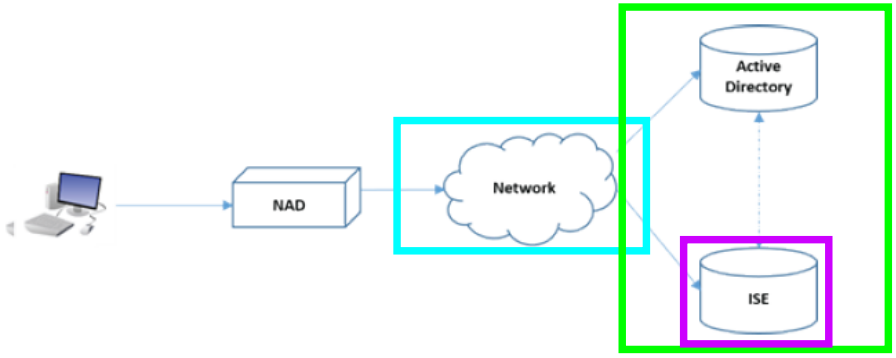
U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

Easy Connect Enforcement Mode Process Flow

The Easy Connect Enforcement mode process is as follows:

1. The user connects to the NAD from a wired endpoint (such as a PC for example).
2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD.
3. The user logs in to the domain and a security audit event is sent to Cisco ISE.
4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event.
5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy.

Figure 20: Easy Connect Enforcement Mode Basic Flow



ISE 3.0 Admin Guide at 581.

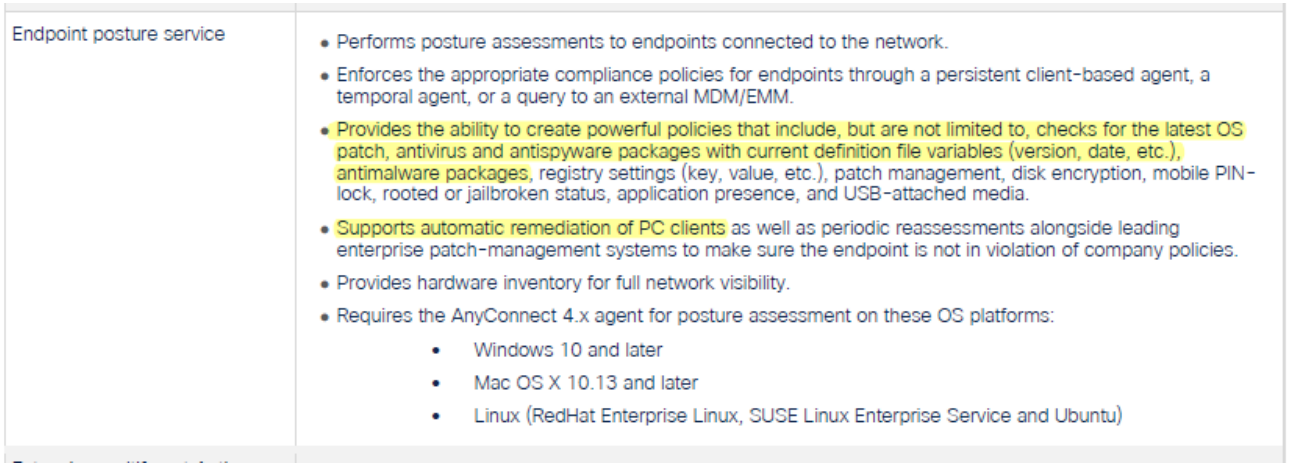
U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

23. The method of claim 22, wherein performing the audit includes using an agent on the access device to collect information regarding the access device.	Cisco ISE performs "[t]he method of claim 22, wherein performing the audit includes using an agent on the access device to collect information regarding the access device" and induces others to do so. As explained above with respect to claim element 1-b and claim 14, Cisco ISE "scan[s] the device to collect information regarding the device . . . wherein the scanning is performed using an agent on the device." Additionally, as explained above with respect to claim elements 16-b and 22-b, Cisco ISE "appl[ies] a security policy to the access device in response to the request, application of the security policy including performing an audit of the access device[.]" Thus, Cisco ISE "perform[s] the audit [by] using an agent on the access device to collect information regarding the access device."
25. The method of claim 22, wherein performing the audit includes receiving operating system information from the access device.	Cisco ISE performs "[t]he method of claim 22, wherein performing the audit includes receiving operating system information from the access device" and induces others to do so. With respect to claim element 1-b, Cisco ISE "scan[s] the device to collect information regarding the device. This information includes ***hardware attributes***. ISE 3.0 Admin Guide at 175. In turn, these hardware attributes can include "operating system information from the access device."

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

	• Status • Network Device Name • Location • UDID • IPv4 Address • Username • Hostname • OS Types • Anomalous Behavior • Endpoint Profile • Description • Endpoint Type ISE 3.0 Admin Guide at 175.

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

26. The method of claim 22, wherein the information includes software.	Cisco ISE performs "[t]he method of claim 22, wherein the information includes software" and induces others to do so. As discussed above with respect to claim elements 16-c and 22-c, Cisco ISE "***provid[es] information*** to the access device to improve compliance of the access device to the security policy, in response to the audit" and induces others to do so. Examples of such information include antivirus information, antispyware information, and Windows Server Update Services "service packs, hotfixes, and patches." *See* ISE 3.0 Admin Guide at 1061-1064; *see also* ISE Data Sheet at 7 (ISE "provides checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages . . ." and also "[s]upports automatic remediation . . . ").  ISE Data Sheet at 7; *and also* ISE 3.0 Admin Guide at 1029 (automatic updates in Windows clients). Thus, "the information includes software."

U.S. Patent No. 8,677,450 (Cisco's Identity Services Engine)

27. The method of claim 22, wherein the information includes a software update of software on the access device.	Cisco ISE performs "[t]he method of claim 22, wherein the information includes a software update of software on the access device" and induces others to do so. As discussed above with respect to claim 26, "the information [provided to an access device] includes software." Moreover, in all of the examples given, the "information include[d] a software update of software on the access device"—including those for antivirus, antispyware, Windows Server Update Services, and antimalware programs. Thus, "the information includes a software update of software on the access device."
28. The method of claim 27, wherein the software update is an update for an anti-virus program.	Cisco ISE performs "[t]he method of claim 27, wherein the software update is an update for an anti-virus program" and induces others to do so. As discussed above with respect to claim 27, "the information [provided to an access device] includes a software update of software on the access device." Moreover, examples of software updates for antivirus programs were described. *See also* ISE 3.0 Admin Guide at 1062; ISE Data Sheet at 7. Thus, "the software update is an update for an anti-virus program."

EXHIBIT F-4

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

U.S. Patent No. 8,347,350	Cisco's Identity Services Engine
[Claim 1—preamble] A method for network access control, the method comprising:	Cisco infringes this claim by making, using, testing, offering for sale, and selling the Identity Services Engine ("ISE") product and system and through performance of each of the claimed steps and/or providing instructions and data from its servers to third-parties to perform at least one of the claimed steps Further, subsequent to Cisco's making, using, testing, offering for sale, and selling of the ISE, Cisco offers services to third-parties and customers with respect to the ISE. For example, these can include "Technical Services," "Advisory Services," and "Cisco Talos Incidence Response" services. (https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/ise-licensing-guide-og.html). For technical services, for example, Cisco encourages customers to purchase "Cisco Smart Net Total Care" for Cisco ISE physical appliances and Software Support (SWSS) contracts for Cisco ISE virtual machines. For advisory services, Cisco offers Expert Services to address "your business objectives with the technology we offer" (including ISE). *Id*. And for the Talos Incident Response, Cisco provides a full suite of proactive and emergency services to help third-parties prepare, respond, and recover from a cybersecurity breach. Cisco explains that third-parties can "order and transact Cisco Talos Incident Response when ordering Cisco ISE subscriptions." *Id*. Additionally, and as set forth in InfoExpress's 3-1 disclosures, Cisco's ISE also includes Cisco's ISE (NAC) appliance. Specifically, these are Cisco-provided tangible hardware and "virtual appliances" on which ISE can be deployed. A list of accused ISE (NAC) Appliances (also referred to as "hardware platforms") which ISE supports, are disclosed in InfoExpress's Disclosure of Asserted Claims and Infringement Contentions per Patent L.R. 3-1 and 3-2 at Section II.B.2. These ISE (NAC) Appliances are listed in Cisco's Identity Services Engine Administrator Guides, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0001603 to 0014308, and also their Release Notes for ISE Releases

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	1.04, 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014606 to 0015185. Cisco's ISE (NAC) appliances are directed to "[g]ranting and denying network access" and using "attributes related to users and their devices" in "determining authorized network access." https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/datasheet-c78-726524.html.[1] Cisco further explains that its NAC appliance (known in one example as "The Cisco Secure Network Server") "supports Cisco's powerful network access and control security applications." *Id.* Further, Cisco explains that the "Cisco Secure Network Server… is configured specifically to support the Cisco Identity Services Engine (ISE) security application." *Id.* To the extent the preamble is limiting, Cisco's ISE[2] is "a security policy management platform that provides secure access to network resources" and thus embodies "[a] method for network access control[."

[1] Certain portions of the evidence cited herein identify and relate to the "Cisco Secure Network Server Data Sheet" for Cisco SNS-3715, SNS-3755, and SNS-3795 Secure Network Server. We understand that each other version of the Accused Technology relating to the Cisco ISE (NAC) appliances including ISE-3315-K9, ISE-3355-K9, and ISE-3395-K9; SNS-3415-K9 and SNS-3495-K9; SNS -3515-K9 and SNS-3595-K9; SNS-3615-K9, SNS-3655-K9, and SNS-3695-K9; and ISE Virtual Machine (S/M/L)-K9 are operationally and functionally the same with respect to and for the purposes of identifying infringement for each of the Asserted Claims.

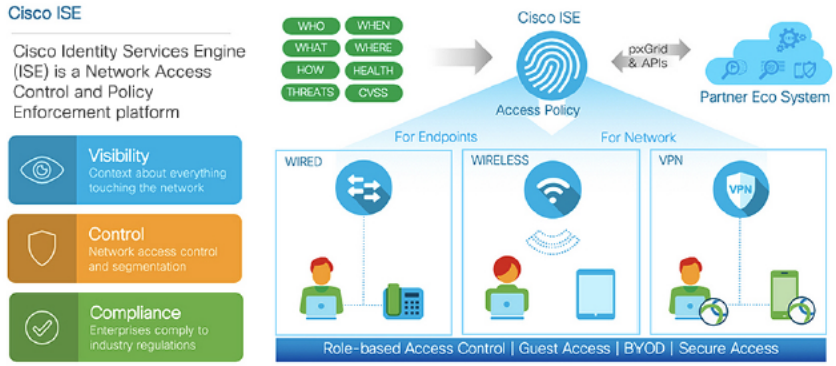
[2] Certain portions of the evidence cited herein identify and relate to the Cisco Identity Services Engine, Release version 3.0. We understand that each version of the Accused Technology is operationally and functionally the same with respect to and for the purposes of identifying infringement for each of the Asserted Claims.

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	Introduction to Cisco Identity Services Engine Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, wireless controllers, Virtual Private Network (VPN) gateways, 5GaaS networks, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation. Cisco ISE is available on secure network server appliances with different performance characterizations, and also as software that can be run on a virtual machines (VMs). Note that you can add more appliances to a deployment for better performance. Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also enables the configuration and management of distinct personas and services, thereby giving you the ability to create and apply services, where needed, in a network, but operate the Cisco ISE deployment as a complete and coordinated system. For detailed Cisco ISE ordering and licensing information, see the *Cisco Identity Services Engine Ordering Guide*. For information on monitoring and troubleshooting the system, see the "Monitoring and Troubleshooting Cisco ISE" section in the *Cisco Identity Services Engine Administrator Guide*. Release Notes for Cisco Identity Services Engine, Release 3.0 ("ISE 3.0 Release Notes") at 1, *available at* https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/release_notes/b_ise_30_rn.html (last accessed June 26, 2023). Cisco further describes ISE as a "Network Access Control and Policy Enforcement platform" which thereby "controls" "network access."

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

Cisco ISE Overview



Cisco Identity Services Engine (ISE) is an identity-based network access control and policy enforcement system. It functions as a common policy engine that enables endpoint access control and network device administration for enterprises.

You can leverage Cisco ISE to ensure compliance, enhance infrastructure security, and streamline service operations.

A Cisco ISE administrator can gather real-time contextual data for a network, including users and user groups (who?), device type (what?), access time (when?), access location (where?), access type (wired, wireless, or VPN) (how?), and network threats and vulnerabilities.

Source: Cisco, Identity Services Engine Administrator Guide, Release 3.0 ("ISE 3.0 Admin Guide"), at 1, *available at* https://www.cisco.com/c/en/us/td/docs/security/ise/30/admin_guide/b_ISE_admin_3_0.pdf (last visited May 31, 2023).

Cisco further describes its ISE as allowing a user "to choose . . . the network permissions on the authorization policy levels[,]" which further shows how it "controls" "network access."

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

Policy Sets

Cisco ISE is a policy-based, network-access-control solution, which offers network access policy sets, allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type, and similar parameters. When you install Cisco ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules.

When creating policy sets, you can configure these rules (configured with conditions and results) in order to choose the network access services on the policy set level, the identity sources on the authentication policy level, and network permissions on the authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE-supported dictionaries for different vendors. Cisco ISE allows you to create conditions as individual resuable policy elements.

The network access service to be used per policy set to communicate with the network devices is defined at the top level of that policy set. Network access services include:

- Allowed protocols—the protocols configured to handle the initial request and protocol negotiation.
- A proxy service—sends requests to an external RADIUS server for processing.

Id. at 856; *see also id.* at 546 ("A user role is a set of permissions that determine what tasks a user can perform and what services they can access on the Cisco ISE network. . . . .Cisco ISE allows you to ***restrict network access*** based on user attributes for both network access users and administrators.")

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

[1-a] receiving audit data pertaining to a device that does not have access to a less-restricted subset of a network;	Cisco's ISE "receiv[es] audit data pertaining to a device that does not have access to a less-restricted subset of a network" and induces others to do so. As to audit data, Cisco generally describes how "ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services." ISE 3.0 Admin Guide at 2. This information regarding "compliance [i.e.] posture, of endpoints" constitutes "audit data pertaining to a device" Furthermore, Cisco describes how ISE obtains this compliance/posture data "before allowing [endpoints] to connect—that is, when they "does not have access to a less-restricted subset of a network[.]" • **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services. ISE 3.0 Admin Guide at 2. Cisco also provides various examples of "audit data" that ISE "receiv[es]." In one example, the ISE receives "***hardware attributes of an endpoint***." ISE 3.0 Admin Guide at 174; *see also id.* at 174-5 (listing attributes), 176 ("Cisco ISE profiles the hardware attributes of a client's system, however, there may be a few hardware attributes Cisco ISE does not profile. . . . The hardware inventory data collection interval can be controlled . . . The default interval is 5 minutes."). These hardware attributes constitute "audit data" that Cisco ISE "receives." The ISE also receives "***endpoint attribute data***" which further includes "Profiling attributes: the Multi-Factor Classification attributes--Hardware Manufacturer, Hardware Model, Operating System, and

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	Endpoint Type[;] Trust Score attributes: Attributes related to Random MAC addresses, profiling changes, spoofing detection, and other behaviors that are monitored by Cisco AI Endpoint Analytics to calculate comprehensive Trust Scores for endpoints.[';] . . . Endpoint Trust Score [and] [Configuration Management Database ("CMDB")] attributes" *Id.* at 874-75; *see also* Randomized Changing MAC at 44 (listing six examples of device attributes). This endpoint attribute data constitutes "audit data" that Cisco ISE "receives." In another example, the ISE receives "simple posture conditions," including file conditions, registry conditions, application conditions, service conditions, and USB conditions on the client (the claimed "access device"). *Id.* at 1027. This simple posture conditions constitute "audit data" that Cisco ISE "receives." For both Cisco and third-party (i.e. non-Cisco) access points, ISE "validates endpoint compliance [and] . . . authorizes the endpoint[.]" Because ISE "validates compliance" here, and because (generally) ISE "validates" or "checks" an endpoint's compliance based off of information regarding the endpoint, by implication, ISE "receiv[es][audit data pertaining to a device." Moreover, because ISE first "validates" the endpoint, then "authorizes" it, and only then gives it "appropriate [network] access," that device did "not have access to a less-restricted subset of a network." ISE 3.0 Admin Guide at 804.

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

Multiple VLANs may be connected to one network interface card by configuring a VLAN IP helper from the NAD configuration. For more information about configuring an IP helper, see the administration guide for the network device for instructions. For guest access flows that include VLANs with IP helpers, define a guest

ISE 3.0 Admin Guide at 804.

With respect to guest devices, Cisco states that "you can . . . require [guests and non-guests] to first download t***he posture agent that checks their posture profile and verifies if their device is compliant***." ISE

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	3.0 Admin Guide at 401. By "check[ing] their posture profile and verif[ying] if their device is compliant[,]" ISE, by implication, "receiv[es][audit data pertaining to a device." Moreover, that device did "not have access to a less-restricted subset of a network"—prior to ISE "verif[ying] complian[ce]." **Guest Device Compliance** When guests and non-guests access the network through credentialed Guest portals, you can check their devices for compliance before they are allowed to gain access. You can route them to a Client Provisioning window and require them to first download the posture agent that checks their posture profile and verifies if their device is compliant. You can do this by enabling the option in the **Guest Device Compliance Settings** in a credentialed Guest portal, which displays the Client Provisioning window as part of the guest flow. **Note** Client posture assessment in guest flow supports only the Temporal agent. The Client Provisioning service provides posture assessments and remediations for guests. The Client Provisioning portal is available only with a Central Web Authorization (CWA) guest deployment. The guest login flow performs a CWA, and the credentialed Guest portal is redirected to the Client Provisioning portal after performing acceptable-use-policy and change-password checks. The posture subsystem performs a Change of Authorization (CoA) on the network access device to reauthenticate the client connection once the posture has been assessed. ISE 3.0 Admin Guide at 401. Cisco also describes the ISE with several ***agents***, which reside on the device (which "does not have access to a less-restricted subset of a network") and through which ISE can "receiv[e] audit data pertaining to [that] device[.]" These include: • The AnyConnect Agent (which can "report[] a complete list of running and installed applications" on the access device, ISE 3.0 Admin Guide at 1102-03; see also id. at 1057-58); • The AnyConnect Stealth Agent (which reports certain information back to ISE, id. at 1010-11); and

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	• The Cisco Temporal Agent, (which is a "temporary executable file that is run on the client to check the compliance status" and which "is removed from the client machine after the login session is terminated"). Similarly, Cisco ISE also uses an ***agentless plug-in***, used in agentless posture mode, whereby ISE "pushes the ***agentless plug-in*** to the client and launches the plug-in.[;] Posture evaluation runs on the client, and sends the status to Cisco ISE.[; and] Cisco ISE removes ***the agentless plug-in*** from the client" (*id.* at 1012-13).
[1-b] auditing the device in accordance with a security policy based at least in part on the audit data;	Cisco's ISE "audit[s] the device in accordance with a security policy based at least in part on the audit data" and induces others to do so. Cisco generally describes how "ISE allows you to check for compliance, also known as posture, of endpoints before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services." ISE 3.0 Admin Guide at 2. By "check[ing] for compliance [i.e. posture]" of endpoints, ISE "audit[s] the device in accordance with a security policy[.]" Furthermore, by having "endpoints receive the ***appropriate*** posture agents," Cisco ISE can be more specific about the "audit data" that it "receives" (per claim element 1-a) and which relates to its "security policy" (per this claim element). • **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services. ISE 3.0 Admin Guide at 2.

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	With respect to the examples of "audit data" that ISE "receives" (per the previous step 1-b), Cisco further shows how it "audit[s] the device in accordance with a security policy based at least in part on [that] audit data[.]" For the "***hardware attributes of an endpoint***," Cisco discloses that the ISE can "check posture compliance" with respect to these hardware attributes. *See* ISE 3.0 Admin Guide at 1032, 1051; *see also id.* at 2 ("Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network.") *and also id.* at 174-6 (listing hardware attributes collected, and the collection scheme). "By "check[ing] for compliance" with respect to these hardware attributes, Cisco ISE "audit[s] the device in accordance with a security policy based at least in part on [that] audit data[.]" As to the "***endpoint attribute data***" Cisco discloses that through the ISE, "a Cisco ISE administrator can then create ***specific authorization rules*** using these values"—and thereby create "a security policy." *See* ISE 3.0 Admin Guide at 874; *see also id.* at 874-75 (examples of these attributes); Randomized Changing MAC at 44 (listing six examples of device attributes). It follows that Cisco ISE could then "audit[] the device in accordance with a security policy [i.e., specific authorization rules] based at least in part on the audit data [i.e., the endpoint attribute data]." For "simple posture conditions," (*id.* at 1027), it was established that "Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network[,]" (*id.* at 2). By "check[ing] for compliance," with respect to these simple posture conditions, Cisco ISE "audit[s] the device in accordance with a security policy based at least in part on the audit data." With respect to both Cisco and third-party (i.e. non-Cisco) access points, ISE "validates endpoint compliance [and] . . . authorizes the endpoint[.]" Because Cisco ISE "validates compliance" here, and

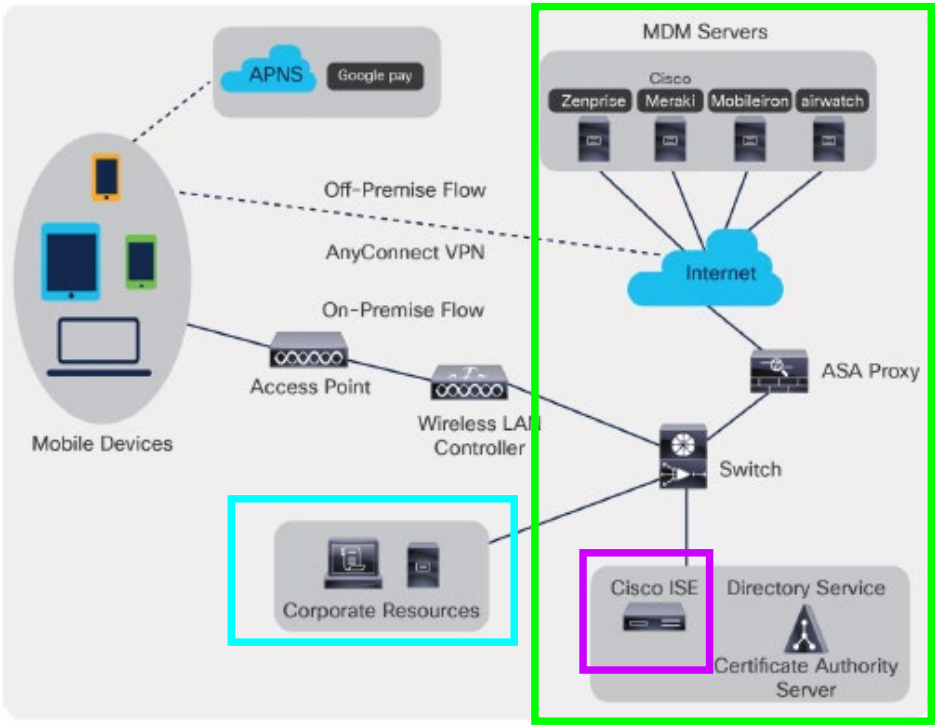
U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	because it (generally) "validates" or "checks" an endpoint's compliance based off of information regarding the endpoint, it "audit[s] the device in accordance with a security policy based at least in part on the audit data." **URL Redirect Mechanism and Auth VLAN** When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE. The following is an example of an Auth VLAN flow: 1. A guest endpoint connects to the NAD. 2. The network device sends the RADIUS or MAB request to Cisco ISE. 3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information. 4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID. 5. The guest endpoint receives network access. 6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service. 7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address. 8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE. 9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window. 10. The guest endpoint user logs in for authentication. 11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole. 12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network. You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN. Multiple VLANs may be connected to one network interface card by configuring a VLAN IP helper from the NAD configuration. For more information about configuring an IP helper, see the administration guide for the network device for instructions. For guest access flows that include VLANs with IP helpers, define a guest

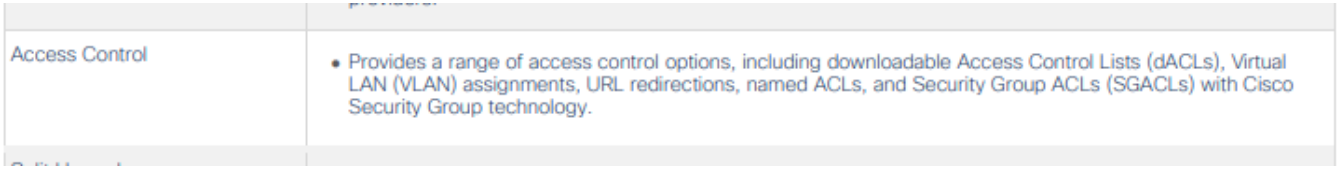
U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	ISE 3.0 Admin Guide at 804. For guest devices, Cisco states that "you can . . . require [guests and non-guests] to first download t***he posture agent that checks their posture profile and verifies if their device is compliant***." ISE 3.0 Admin Guide at 401. By "check[ing] their posture profile and verif[ying] if their device is compliant[,]" Cisco ISE, "audit[s] the device in accordance with a security policy based at least in part on the audit data." **Guest Device Compliance** When guests and non-guests access the network through credentialed Guest portals, you can check their devices for compliance before they are allowed to gain access. You can route them to a Client Provisioning window and require them to first download the posture agent that checks their posture profile and verifies if their device is compliant. You can do this by enabling the option in the **Guest Device Compliance Settings** in a credentialed Guest portal, which displays the Client Provisioning window as part of the guest flow. **Note** Client posture assessment in guest flow supports only the Temporal agent. The Client Provisioning service provides posture assessments and remediations for guests. The Client Provisioning portal is available only with a Central Web Authorization (CWA) guest deployment. The guest login flow performs a CWA, and the credentialed Guest portal is redirected to the Client Provisioning portal after performing acceptable-use-policy and change-password checks. The posture subsystem performs a Change of Authorization (CoA) on the network access device to reauthenticate the client connection once the posture has been assessed. ISE 3.0 Admin Guide at 401.
[1-c] reconfiguring an access point to allow access to the	Cisco's ISE "reconfigur[es] an access point to allow access to the less- restricted subset of the network in response to the security policy audit" and induces others to do so.

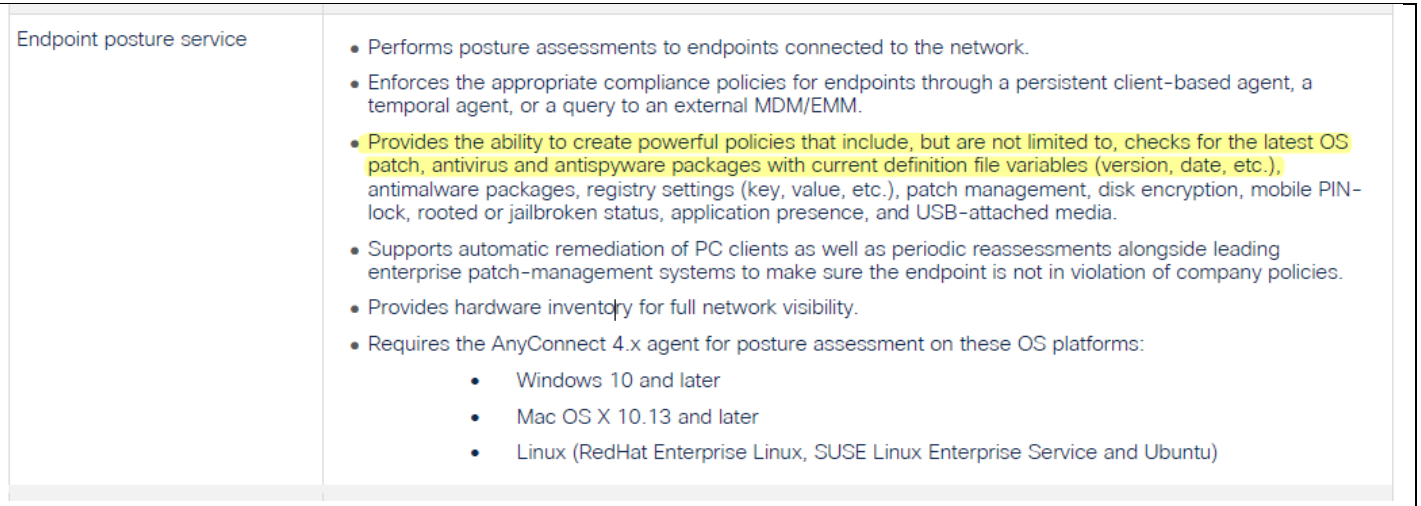
U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

less-restricted subset of the network in response to the security policy audit;	 As shown, ISE reconfigures an access point to allow the device (here, "Mobile Devices") to communicate with the less-restricted subset of the protected network (here, "Corporate Resources) "in response to [the] security policy audit." Randomized Changing MAC at 43; *see also id.* at 57 ("If the device is registered with Cisco ISE, is registered with MDM, and is compliant with Cisco ISE and MDM policies, it is ***granted access to the network based on the access control policies configured in Cisco ISE***.").

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	Cisco also describes in its Data Sheet "a range of access control options" for the ISE for this step, "including downloadable Access Control Lists (dACLs), Virtual LAN (VLAN) assignments, URL redirections, named ACLs, and Security Group ACLs (SGACLs) with Cisco Security Group technology[.]" By using any or all of these methods, ISE "reconfigur[es] an access point to allow access to the less-restricted subset of the network in response to the security policy audit"—for example, network resources. *See also* Data Sheet at 7 ("[ISE] [P]rovides the ability to ***create powerful policies*** that include, but are not limited to, ***checks*** for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PINlock, rooted or jailbroken status, application presence, and USB-attached media.")  Access Control • Provides a range of access control options, including downloadable Access Control Lists (dACLs), Virtual LAN (VLAN) assignments, URL redirections, named ACLs, and Security Group ACLs (SGACLs) with Cisco Security Group technology. ISE Data Sheet at 5.

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)



Endpoint posture service	• Performs posture assessments to endpoints connected to the network.
	• Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM.
	• Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media.
	• Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies.
	• Provides hardware inventory for full network visibility.
	• Requires the AnyConnect 4.x agent for posture assessment on these OS platforms:
	  ◦ Windows 10 and later
	  ◦ Mac OS X 10.13 and later
	  ◦ Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu)

ISE Data Sheet at 7.

By way of one example previously described—both Cisco and third-party (i.e. non-Cisco) access points—Cisco ISE "audit[s] the device in accordance with a security policy based at least in part on the audit data[,]" as shows above with respect to claim element 1-b. After doing so, Cisco ISE sends the [change of authorization ("CoA")], authorizes the endpoint, and bypasses the sink hole[,]"—thus it "reconfigure[es] an access point].]" Furthermore, upon sending such CoA, "the guest user receives the appropriate [network] access based on the CoA"—thus ISE "allow[s] access to the less-restricted subset of the network in response to the security policy audit."

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

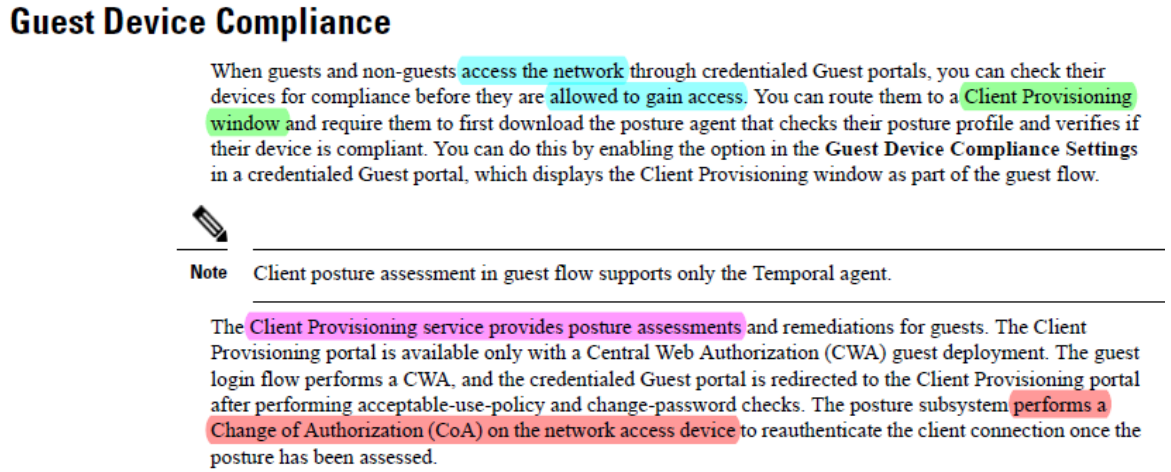
You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

Multiple VLANs may be connected to one network interface card by configuring a VLAN IP helper from the NAD configuration. For more information about configuring an IP helper, see the administration guide for the network device for instructions. For guest access flows that include VLANs with IP helpers, define a guest portal, and select that portal in an authorization profile that is bound to MAB authorization. For more information about guest portals, see the Cisco ISE Guest Services section in *Cisco ISE Admin Guide: Guest and BYOD* .

The following diagram displays a basic network setup when an Auth VLAN is defined (the Auth VLAN is connected directly to a Cisco ISE node).

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

By way of another example previously described—guest device compliance—Cisco states that after auditing such devices (as shown above with respect to claim element 1-b), ISE will "perform[] a Change of Authorization (CoA) on the network access device"—that is, it will "reconfigure the access point." Upon such a CoA, the device can "gain access to the network"—and thus ISE "allow[s] access to the less-restricted subset of the network[.]"



Guest Device Compliance

When guests and non-guests access the network through credentialed Guest portals, you can check their devices for compliance before they are allowed to gain access. You can route them to a Client Provisioning window and require them to first download the posture agent that checks their posture profile and verifies if their device is compliant. You can do this by enabling the option in the **Guest Device Compliance Settings** in a credentialed Guest portal, which displays the Client Provisioning window as part of the guest flow.

Note Client posture assessment in guest flow supports only the Temporal agent.

The Client Provisioning service provides posture assessments and remediations for guests. The Client Provisioning portal is available only with a Central Web Authorization (CWA) guest deployment. The guest login flow performs a CWA, and the credentialed Guest portal is redirected to the Client Provisioning portal after performing acceptable-use-policy and change-password checks. The posture subsystem performs a Change of Authorization (CoA) on the network access device to reauthenticate the client connection once the posture has been assessed.

ISE 3.0 Admin Guide at 401-02.

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

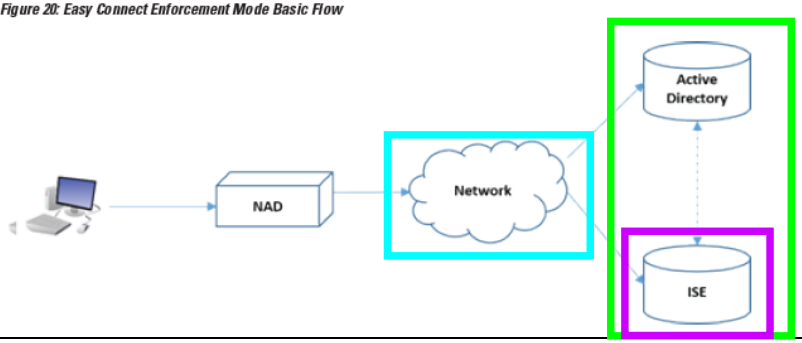
	By way of one final example—ISE's Easy Connect Enforcement Mode—ISE collects certain data, after which it "issues a CoA to the [network access device, ("NAD"] (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy." ISE 3.0 Admin Guide at 580-81. By issuing a CoA to the NAD, to provide the user access to the network, ISE "reconfigur[es] an access point to allow access to the less-restricted subset of the network in response to the security policy audit[.]"

Easy Connect Enforcement Mode Process Flow

The Easy Connect Enforcement mode process is as follows:

1. The user connects to the NAD from a wired endpoint (such as a PC for example).
2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD.
3. The user logs in to the domain and a security audit event is sent to Cisco ISE.
4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event.
5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy.

Figure 20: Easy Connect Enforcement Mode Basic Flow



U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	A list of "access points" that are compatible with its ISE—including switches, routers, and remote access devices (i.e. firewalls)— is listed in Cisco's Identity Services Engine Network Component Compatibility documents, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as which have been produced as INFOEX-CSCO_0014309 to INFOEX-CSCO_0014605. These Cisco documents describe "Cisco Identity Services Engine (ISE) validated compatibility with switches, wireless LAN controllers, and other policy enforcement devices as well as operating systems with which Cisco ISE interoperates." INFOEX-CSCO_0014586 at 14586. They further state, with respect to "Validated Network Access Devices," that "Cisco ISE supports interoperability with any Cisco or non-Cisco RADIUS client network access device (NAD) that implements common RADIUS behavior (similar to Cisco IOS 12.x) for standards-based authentication." INFOEX-CSCO_0014586 at 14587. These hardware devices include those made by both Cisco and also third-parties. Cisco also describes ISE-compatible third-party devices in its ISE 3.0 Admin Guide at 806-07, including those made by Aruba, Motorola, HP, Ruckus, Alcatel, Brocade, and Juniper.
[1-d] receiving updated audit data pertaining to the device subsequent to reconfiguring the access point; and **[1-e]** monitoring continued compliance of the	Cisco's ISE "receiv[es] updated audit data pertaining to the device subsequent to reconfiguring the access point; and monitor[s] continued compliance of the device with the security policy using the updated audit data" and induces others to do so. As described above with respect to claim element 1-a, Cisco's ISE employs several ***agents*** and an agentless plug-in through which ISE can "receiv[e] audit data pertaining to [that] device[.]" Cicso's ISE can use these agents in ***continuous endpoint attribute monitoring***. With respect to ***continuous endpoint attribute monitoring***, Cisco states that it takes place in the time "[a]fter initial posture [assessment]—that is, after "[1-b] ***auditing*** the device . . ." and after "[1-c] ***reconfiguring*** an access point to allow access to the less-restricted subset of the network in response to the security policy audit[.]"

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

device with the security policy using the updated audit data.	Cisco goes on to explain that for the ISE and "[a]fter initial posture, the AnyConnect agent scans the applications every X minute and sends ***the differences from the last scan to the server***. The server displays the complete list of running and installed applications." **Continuous Endpoint Attribute Monitoring** You can use the AnyConnect agent to continuously monitor different endpoint attributes to ensure that dynamic changes are observed during posture assessment. This improves the overall visibility of an endpoint and helps you create posture policies based on their behavior. The AnyConnect agent monitors applications that are installed and running on an endpoint. You can turn on and off the feature and configure how often the data should be monitored. By default, data is collected every 5 minutes and is stored in the database. During initial posture, AnyConnect reports a complete list of running and installed applications. After initial posture, the AnyConnect agent scans the applications every X minute and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications. ISE 3.0 Admin Guide at 1102-03. Thus the "the differences from the last scan to the server" constitute the "updated audit data pertaining to the device[.]" And since the AnyConnect agent "sends" this "updated audit data" to the server, the server "receives" it. And finally, it follows that with receipt of this information, ISE "monitor[s] continued compliance of the device with the security policy using the updated audit data"—similar to how it had done prior to reconfiguring. In addition to making, using, offering for sale, and selling the ISE, Cisco also induces third-parties to infringe this claim as set forth in InfoExpress's 3-1 disclosures under 35 USC 271(b). For this claim, the underlying direct infringement is caused by the third-parties including Cisco's customers, subscribers, users and developers. And Cisco's acts of induced infringement including the following: as set forth herein, the Release Notes, Admin Guide, Randomized and Changing MAC Deployment Guide and Data

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	Sheets for the ISE are all provided by Cisco to third-parties which provide deliberate and specific instruction and guidance for third-parties to use the ISE in a manner infringed by this claim. In addition, Cisco's Identity Services Engine Administrator Guide ("ISE AG) explains also provide such specific guidance of infringement to third-parties explaining that "[a]dministrators can use the admin portal to: Manage deployments, help desk operations, and network devices, and node monitoring and troubleshooting; Manage Cisco ISE services, policies, administrator accounts, and system configuration and operations." https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/admin_guide/b_ise_admin_3_3/b_ISE_admin_33_overview.html For example, the Admin Guide explains that its audience can be third party administrators ("Cisco ISE administrators can perform various administrative tasks based on the administrative group to which they belong. These administrators are critical. Grant administrative access only to users who are authorized to administer Cisco ISE in your network" ISE 3.0 Admin Guide at 13); developers ("On Facebook, create a Facebook application: a) Log on to http://developers.facebook.com and sign up as a developer," ISE 3.0 Admin Guide at. 397), and it instructs these third-parties on configuring the ISE, for example, with respect to the claimed authentication, compliance, and access point reconfiguration. With respect to this claim, the Admin Guide instructs third-parties how to "Create a Certificate Authentication Profile for TLS-Based Authentication." ISE 3.0 Admin Guide at 269-270. In particular, Cisco instructs these third-parties how to "use certificates for authenticating endpoints that connect to your network" and "defin[ing] a certificate authentication profile in Cisco ISE…" *Id.* In another example, the Cisco's Admin guide instructs third-parties how to apply and/or configure security policies. For example, Cisco explains that the third-parties can "globally configure the Admin portal for posture services." ISE 3.0 Admin Guide at 1015. There, Cisco's Admin guide instructs third-parties how to "download updates automatically to the Cisco ISE through the web from Cisco. *Id*. Further, Cisco explains the various steps for how to "create a posture requirement." Id.. at. 1015-17; *see also id.* at 1066 (Cisco instructing third-parties on "Create[ing] Client Posture Requirements"); *id* at 1067 ("Posture

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	Reassessment Configuration Settings"); *id*. at 1023 ("You can use the Posture Update window to download updates dynamically from the web."); *id.* at 1072 ("Creat[ing] a Posture Condition", "Creat[ing] Posture Remediation."); *id.* at 1073 ("Create Posture Policy"). The ISE AG provides third-parties with an "Administration Portal" which provides third-parties "Policy windows include[ing] tools for managing network security in the areas of authentication, authorization, profiling, posture, and client provisioning." https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/admin_guide/b_ise_admin_3_3/b_ISE_admin_33_basic_setup.html#reference_D93EF6652 C8D4EB8B56EC6B857DA6F9A. Further, the ISE AG permits third-parties to create "Posture conditions" by following the following field path at the Administration Portal: "Policy -> Policy Elements -> Conditions -> Posture windows." Id. In another example, Cisco's Admin guide instructs third-parties with respect to "Quarantine [for] a Vulnerable Endpoint." ISE 3.0 Admin Guide at 1127. Specifically, Cisco explains that "You can choose to quarantine the endpoint, provide limited access (redirect to a different portal), or reject the request" and then provides three steps for doing so. *Id*.
2. The method of claim 1, wherein monitoring of the device for continued compliance with the security	Cisco's ISE performs "[t]he method of claim 1, wherein monitoring of the device for continued compliance with the security policy includes continued communications with the device" and induces others to do so. As described above with respect to claim elements 1-d & e, Cisco "receiv[es] updated audit data pertaining to the device subsequent to reconfiguring the access point; and monitor[s] continued compliance of the device with the security policy using the updated audit data" and induces others to do so.

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

policy includes continued communications with the device.	Cisco explains how "After initial posture, the AnyConnect agent scans the applications every X minute and ***sends the differences from the last scan to the server***. The server displays the complete list of running and installed applications." ISE 3.0 Admin Guide at 1102-03. When the agent—which resides on the device—"sends the differences from the last scan to the server" this constitutes "continued communications with the device."
4. The method of claim 1, wherein the access point is reconfigured to allow access to a different subset of the network in response to the device failing to comply with the security policy while being monitored.	Cisco's ISE performs "[t]he method of claim 1, wherein the access point is reconfigured to allow access to a different subset of the network in response to the device failing to comply with the security policy while being monitored" and induces others to do so. By way of an example—Adaptive Network Control—Cisco describes how ISE can "quarantine" a user "essentially" by "mov[ing] an endpoint ***from its default VLAN*** to a ***specified Quarantine VLAN***." ISE 3.0 Admin Guide at 300. Similarly, ISE can "unquarantined" a user by "returning the endpoint to its original VLAN" and thus "permit[ting] full access to the network for an endpoint."

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

Adaptive Network Control

Adaptive Network Control (ANC) is a service that runs on the Administration node. This service monitors and controls network access of endpoints. ANC is invoked by the ISE administrator on the admin GUI, and also can be invoked through pxGrid from third-party systems. ANC supports wired and wireless deployments and requires an Advantage License.

You can use ANC to change the authorization state without having to modify the overall authorization policy of the system. ANC allows you to set the authorization state when you quarantine an endpoint. As a result, the established authorization policies where authorization policies are defined to check for ANCPolicy to limit or deny network access. You can unquarantine an endpoint for full network access. You can also shut down the port on the network attached system (NAS) that disconnects the endpoint from the network.

There are no limits to the number of users that can be quarantined at one time. Also, there are no time constraints on the quarantine period length.

You can perform the following operations to monitor and control network access through ANC:

- Quarantine: Allows you to use Exception policies (authorization policies) to limit or deny an endpoint access to the network. You must create Exception policies to assign different authorization profiles (permissions) depending on the ANCPolicy. Setting to the Quarantine state essentially moves an endpoint from its default VLAN to a specified Quarantine VLAN. You must define the Quarantine VLAN previously that is supported on the same NAS as the endpoint.
- Unquarantine: Allows you to reverse the quarantine status that permits full access to the network for an endpoint. This happens by returning the endpoint to its original VLAN.
- Shutdown: Allows you to deactivate a port on the NAS and disconnect the endpoint from the network. Once the port is shut down on the NAS to which an endpoint is connected, manually reset the port on the NAS again. This allows an endpoint to connect to the network, which is not available for wireless deployments.

Quarantine and unquarantine operations can be triggered from the session directory reports for active endpoints.

ISE 3.0 Admin Guide at 300. Thus by "mov[ing] an endpoint from its default VLAN to a specified Quarantine VLAN" Cisco ISE "the access point is reconfigured to allow access to a different subset of the network in response to the device failing to comply with the security policy." *See also* above with respect

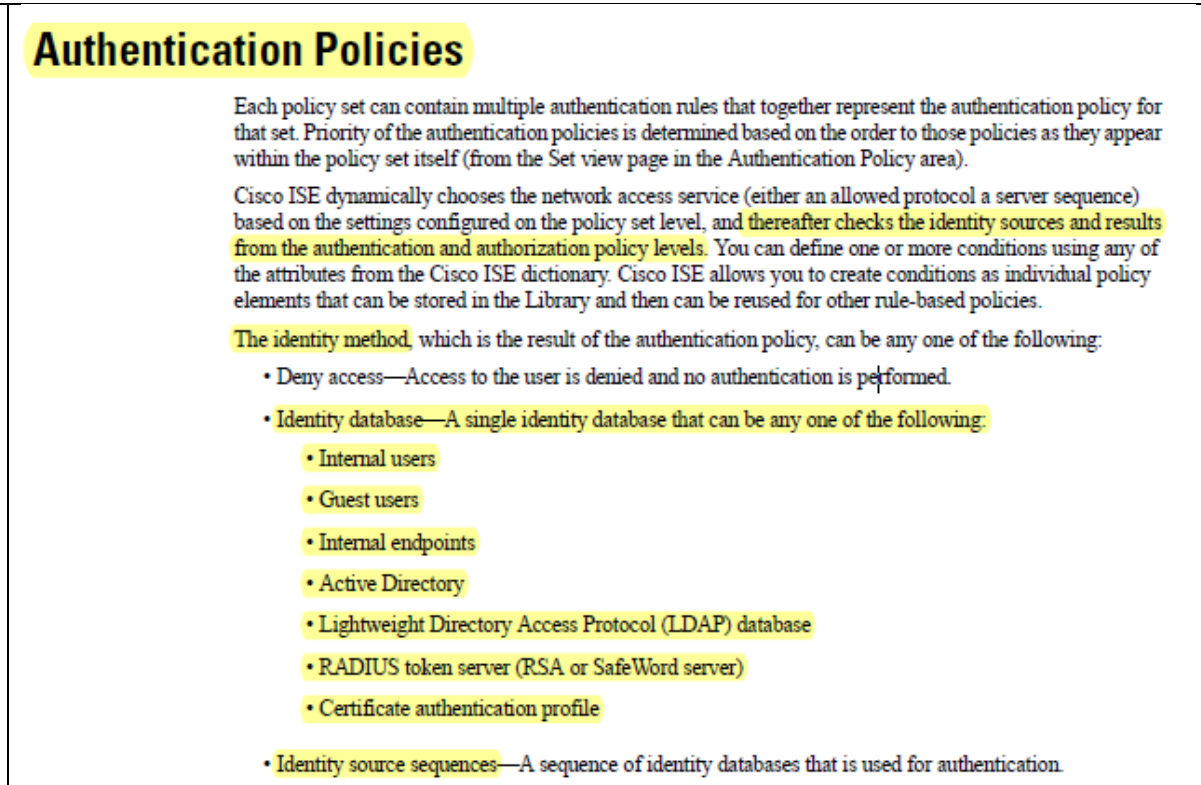
U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	to claim element 1-c, which explains how VLAN assignment is but one example within ISE of "reconfiguring" an access point, and which cites to the ISE 3.0 Data Sheet at 5). Furthermore, this example explains how ISE can "***monitor*** and control network access through ANC" — and thus this step takes place "while being monitored."
5. The method of claim 1, wherein the security policy includes authentication of the user of the device.	Cisco's ISE performs "[t]he method of claim 1, wherein the security policy includes authentication of the user of the device" and induces others to do so. Cisco's ISE "authenticat[es] a user of the access device" of a device (which Cisco terms an "endpoint"). Cisco explains how its ISE "***uses*** a wide range of ***authentication protocols*** to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods." ISE 3.0 Admin Guide at 2.

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	• **Bring Your Own Device (BYOD)**: Cisco ISE allows your employees and guests to securely use their personal devices on your enterprise network. BYOD feature end users can use configured pathways to add their devices, and provision predefined authentications and levels of network access. • **Asset Visibility**: Cisco ISE gives you visibility and control over who and what is on your network consistently, across wireless, wired, and VPN connections. Cisco ISE uses probes and device sensors to listen to the way devices connect to the network. The Cisco ISE profile database, which is extensive, then classifies the device. This gives the visibility and context you need to grant the right level of network access. • **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods. • **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation. Cisco also explains that with respect to authentication policies, Cisco ISE "checks the identity sources and results from the authentication and authorization policy levels." ISE 3.0 Admin Guide at 858. Furthermore, a "single identity database" can include, for example, "internal users" and guest users." *Id.*

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)



Authentication Policies

Each policy set can contain multiple authentication rules that together represent the authentication policy for that set. Priority of the authentication policies is determined based on the order to those policies as they appear within the policy set itself (from the Set view page in the Authentication Policy area).

Cisco ISE dynamically chooses the network access service (either an allowed protocol a server sequence) based on the settings configured on the policy set level, and thereafter checks the identity sources and results from the authentication and authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE dictionary. Cisco ISE allows you to create conditions as individual policy elements that can be stored in the Library and then can be reused for other rule-based policies.

The identity method, which is the result of the authentication policy, can be any one of the following:

- Deny access—Access to the user is denied and no authentication is performed.
- Identity database—A single identity database that can be any one of the following:
  - Internal users
  - Guest users
  - Internal endpoints
  - Active Directory
  - Lightweight Directory Access Protocol (LDAP) database
  - RADIUS token server (RSA or SafeWord server)
  - Certificate authentication profile
- Identity source sequences—A sequence of identity databases that is used for authentication.

By way of one example, Cisco's ISE provides authentication via Cisco's Adaptive Security Appliances (ASA) (i.e., firewalls): "The ASA proceeds to ***primary user authentication (AAA) using the username/password*** and passes the information to the authentication server (ISE)." ISE 3.0 Admin Guide at 280-81. And in a later step, "The ***user can again authenticate*** using the certificate and a normal VPN connection is established." *Id.* By ***using "primary user authentication (AAA) using the username/password"*** Cisco "authenticat[es] a user of the access device[.]"

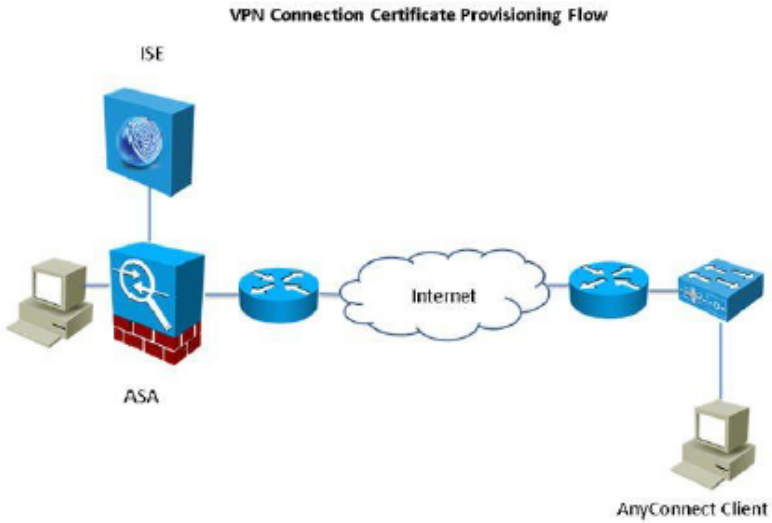
U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	Cisco ISE CA Issues Certificates to ASA VPN Users ISE CA issues certificates to client machines connecting over ASA VPN. Using this feature, you can automatically provision certificates to end devices that connect over ASA VPN. Cisco ISE uses the Simple Certificate Enrollment Protocol (SCEP) for enrollment and to provision certificates to the client machines. The AnyConnect client sends the SCEP request to the ASA over an HTTPS connection. The ASA evaluates the request and enforces policies before it relays the request to Cisco ISE over an HTTP connection established between Cisco ISE and ASA. The response from the Cisco ISE CA is relayed back to the client. The ASA cannot read the contents of the SCEP message and functions as a proxy for the Cisco ISE CA. The Cisco ISE CA decrypts the SCEP message from the client and sends the response in an encrypted form. The ISE CA SCEP URL is http://<*IP Address or FQDN of ISE CA server*>:9090/auth/caservice/pkiclient.exe. If you are using FQDN of the ISE node, the DNS server connected to ASA must be able to resolve the FQDN. You can configure certificate renewal before expiration in the AnyConnect Client profile. If the certificate has already expired, the renewal flow is similar to a new enrollment. Supported versions include: • Cisco ASA 5500 Series Adaptive Security Appliances that run software version 8.x • Cisco AnyConnect VPN version 2.4 or later

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

VPN Connection Certificate-Provisioning Flow

Figure 10: Certificate Provisioning for ASA VPN Users



1. The user initiates a VPN connection.

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	2. The AnyConnect client scans the client machine and sends the attributes such as the unique device identifier (for example, IMEI) to the ASA. 3. The ASA requests certificate-based authentication from the client. The authentication fails because there is no certificate. 4. The ASA proceeds to primary user authentication (AAA) using the username/password and passes the information to the authentication server (ISE). a. If authentication fails, the connection is terminated immediately. b. If authentication passes, limited access is granted. You can configure dynamic access policies (DAP) for client machines that request a certificate using the aaa.cisco.sceprequired attribute. You can set the value for this attribute to "true" and apply ACLs and web ACLs. 5. The VPN connection is established after the relevant policies and ACLs are applied. The client starts key generation for SCEP only after AAA authentication succeeds and the VPN connection is established. 6. The client starts the SCEP enrollment and sends SCEP requests to ASA over HTTP. 7. ASA looks up the session information of the request and relays the request to ISE CA, if the session is allowed for enrollment. 8. ASA relays the response from ISE CA back to the client. 9. If enrollment succeeds, the client presents a configurable message to the user and disconnects the VPN session. 10. The user can again authenticate using the certificate and a normal VPN connection is established. ISE 3.0 Admin Guide at 280-81; *see also id.* at 635 ("Cisco ISE can ***authenticate*** a subject (user or host) against an [Lightweight Directory Access Protocol ('LDAP')] identity source . . ."); 862 (Password-Based Authentication).
6. The method of claim 4, wherein an agent running on the device	Cisco's ISE performs "[t]he method of claim 4, wherein an agent running on the device collects the audit data" and induces others to do so.

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

collects the audit data.	Cisco generally describes how "ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the ***appropriate posture agents*** for posturing services." ISE 3.0 Admin Guide at 2. • **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services. ISE 3.0 Admin Guide at 2. As explained above with respect to claim element 1-a, Cisco describes several specific agents, through which ISE can "receiv[e] audit data pertaining to [that] device[.]" These include: • The ***AnyConnect Agent*** (which can "report[] a complete list of running and installed applications" on the access device, ISE 3.0 Admin Guide at 1102-03; *see also id.* at 1057-58); • The ***AnyConnect Stealth Agent*** (which reports certain information back to ISE, *id.* at 1010-11); and • The ***Cisco Temporal Agent***, (which is a "temporary executable file that is run on the client to check the compliance status" and which "is removed from the client machine after the login session is terminated").
7. The method of claim 6, further comprising updating the device to comply with the security	Cisco's ISE performs "[t]he method of claim 6, further comprising updating the device to comply with the security policy when the device fails to comply with the security policy" and induces others to do so. Cisco describes "Posture Remediation Options," and also "Custom Posture Remediation Actions," which include "a file, a link, an antivirus or antispyware definition ***updates***, launching programs, Windows

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

policy when the device fails to comply with the security policy.

updates, or Windows Server Update Services (WSUS) remediation types." ISE 3.0 Admin Guide at 1059, 1061.

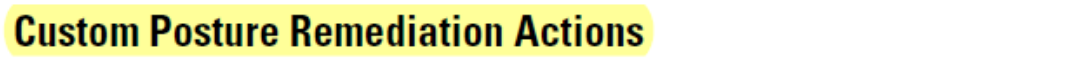
Posture Remediation Options

The following table provides a list of posture remediation options that are supported by the Cisco ISE Posture Agents for Windows and Macintosh, and the Web Agent for Windows.

Table 162: Posture Remediation Options

ISE Posture Agent for Windows	ISE Posture Agent for Macintosh OS X
Message Text (Local Check)	Message Text (Local Check)
URL Link (Link Distribution)	URL Link (Link Distribution)
File Distribution	—
Launch Program	—
Antivirus Definition Update	Antivirus Live Update
Antispyware Definition Update	Antispyware Live Update
Patch Management Remediation (AC 4.1 - and ISE 1.4)	—
Windows Update	—
WSUS	—

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

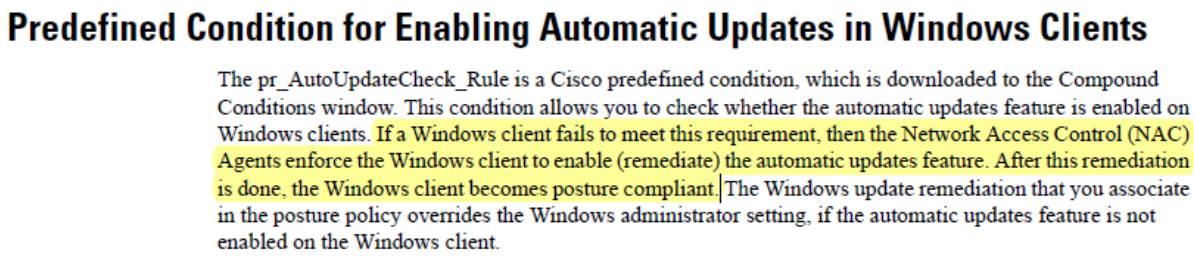


Custom Posture Remediation Actions

A custom posture remediation action is a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) remediation types.

By "remediat[ing]" an endpoint, Cisco "update[s] the device to comply with the security policy when the device fails to comply with the security policy." *See also* ISE 3.0 Admin Guide at 1061-64 ("Add an Antispyware Remediation: You can create an antispyware remediation, which ***updates clients*** with up-to-date file definitions for compliance after remediation." And similar disclosures of updates including Antivirus Remediation, Patch Management Remediation, and Windows Server Update Services (WSUS) remediations, and remediation mechanisms including downloading files, launching programs/applications, or accessing remediation resources through a URL link).

Cisco similarly describes, with respect to automatic updates in Windows clients, "After this remediation is done, the Windows client becomes posture compliant." ISE 3.0 Admin Guide at 1029. Thus, because the update brings the device into "posture compliance," it is performed when "when the device fails to comply with the security policy."



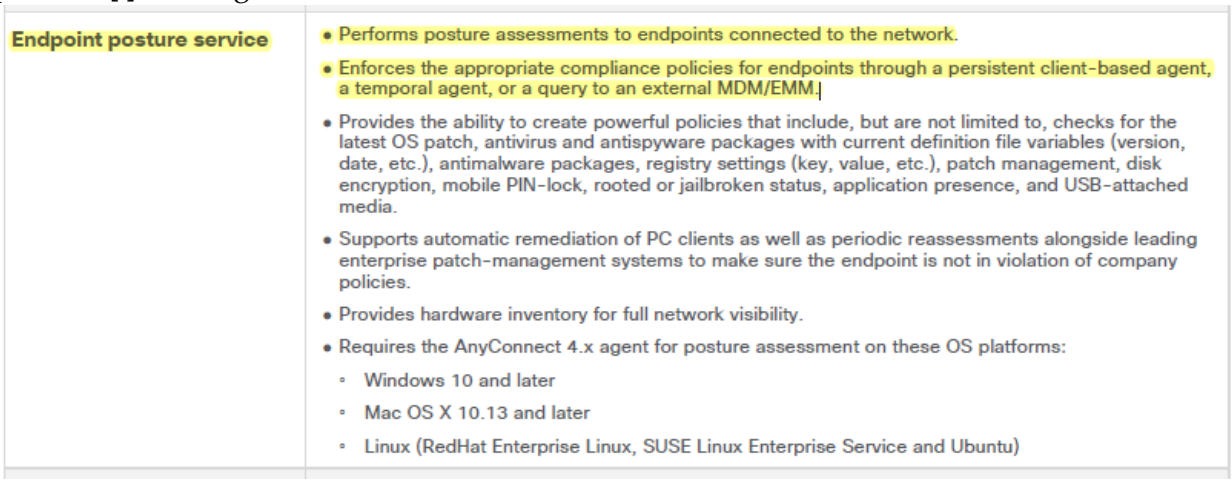
Predefined Condition for Enabling Automatic Updates in Windows Clients

The pr_AutoUpdateCheck_Rule is a Cisco predefined condition, which is downloaded to the Compound Conditions window. This condition allows you to check whether the automatic updates feature is enabled on Windows clients. If a Windows client fails to meet this requirement, then the Network Access Control (NAC) Agents enforce the Windows client to enable (remediate) the automatic updates feature. After this remediation is done, the Windows client becomes posture compliant. The Windows update remediation that you associate in the posture policy overrides the Windows administrator setting, if the automatic updates feature is not enabled on the Windows client.

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

8. The method of claim 6, wherein the security policy audit is based at least in part on audit data collected by the agent concerning operating system of the device.	Cisco's ISE performs "[t]he method of claim 6, wherein the security policy audit is based at least in part on audit data collected by the agent concerning operating system of the device" and induces others to do so. Cisco states that ***hardware attributes*** (one type of "audit data" discussed with respect to claim element 1-a) can include "operating system types. ISE 3.0 Admin Guide at 175. • Status • Network Device Name • Location • UDID • IPv4 Address • Username • Hostname • OS Types • Anomalous Behavior • Endpoint Profile • Description • Endpoint Type

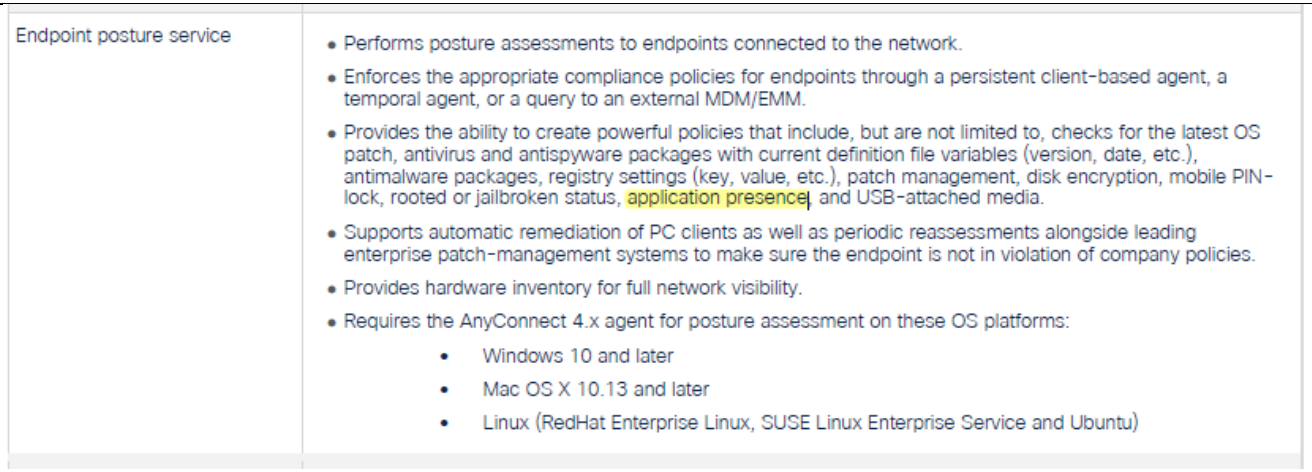
U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	ISE 3.0 Admin Guide at 175. Thus "the security policy audit is based at least in part on audit data collected by the agent concerning operating system of the device."
9. The method of claim 6, wherein the security policy audit is based at least in part on audit data collected by the agent, and that concerns antivirus software on the device.	Cisco's ISE performs "[t]he method of claim 6, wherein the security policy audit is based at least in part on audit data collected by the agent, and that concerns antivirus software on the device" and induces others to do so. Cisco states that it "[p]erforms posture assessments to endpoints connected to the network" and "enforces the appropriate compliance policies for [those] endpoints" through different mechanisms. Such "security policies" "include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages . . . antimalware packages . . . patch management . . . rooted or jailbroken status [and] application presence[,]" among others.  **Endpoint posture service** • Performs posture assessments to endpoints connected to the network. • Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM. • Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media. • Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies. • Provides hardware inventory for full network visibility. • Requires the AnyConnect 4.x agent for posture assessment on these OS platforms: ◦ Windows 10 and later ◦ Mac OS X 10.13 and later ◦ Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu) ISE Data Sheet at 6. Thus, "the security policy audit is based at least in part on audit data collected by the agent, and that concerns antivirus software on the device."

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

10. The method of claim 6, wherein the security policy audit is based at least in part on audit data collected by the agent, and that concerns other devices coupled to the device.	Cisco's ISE performs "[t]he method of claim 6, wherein the security policy audit is based at least in part on audit data collected by the agent, and that concerns other devices coupled to the device" and induces others to do so. Cisco states, with respect to "hardware attributes," that they include a field for "attached devices." ISE 3.0 Admin Guide at 174-75. Cisco further explains that "You can click the number in the ***Attached Devices*** column that corresponds to an endpoint to view the Name, Category, Manufacturer, Type, Product ID, and Vendor ID of the USB devices that are currently attached to the endpoint." *Id.*; *see also id.* at 1027 (USB Conditions), 1051 (USB Condition Settings), 1057 (USB_Block "[e]nsures that the endpoint device does not have any USB storage devices connected"). Thus, because Cisco's ISE can determine "attached devices" such as a USB (which are so attached to the endpoint), it follows that "the security policy audit is based at least in part on audit data collected by the agent, and that concerns other devices coupled to the device."
13. The method of claim 6, wherein the security policy audit is based at least in part on audit data collected by the agent, and that concerns applications executing on the device.	Cisco's ISE performs "[t]he method of claim 6, wherein the security policy audit is based at least in part on audit data collected by the agent, and that concerns applications executing on the device" and induces others to do so. Cisco states that it "[p]erforms posture assessments to endpoints connected to the network" and "enforces the appropriate compliance policies for [those] endpoints" through different mechanisms. Such "security policies" "include, but are not limited to, checks for . . . application presence[,]" among other criteria. Thus "the security policy audit is based at least in part on audit data collected by the agent, and that concerns applications executing on the device."

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

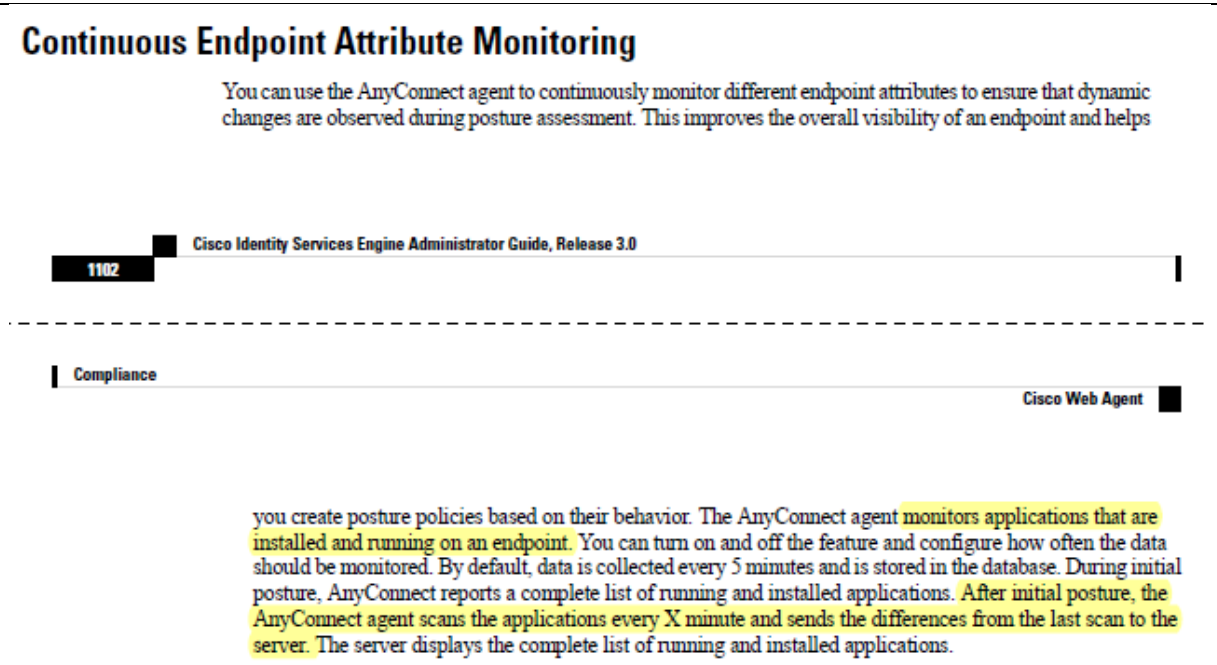


Endpoint posture service	• Performs posture assessments to endpoints connected to the network.
	• Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM.
	• Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media.
	• Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies.
	• Provides hardware inventory for full network visibility.
	• Requires the AnyConnect 4.x agent for posture assessment on these OS platforms:
	  ◦ Windows 10 and later
	  ◦ Mac OS X 10.13 and later
	  ◦ Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu)

ISE Data Sheet at 6.

Finally, with respect to the AnyConnect Agent, Cisco states that it can "report[] a complete list of ***running*** and installed applications" on the device, ISE 3.0 Admin Guide at 1102-03. Thus "the security policy audit is based at least in part on audit data collected by the agent, and that concerns applications executing on the device."

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	 ISE 3.0 Admin Guide at 1102-03.
18. The method of claim 6, wherein updated audit data pertaining to the device continues to be received from the agent after	Cisco's ISE performs "[t]he method of claim 6, wherein updated audit data pertaining to the device continues to be received from the agent after reconfiguring the access point" and induces others to do so. As described above with respect to claim elements 1-d & e, Cisco's ISE "receiv[es] updated audit data pertaining to the device subsequent to reconfiguring the access point; and monitor[s] continued compliance of the device with the security policy using the updated audit data" and induces others to do so.

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

reconfiguring the access point.	Also as described above with respect to claim 2, Cisco's ISE performs "[t]he method of claim 1, wherein monitoring of the device for continued compliance with the security policy includes continued communications with the device" and induces others to do so. Cisco accomplishes this with its AnyConnect Agent, which operates (as is relevant to this claim) "[a]fter the initial posture" *see ISE* 3.0 Admin Guide at 1102-03—that is, after "auditing the device . . . [and] reconfiguring an access point . . ." Cisco explains how the AnyConnect Agent "scans the applications every X minute and ***sends the differences from the last scan to the server***. The server displays the complete list of running and installed applications." ISE 3.0 Admin Guide at 1102-03. These "differences from the last scan" constitute "updated audit data"; they are received by the server from the AnyConnect Agent.
19. The method of claim 6, wherein updated audit data pertaining to the device continues to be received from the agent while the device has access to the less-restricted subset of the network.	Cisco's ISE performs "[t]he method of claim 6, wherein updated audit data pertaining to the device continues to be received from the agent while the device has access to the less-restricted subset of the network" and induces others to do so. As described above with respect to claim elements 1-d & e, Cisco "receiv[es] updated audit data pertaining to the device subsequent to reconfiguring the access point; and monitor[s] continued compliance of the device with the security policy using the updated audit data" and induces others to do so. Also as described above with respect to claim 2, Cisco's ISE performs "[t]he method of claim 1, wherein monitoring of the device for continued compliance with the security policy includes continued communications with the device" and induces others to do so. Cisco accomplishes this with its AnyConnect Agent, which operates (as is relevant to this claim) "[a]fter the initial posture" *see ISE* 3.0 Admin Guide at 1102-03—that is, after "auditing the device . . . [and] reconfiguring an access point . . ." and thus "while the device has access to the less-restricted subset of the network." Cisco explains how the AnyConnect Agent "scans the applications every X minute and ***sends the differences from the last scan to the server***. The server displays the complete list of running and installed

U.S. Patent No. 8,347,350 (Cisco's Identity Services Engine)

	applications." ISE 3.0 Admin Guide at 1102-03. These "differences from the last scan" constitute "updated audit data." Finally, such data is sent periodically (by default, every 5 minutes), thus the "updated audit data pertaining to the device continues to be received from the agent while the device has access to the less-restricted subset of the network."

EXHIBIT F-5

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

U.S. Patent No. 8,578,444	Cisco's Identity Services Engine
[Claim 1 – preamble] A method for auditing a device, the method comprising:	Cisco infringes this claim by making, using, testing, offering for sale, and selling the Identity Services Engine ("ISE") product and system and through performance of each of the claimed steps and/or providing instructions and data from its servers to third-parties to perform at least one of the claimed steps. Further, subsequent to Cisco's making, using, testing, offering for sale, and selling of the ISE, Cisco offers services to third-parties and customers with respect to the ISE. For example, these can include "Technical Services," "Advisory Services," and "Cisco Talos Incidence Response" services. (https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/ise-licensing-guide-og.html). For technical services, for example, Cisco encourages customers to purchase "Cisco Smart Net Total Care" for Cisco ISE physical appliances and Software Support (SWSS) contracts for Cisco ISE virtual machines. For advisory services, Cisco offers Expert Services to address "your business objectives with the technology we offer" (including ISE). *Id*. And for the Talos Incident Response, Cisco provides a full suite of proactive and emergency services to help third-parties prepare, respond, and recover from a cybersecurity breach. Cisco explains that third-parties can "order and transact Cisco Talos Incident Response when ordering Cisco ISE subscriptions." *Id*. Additionally, and as set forth in InfoExpress's 3-1 disclosures, Cisco's ISE also includes Cisco's ISE (NAC) appliance. Specifically, these are Cisco-provided tangible hardware and "virtual appliances" on which ISE can be deployed. A list of accused ISE (NAC) Appliances (also referred to as "hardware platforms") which ISE supports, are disclosed in InfoExpress's Disclosure of Asserted Claims and Infringement Contentions per Patent L.R. 3-1 and 3-2 at Section II.B.2. These ISE (NAC) Appliances are listed in Cisco's Identity Services Engine Administrator Guides, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0001603 to 0014308, and also their

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

	Release Notes for ISE Releases 1.04, 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014606 to 0015185. Cisco's ISE (NAC) appliances are directed to "[g]ranting and denying network access" and using "attributes related to users and their devices" in "determining authorized network access." https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/datasheet-c78-726524.html.[1] Cisco further explains that its NAC appliance (known in one example as "The Cisco Secure Network Server") "supports Cisco's powerful network access and control security applications." *Id*. Further, Cisco explains that the "Cisco Secure Network Server… is configured specifically to support the Cisco Identity Services Engine (ISE) security application." *Id*. To the extent the preamble is limiting, Cisco's ISE[2] "allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network" and thereby "audit[s] a device."

[1] Certain portions of the evidence cited herein identify and relate to the "Cisco Secure Network Server Data Sheet" for Cisco SNS-3715, SNS-3755, and SNS-3795 Secure Network Server. We understand that each other version of the Accused Technology relating to the Cisco ISE (NAC) appliances including ISE-3315-K9, ISE-3355-K9, and ISE-3395-K9; SNS-3415-K9 and SNS-3495-K9; SNS -3515-K9 and SNS-3595-K9; SNS-3615-K9, SNS-3655-K9, and SNS-3695-K9; and ISE Virtual Machine (S/M/L)-K9 are operationally and functionally the same with respect to and for the purposes of identifying infringement for each of the Asserted Claims.

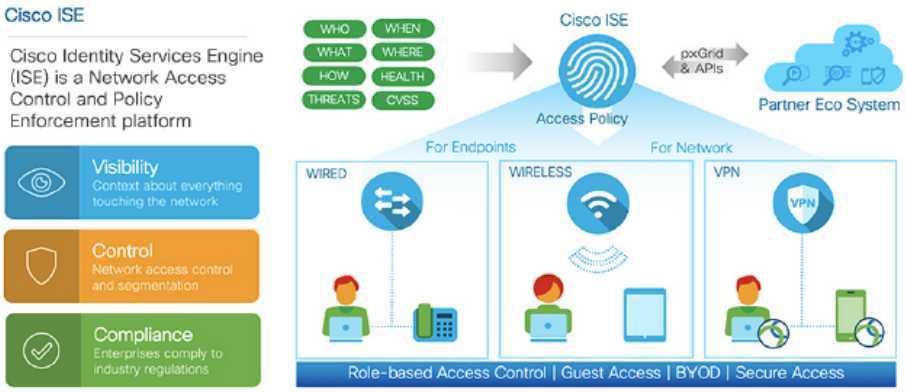
[2] Certain portions of the evidence cited herein identify and relate to the Cisco Identity Services Engine, Release 3.0. We understand that each version of the Accused Technology is operationally and functionally similar with respect to and for infringement of each of the Asserted Claims.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

	• **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation. • **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services. • **Threat Containment**: If Cisco ISE detects threat or vulnerability attributes from an endpoint, adaptive network control policies are sent to dynamically change its access levels of the endpoint. After the threat or vulnerability is evaluated and addressed, the endpoint is given back its original access policy. Cisco Identity Services Engine Administrator Guide, Release 3.0 ("ISE 3.0 Admin Guide"), at 2, available at https://www.cisco.com/c/en/us/ td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf. *See also* ISE 3.0 Admin Guide at 1 ("A Cisco ISE administrator can gather real-time contextual data for a network, including users and user groups (who?), ***device type (what?)***, . . .")

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

Cisco ISE Overview



Cisco Identity Services Engine (ISE) is an identity-based network access control and policy enforcement system. It functions as a common policy engine that enables endpoint access control and network device administration for enterprises.

You can leverage Cisco ISE to ensure compliance, enhance infrastructure security, and streamline service operations.

A Cisco ISE administrator can gather real-time contextual data for a network, including users and user groups (who?), device type (what?), access time (when?), access location (where?), access type (wired, wireless, or VPN) (how?), and network threats and vulnerabilities.

See also ISE 3.0 Admin Guide at 1 ("A Cisco ISE administrator can gather real-time contextual data for a network, including users and user groups (who?), ***device type (what?)***, . . .")

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

[1-a] performing an authentication using an EAP protocol from the device, the device being connected via a computer network to an access point configured to use an 802.1x protocol;	Cisco ISE "perform[s] an authentication using an EAP protocol from the device, the device being connected via a computer network to an access point configured to use an 802.1x protocol" and induces others to do so. Cisco ISE "uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods." ISE 3.0 Admin Guide at 2. • **Bring Your Own Device (BYOD)**: Cisco ISE allows your employees and guests to securely use their personal devices on your enterprise network. BYOD feature end users can use configured pathways to add their devices, and provision predefined authentications and levels of network access. • **Asset Visibility**: Cisco ISE gives you visibility and control over who and what is on your network consistently, across wireless, wired, and VPN connections. Cisco ISE uses probes and device sensors to listen to the way devices connect to the network. The Cisco ISE profile database, which is extensive, then classifies the device. This gives the visibility and context you need to grant the right level of network access. • **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods. • **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation. ISE performs authentication using several different EAP protocols, including Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), and Protected Extensible Authentication

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

Protocol (PEAP). ISE 3.0 Admin Guide at 903. Cisco's ISE therefore contains "an extensible authentication protocol (EAP) server layer (SL) stored in memory."

Policy Set Protocol Settings

You must define global protocol settings in Cisco ISE before you can use these protocols to create, save and implement a policy set. You can use the Protocol Settings page to define global options for the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), and Protected Extensible Authentication Protocol (PEAP) protocols, which communicate with the other devices in your network.

Supported Network Access Policy Set Protocols

The following is a list of protocols that you can choose while defining your Network Access Policy Set policy:

- Password Authentication Protocol (PAP)
- Protected Extensible Authentication Protocol (PEAP)
- Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2)
- Extensible Authentication Protocol-Message Digest 5 (EAP-MD5)
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)
- Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS)
- Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)

ISE 3.0 Admin Guide at 903.

Cisco goes on to describe the guidelines for each of these EAP types. ISE 3.0 Admin Guide at 903-06 (EAP-FAST); 906-07 (EAP-TTLS); 907-08 (EAP-TLS); 908-09 (PEAP); 919-25 (allowed protocols in ISE include EAP-MD5, EAP-TLS, LEAP, PEAP, EAP-FAST, EAP-TTLS, Tunnel Extensible Authentication Protocol (TEAP).

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

	Cisco also describes several RADIUS-based EAP protocols in ISE: **RADIUS-Based EAP Protocols** EAP provides an extensible framework that supports various authentication types. This section describes the EAP methods supported by Cisco ISE and contains the following topics: **Simple EAP Methods** • EAP-Message Digest 5 • Lightweight EAP **EAP Methods That Use Cisco ISE Server Certificate for Authentication** • PEAP/EAP-MS-CHAPv2 • PEAP/EAP-GTC • EAP-FAST/EAP-MS-CHAPv2 • EAP-FAST/EAP-GTC Apart from the methods listed above, there are EAP methods that use certificates for both server and client authentication. ISE 3.0 Admin Guide at 934.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

RADIUS-Based EAP Authentication Flow

Whenever EAP is involved in the authentication process, the process is preceded by an EAP negotiation phase to determine which specific EAP method (and inner method, if applicable) should be used. EAP-based authentication occurs in the following process:

1. A host connects to a network device.
2. The network device sends an EAP Request to the host.
3. The host replies with an EAP Response to the network device.
4. The network device encapsulates the EAP Response that it received from the host into a RADIUS Access-Request (using the EAP-Message RADIUS attribute) and sends the RADIUS Access-Request to Cisco ISE.
5. Cisco ISE extracts the EAP Response from the RADIUS packet and creates a new EAP Request, encapsulates it into a RADIUS Access-Challenge (again, using the EAP-Message RADIUS attribute), and sends it to the network device.
6. The network device extracts the EAP Request and sends it to the host.

In this way, the host and Cisco ISE indirectly exchange EAP messages (transported over RADIUS and passed through the network device). The initial set of EAP messages that are exchanged in this manner negotiate the specific EAP method that will subsequently be used to perform the authentication.

The EAP messages that are subsequently exchanged are then used to carry the data that is needed to perform the actual authentication. If it is required by the specific EAP authentication method that is negotiated, Cisco ISE uses an identity store to validate user credentials.

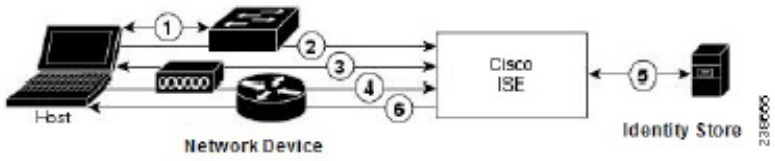
After Cisco ISE determines whether the authentication should pass or fail, it sends either an EAP-Success or EAP-Failure message, encapsulated into a RADIUS Access-Accept or Access-Reject message to the network device (and ultimately also to the host).

ISE 3.0 Admin Guide at 934.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

The following figure shows a RADIUS-based authentication with EAP.

Figure 47: RADIUS-Based Authentication with EAP



ISE 3.0 Admin Guide at 935; *see also id.* at 935-37 (EAP-MD5, LEAP, PEAP advantages and protocol flow, EAP-FAST benefits and protocol flow); 940-41 (EAP-FAST is used within Cisco's TrustSec architecture).

Furthermore, in Cisco ISE, the "device [is] connected via a computer network to an access point configured to use an 802.1x protocol."

Cisco describes how in its Component Compatibility documents for ISE, the authentication, authorization, and accounting (AAA) feature supports the 802.1X authentication functionality in access points, including access switches, routers, wireless LAN controllers, and remote access devices (i.e. Adaptive Security Appliance (ASA) series firewalls). INFOEX-CSCO_0014309 to INFOEX-CSCO_0014605. These devices include Cisco-made and third-party products. Cisco also describes ISE-compatible third-party devices in its ISE 3.0 Admin Guide at 806-07, including those made by Aruba, Motorola, HP, Ruckus, Alcatel, Brocade, and Juniper. Cisco describes these third-party products as "Supported or Validated Use Cases" for 802.1X authentication.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

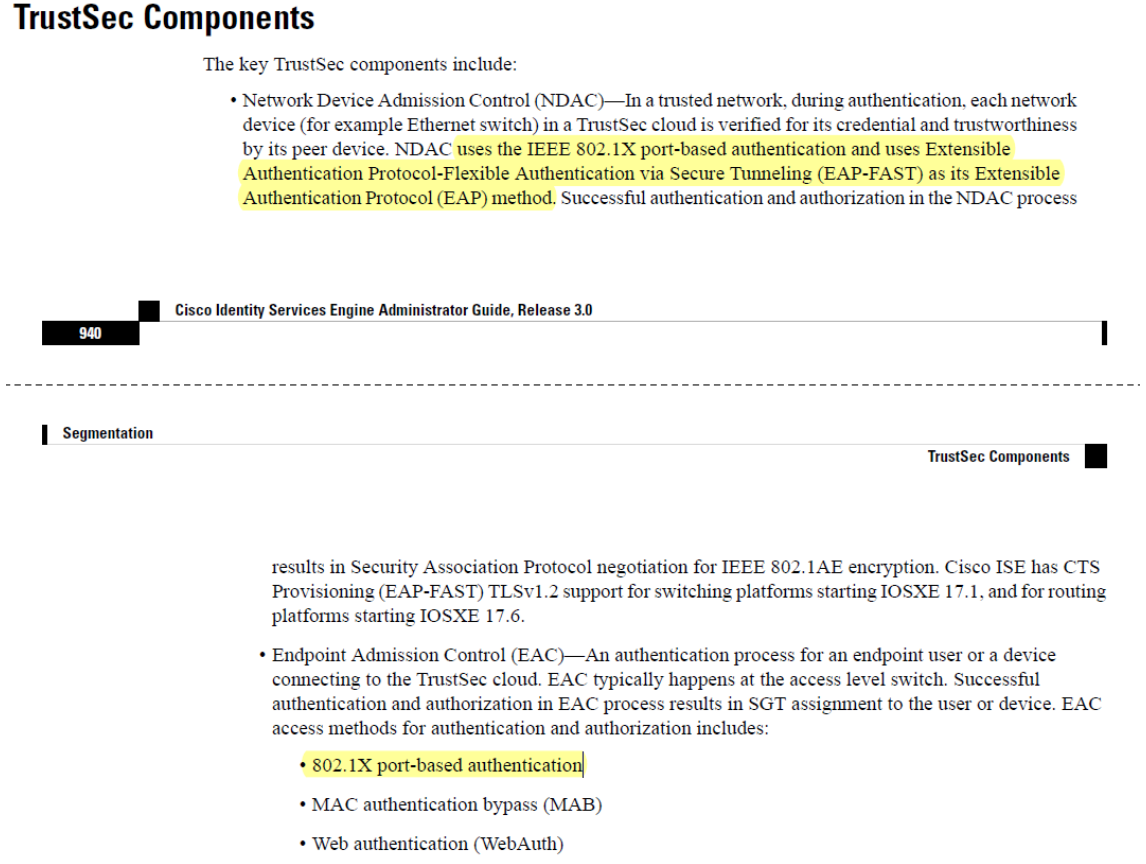
	Furthermore, Cisco provides several examples of "performing an authentication using an EAP protocol from the device, the device being connected via a computer network to an access point configured to use an 802.1x protocol":
	
	• For Apple endpoint devices running iOS (e.g., iMac laptops, iPhones) and accessing the network through a Bring Your Own Device (BYOD) program, "The Cisco ISE policy server sends a new profile using Apple's iOS over the air to the IOS device, which includes: . . . A Wi-Fi supplicant profile that enforces the use of ***EAP-[Transport Layer Security (TLS)) for 802.1X authentication***." ISE Admin guide at 766.
	
	Note Starting with version MacOS 10.15, the user must allow download of the Supplicant Provisioning Wizard (SPW). A window displays on the user's device asking them to allow or deny downloads from the Cisco ISE server.
	
	• iOS devices: The Cisco ISE policy server sends a new profile using Apple's iOS over the air to the IOS device, which includes:
	  • The issued certificate (if configured) is embedded with the IOS device's MAC address and employee's username.
	  • A Wi-Fi supplicant profile that enforces the use of EAP-TLS for 802.1X authentication. An additional profile can be installed on the endpoint device to protect Over-The-Air (OTA) communication.
	
	• Cisco ISE supports several different Protected Extensible Authentication Protocol (PEAP) methods, and "PEAP is compatible with the IEEE 802.1X standard and RADIUS protocol[.]" *Id.* at 935.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

	Protected Extensible Authentication Protocol Protected Extensible Authentication Protocol (PEAP) provides mutual authentication, ensures confidentiality and integrity to vulnerable user credentials, protects itself against passive (eavesdropping) and active (man-in-the-middle) attacks, and securely generates cryptographic keying material. PEAP is compatible with the IEEE 802.1X standard and RADIUS protocol. Cisco ISE supports PEAP version 0 (PEAPv0) and PEAP version 1 (PEAPv1) with Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol (EAP-MS-CHAP), Extensible Authentication Protocol-Generic Token Card (EAP-GTC), and EAP-TLS inner methods. The Cisco Secure Services Client (SSC) supplicant supports all of the PEAPv1 inner methods that Cisco ISE supports. • Cisco's TrustSec Architecture "uses the IEEE 802.1X port-based authentication and uses Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) as

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

its Extensible Authentication Protocol (EAP) method." *Id.* at 940-41.



TrustSec Components

The key TrustSec components include:

- Network Device Admission Control (NDAC)—In a trusted network, during authentication, each network device (for example Ethernet switch) in a TrustSec cloud is verified for its credential and trustworthiness by its peer device. NDAC uses the IEEE 802.1X port-based authentication and uses Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) as its Extensible Authentication Protocol (EAP) method. Successful authentication and authorization in the NDAC process

Cisco Identity Services Engine Administrator Guide, Release 3.0

940

Segmentation

TrustSec Components

results in Security Association Protocol negotiation for IEEE 802.1AE encryption. Cisco ISE has CTS Provisioning (EAP-FAST) TLSv1.2 support for switching platforms starting IOSXE 17.1, and for routing platforms starting IOSXE 17.6.

- Endpoint Admission Control (EAC)—An authentication process for an endpoint user or a device connecting to the TrustSec cloud. EAC typically happens at the access level switch. Successful authentication and authorization in EAC process results in SGT assignment to the user or device. EAC access methods for authentication and authorization includes:
  - 802.1X port-based authentication
  - MAC authentication bypass (MAB)
  - Web authentication (WebAuth)

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

- For the Google Admin Console, one can use 802.1X security in combination with an EAP-TLS or PEAP authentication protocol. *Id.* at 1094.

Google Admin Console - Wi-Fi Network Settings

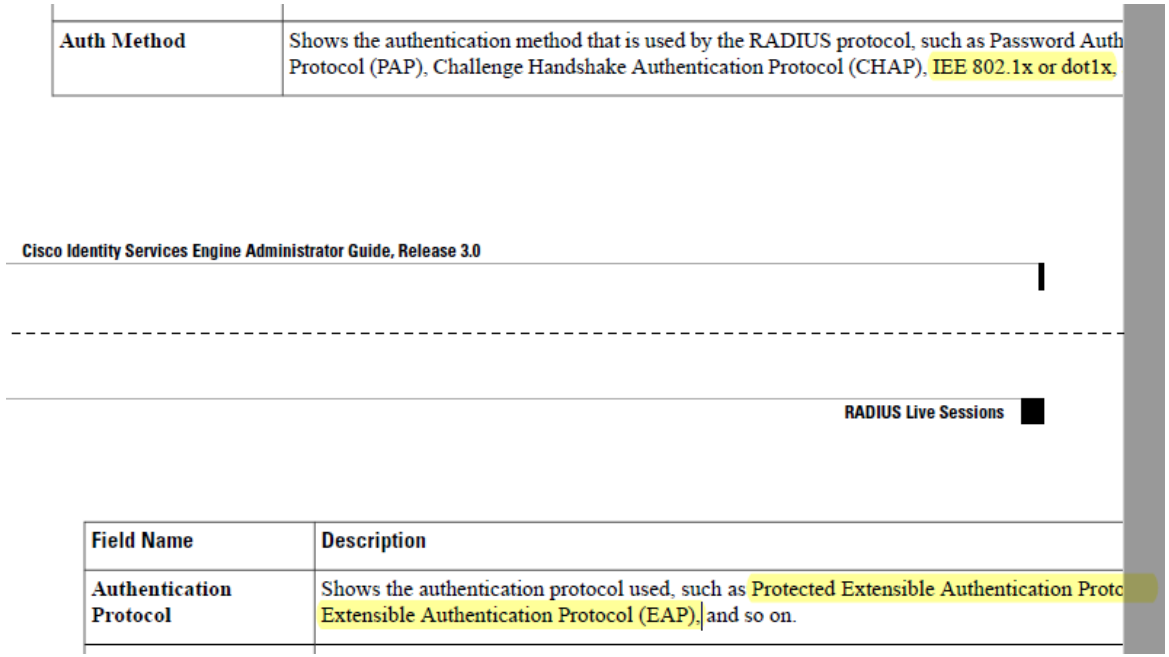
The Wi-Fi network configuration is used to configure an SSID in a customer network or to match the certificate using certificate attributes (for EAP-TLS). When the certificate is installed in the Chromebook, it is synchronized with the Google admin settings. Connection is established only when one of the defined certificate attributes matches the SSID configuration.

Listed below are the mandatory fields, specific to EAP-TLS, PEAP, and Open network flows, which the Google administrator configures to set up the Wi-Fi network in the Google Admin Console page (**Device Management** > **Network** > **Wi-Fi** > **Add Wi-Fi**) for each Chromebook user.

Field	EAP-TLS	PEAP	Open
Name	Enter the name of the network connection.	Enter the name of the network connection.	Enter the name of the network connection.
Service Set Identifier (SSID)	Enter the SSID (for example, tls_ssid).	Enter the SSID (for example, tls_ssid).	Enter the SSID (for example, tls_ssid).
This SSID Is Not Broadcast	Select the option.	Select the option.	Select the option.
Automatically Connect	Select the option.	Select the option.	Select the option.
Security Type	WPA/WPA2 Enterprise (802.1x)	WPA/WPA2 Enterprise (802.1x)	Open
Extensible Authentication Protocol	EAP-TLS	PEAP	—
Inner Protocol	—	• Automatic • MSCHAP v2 (Select the option) • MD5 • PAP • MSCHAP • GTC	—

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

- For RADIUS-based authentication, one can use 802.1X security and an EAP protocol. *Id.* at 1234-35.



Auth Method	Shows the authentication method that is used by the RADIUS protocol, such as Password Auth Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), IEE 802.1x or dot1x,

Cisco Identity Services Engine Administrator Guide, Release 3.0

RADIUS Live Sessions

Field Name	Description
Authentication Protocol	Shows the authentication protocol used, such as Protected Extensible Authentication Protc Extensible Authentication Protocol (EAP), and so on.

See also id. at 884 ("To define conditions that are based on an endpoint identity group that has been previously authenticated, Cisco ISE supports authorization that was defined during endpoint identity group 802.1X authentication status."); 1186 ("Enable 802.1X Port-Based Authentication for Switch Ports"), 1188 ("Enable Switch Ports for 802.1X and MAB"), 1190 ("Command to Enable 802.1X based on Identity-Based Networking Services").

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

[1-b] sending a request for audit data to an agent running on the device; [and] **[1-c]** receiving the audit data at a gatekeeper configured to control access to a network, from the agent, the audit data pertaining to the device and having been obtained by the agent;	Cisco ISE "send[s] a request for audit data to an agent running on the device[and] receiv[es] the audit data at a gatekeeper configured to control access to a network, from the agent, the audit data pertaining to the device and having been obtained by the agent[,]" and induces others to do so. Cisco ISE "allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the ***appropriate posture agents*** for posturing services." ISE Admin Guide at 2. In one example, Cisco's ISE describes agents running on the device. • **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods. • **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation. • **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services. ISE Admin Guide at 2. Cisco further describes several different "posture agents[.]" which exchange information with the ISE in response to a request. These include:

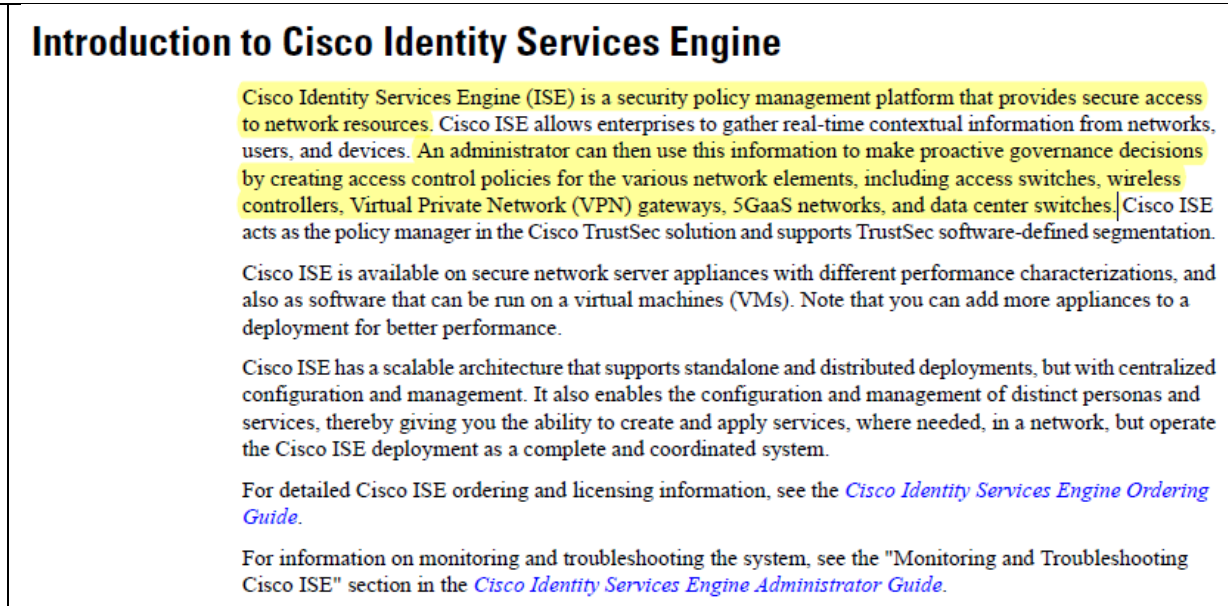
U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

	• The ***AnyConnect Agent***, which can "report[] a complete list of running and installed applications" on the access device, (ISE 3.0 Admin Guide at 1102-03; *see also id.* at 1057-58); • The ***AnyConnect Stealth Agent***, which reports certain information back to ISE, (*id.* at 1010-11); • The ***Cisco Temporal Agent***, which is a "temporary executable file that is run on the client to check the compliance status" and which "is removed from the client machine after the login session is terminated," (*id.* at 1057), and • The ***Cisco Web Agent***, which "provides temporal posture assessment for client machines" and which "gets the requirements that are configured for the user role and the operating system from the Cisco ISE server, checks the host registry, processes, applications, and services for required packages and sends a report back to the Cisco ISE server," *id.* at 1103. Thus, Cisco ISE "send[s] a request for audit data to an agent running on the device[.]" Cisco next describes several types of "audit data" that ISE can "request [from] and agent running on the device." These include: • "Hardware attributes of an endpoint." ISE 3.0 Admin Guide at 174; *see also id.* at 174-5 (listing attributes), 176 ("Cisco ISE profiles the hardware attributes of a client's system, however, there may be a few hardware attributes Cisco ISE does not profile. . . . The hardware inventory data collection interval can be controlled . . . The default interval is 5 minutes."). • "Endpoint attribute data" which is received "from multiple sources, such as Cisco Catalyst 9000 Series devices, CMBD connections, telemetry devices, and more" and which further includes "Profiling attributes: the Multi-Factor Classification attributes--Hardware Manufacturer, Hardware Model, Operating System, and Endpoint Type[;] Trust Score attributes: Attributes related to Random MAC addresses, profiling changes, spoofing detection, and other behaviors that are monitored by Cisco AI Endpoint Analytics to calculate comprehensive Trust Scores for endpoints.[';] . . . Endpoint Trust Score [and] [Configuration Management Database ("CMDB")]

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

	attributes" (*Id.* at 874-75; *see also* Cisco, Randomized and Changing MAC Deployment Guide (2022) ("Randomized and Changing MAC") at 44, https://www.cisco.com/c/en/us/products/collateral/wireless/randomized-changing-mac-dg.pdf (last visited June 27, 2023) (listing six examples of device attributes); • "Simple posture conditions," including file conditions, registry conditions, application conditions, service conditions, and USB conditions on the client (the claimed "access device"). *Id.* at 1027. Cisco ISE "receiv[es] the audit data at a gatekeeper configured to control access to a network, from the agent[.]" As noted above with respect to the AnyConnect Agent, AnyConnect Stealth Agent, and the Web Agent, they all "report" audit data or "send a report" to the ISE server. And since they "report" or "send a report," Cisco ISE thereby "receives" this audit data. Moreover, Cisco ISE comprises a "gatekeeper configured to control access to a network[.]" Cisco describes ISE as "a security policy management platform that provides secure access to network resources[.]" ISE gathers certain information from the network, which an administrator can use "to make proactive governance decisions by creating ***access control policies*** for the various network elements, including access switches, wireless controllers, Virtual Private Network (VPN) gateways, 5GaaS networks, and data center switches." Furthermore, "ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation[.]" Therefore, ISE comprises a "gatekeeper configured to control access to a network."

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)



Introduction to Cisco Identity Services Engine

Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, wireless controllers, Virtual Private Network (VPN) gateways, 5GaaS networks, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation.

Cisco ISE is available on secure network server appliances with different performance characterizations, and also as software that can be run on a virtual machines (VMs). Note that you can add more appliances to a deployment for better performance.

Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also enables the configuration and management of distinct personas and services, thereby giving you the ability to create and apply services, where needed, in a network, but operate the Cisco ISE deployment as a complete and coordinated system.

For detailed Cisco ISE ordering and licensing information, see the *Cisco Identity Services Engine Ordering Guide*.

For information on monitoring and troubleshooting the system, see the "Monitoring and Troubleshooting Cisco ISE" section in the *Cisco Identity Services Engine Administrator Guide*.

Release Notes for Cisco Identity Services Engine, Release 3.0 ("ISE 3.0 Release Notes") at 1, *available at* https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/release_notes/b_ise_30_rn.html (last accessed June 26, 2023); *see also* ISE 3.0 Admin Guide at 1 (further describing ISE as "an identity-based network access control and policy enforcement system [that] functions as a common policy engine that enables endpoint access control and network device administration[.]").

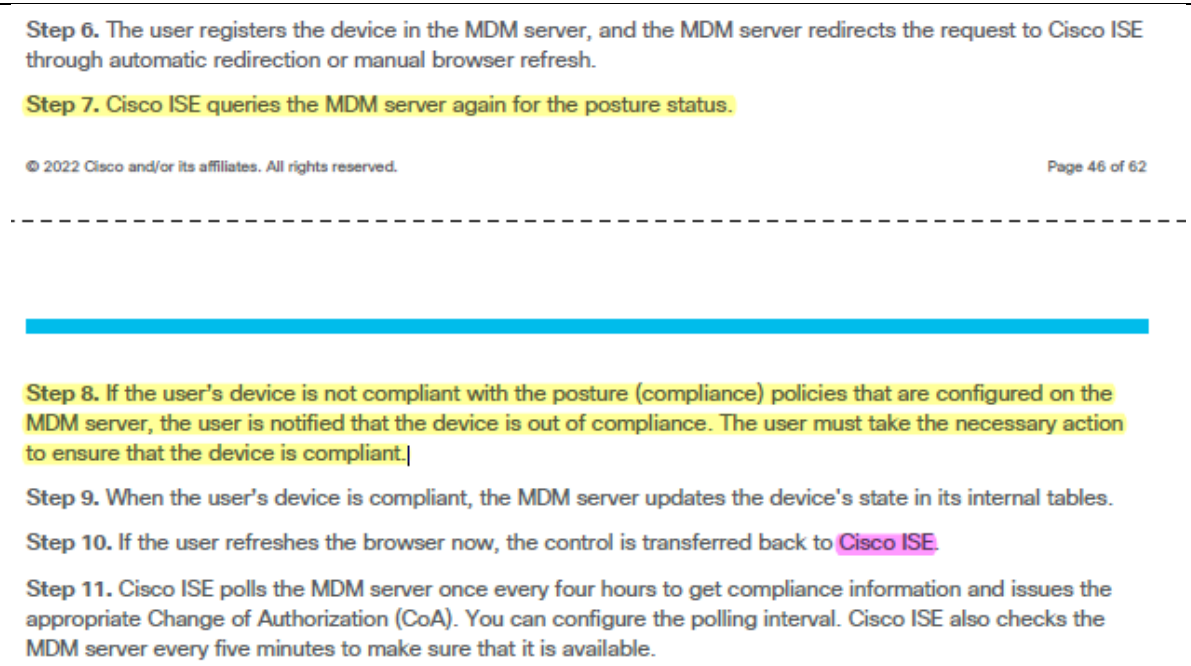
U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

[1-d] applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication, the applying of the security policy taking place under control of the gatekeeper.	Cisco's ISE "appl[ies] a security policy that includes at least one requirement[] pertaining to the audit data and at least one requirement pertaining to the authentication, the applying of the security policy taking place under control of the gatekeeper" and induces others to do so." Cisco explains that "Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods." Separate and apart from authentication, Cisco describes how "Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the ***appropriate posture agents*** for posturing services." Thus, Cisco "appl[ies] a security policy" that includes at least one requirement pertaining to the audit data (discussed above with respect to claim elements 1-b & c) and at least one requirement pertaining to the authentication (discussed above with respect to claim element 1-a). • **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods. • **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation. • **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services. ISE 3.0 Admin Guide at 2.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

	With respect to an MDM server integrated with ISE, "ISE is the enforcement point[, which] obtains data from the MDM server [and] then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points." Randomized and Changing MAC Deployment Guide at 43. That same guide separately discusses authentication (via device-unique ID (DUID) and/or global-unique ID (GUID)) and posture compliance assessment. **Handle random and changing MAC addresses with an MDM server** To avoid issues caused by the use of the MAC address randomization method, configure Cisco ISE to identify endpoints that are connected to an MDM server by a unique device identifier instead of a MAC address. Mobile devices increasingly use random and changing MAC addresses for each SSID. This means that an endpoint presents different MAC addresses to the MDM server and to Cisco ISE. As a result, when the MDM server and Cisco ISE are integrated and an action is initiated for an endpoint, issues arise because the endpoint's identity is different in the two systems. In Cisco ISE, you can now work around this problem by configuring Cisco ISE to use a unique device identifier instead of MAC addresses. When an endpoint enrolls with an MDM server, the MDM server sends a certificate with a GUID value to the endpoint. The endpoint uses this certificate for authentication with Cisco ISE. Cisco ISE receives the GUID for the endpoint from the certificate. All communications between Cisco ISE and the MDM server now use the GUID to identify the endpoint, helping ensure accuracy and consistency between the two systems. Note that GUIDs are available only in certificate-based authentication methods. Basic authentication methods that use only a username and password will not be able to leverage the GUID-based solution. The Cisco ISE MDM APIs have been updated (Cisco ISE MDM APIs Version 3) to facilitate the gathering and management of GUID data. Currently, MobileIron supports Cisco ISE MDM APIs Version 3, and sends GUID information to Cisco ISE. Randomized and Changing MAC Deployment Guide at 48.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)



Step 6. The user registers the device in the MDM server, and the MDM server redirects the request to Cisco ISE through automatic redirection or manual browser refresh.

Step 7. Cisco ISE queries the MDM server again for the posture status.

© 2022 Cisco and/or its affiliates. All rights reserved.

Step 8. If the user's device is not compliant with the posture (compliance) policies that are configured on the MDM server, the user is notified that the device is out of compliance. The user must take the necessary action to ensure that the device is compliant.

Step 9. When the user's device is compliant, the MDM server updates the device's state in its internal tables.

Step 10. If the user refreshes the browser now, the control is transferred back to Cisco ISE.

Step 11. Cisco ISE polls the MDM server once every four hours to get compliance information and issues the appropriate Change of Authorization (CoA). You can configure the polling interval. Cisco ISE also checks the MDM server every five minutes to make sure that it is available.

Randomized and Changing MAC Deployment Guide at 46-47.

Thus, Cisco "appl[ies] a security policy" that includes at least one requirement pertaining to the audit data (discussed above with respect to claim elements 1-b & c) and at least one requirement pertaining to the authentication (discussed above with respect to claim element 1-a).

In an example, Cisco explains how ISE "appl[ies] a security policy, the security policy including one or more requirements pertaining to the authentication and the information" when it operates with respect

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

	to both Cisco and third-party (i.e. non-Cisco) network access devices (NAD) (the claimed "access points"). A guest endpoint (the claimed "device") connects to the network through a third-party ***network access device*** or ***NAD***. ISE applies a security policy: As described in step 3, "Cisco ISE runs the configured authentication and authorization policy"—which is "pertaining to the authentication." Furthermore in step 11, Cisco ISE "validates endpoint compliance" and/or "authorizes the endpoint—which are "pertaining to the audit data." Thus, Cisco "appl[ies] a security policy" that includes at least one requirement pertaining to the audit data (discussed above with respect to claim elements 1-b & c) and at least one requirement pertaining to the authentication (discussed above with respect to claim element 1-a).

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

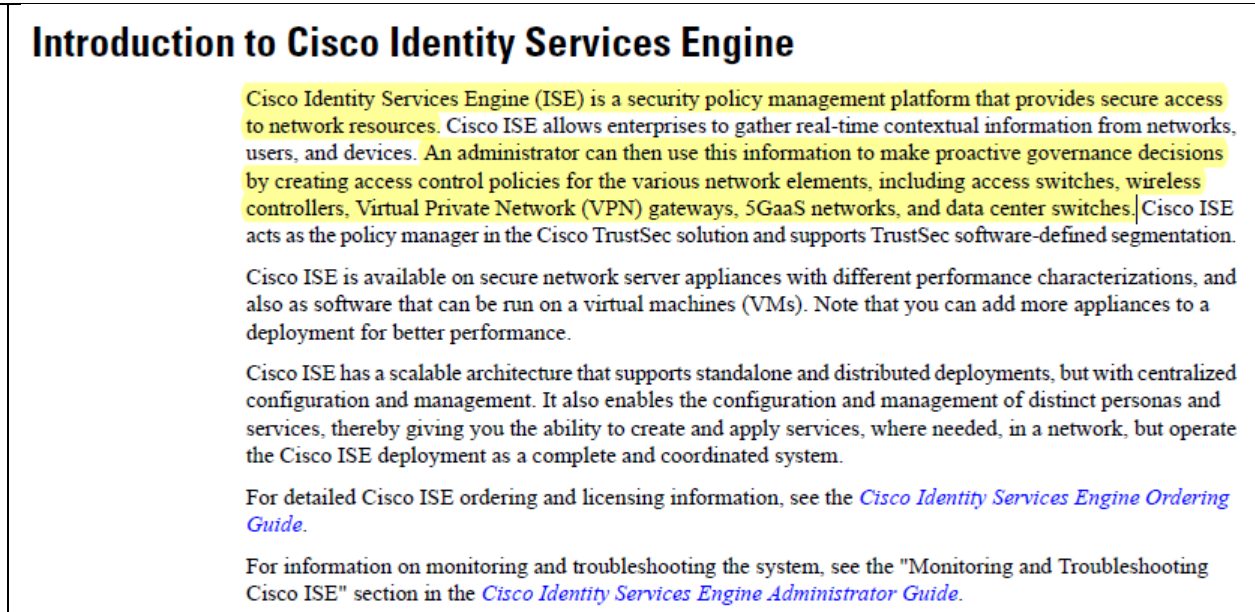
You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

ISE 3.0 Admin Guide at 804; *see also id.* at 805-06 (schematics of same).

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

	Finally, "the applying of the security policy tak[es] place under control of the gatekeeper [.]" Cisco describes ISE as "a security policy management platform that provides secure access to network resources[.]" ISE 3.0 Release Notes at 1. ISE gathers certain information from the network, which an administrator can use "to make proactive governance decisions by creating ***access control policies*** for the various network elements, including access switches, wireless controllers, Virtual Private Network (VPN) gateways, 5GaaS networks, and data center switches." *Id.* Furthermore, "ISE acts as the ***policy manager*** in the Cisco TrustSec solution and supports TrustSec software-defined segmentation[.]" *Id.* Therefore, because ISE contains a gatekeeper, which "creates" and "manages" security policies, "the applying of the security policy tak[es] place under control of the gatekeeper[.]"

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)



Introduction to Cisco Identity Services Engine

Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, wireless controllers, Virtual Private Network (VPN) gateways, 5GaaS networks, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation.

Cisco ISE is available on secure network server appliances with different performance characterizations, and also as software that can be run on a virtual machines (VMs). Note that you can add more appliances to a deployment for better performance.

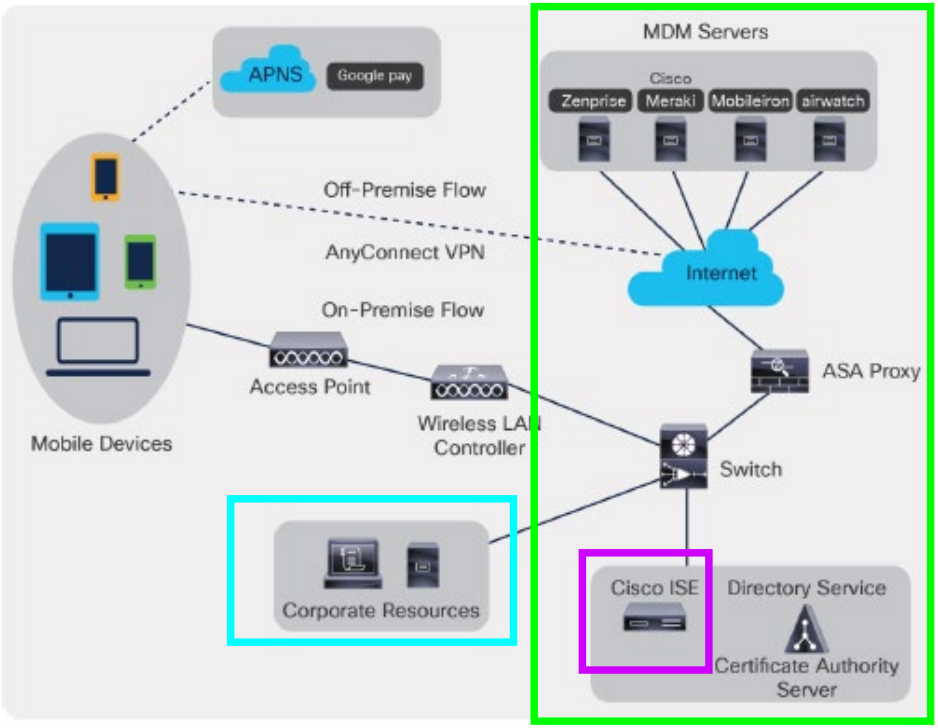
Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also enables the configuration and management of distinct personas and services, thereby giving you the ability to create and apply services, where needed, in a network, but operate the Cisco ISE deployment as a complete and coordinated system.

For detailed Cisco ISE ordering and licensing information, see the *Cisco Identity Services Engine Ordering Guide*.

For information on monitoring and troubleshooting the system, see the "Monitoring and Troubleshooting Cisco ISE" section in the *Cisco Identity Services Engine Administrator Guide*.

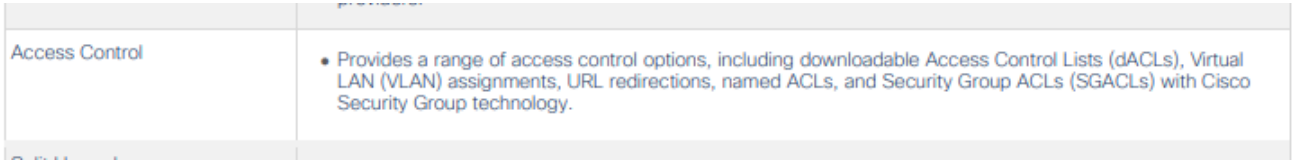
ISE 3.0 Release Notes at 1, *see also* ISE 3.0 Admin Guide at 1, (further describing ISE as "an identity-based network access control and ***policy enforcement system*** [that] functions as a common policy engine that enables endpoint access control and network device administration[.]")

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

2. The method of claim 1, wherein applying the security policy includes configuring the access point.	Cisco ISE performs "[t]he method of claim 1, wherein applying the security policy includes configuring the access point" and induces others to do so.  As shown, once ISE applies a security policy, it configures the access point (here, the switch) to allow the device access to the network (here, "Corporate Resources)." Randomized Changing MAC at 43; *see also id.* at 57 ("If the device is registered with Cisco ISE, is registered with MDM, and is compliant with Cisco ISE and MDM policies, it is ***granted access to the network based on the access control policies configured in Cisco ISE***.").

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

Cisco also describes in its Data Sheet "a range of access control options" for this step, "including downloadable Access Control Lists (dACLs), Virtual LAN (VLAN) assignments, URL redirections, named ACLs, and Security Group ACLs (SGACLs) with Cisco Security Group technology[.]" By using any or all of these methods, ISE "configur[es] the access point[,]"



Access Control	• Provides a range of access control options, including downloadable Access Control Lists (dACLs), Virtual LAN (VLAN) assignments, URL redirections, named ACLs, and Security Group ACLs (SGACLs) with Cisco Security Group technology.

Cisco Identity Services Engine Data Sheet (2023) ("ISE Data Sheet") at 5, available at https://www.cisco.com/c/en/us/products/security/identity-services-engine/ise-ds.pdf (last visited September 22, 2023).

With respect to the example above—involving both Cisco and third-party (i.e. non-Cisco) access points—once ISE determines that "requirements of the security policy are satisfied," it "sends the [change of authorization ("CoA")], authorizes the endpoint, and bypasses the sink hole[,] and then the "the guest user receives the appropriate [network] access based on the CoA." ISE 3.0 Admin Guide at 804. Thus, by sending CoA commands, and by granting the "guest user [] the appropriate [network] access based on th[at] CoA[,]" Cisco ISE "configur[es] the access point[.]"

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

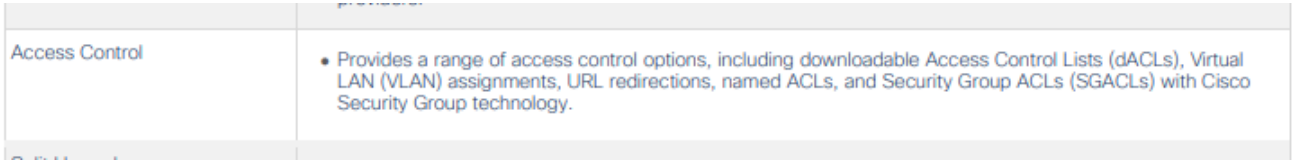
1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

Multiple VLANs may be connected to one network interface card by configuring a VLAN IP helper from the NAD configuration. For more information about configuring an IP helper, see the administration guide for the network device for instructions. For guest access flows that include VLANs with IP helpers, define a guest portal, and select that portal in an authorization profile that is bound to MAB authorization. For more information about guest portals, see the Cisco ISE Guest Services section in *Cisco ISE Admin Guide: Guest and BYOD* .

The following diagram displays a basic network setup when an Auth VLAN is defined (the Auth VLAN is connected directly to a Cisco ISE node).

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

3. The method of claim 2, wherein configuring the access point includes assigning an access control list.	Cisco ISE performs "[t]he method of claim 2, wherein configuring the access point includes assigning an access control list" and induces others to do so. Cisco also describes in its Data Sheet "a range of access control options" for this step, "including downloadable ***Access Control Lists (dACLs)***, Virtual LAN (VLAN) assignments, URL redirections, named ACLs, and Security Group ACLs (SGACLs) with Cisco Security Group technology[.]" By using any or all of these methods, ISE "configur[es] the access point[,]"  ISE Data Sheet at 5. *See also* ISE 3.0 Admin Guide at 867-68:

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

Downloadable ACLs

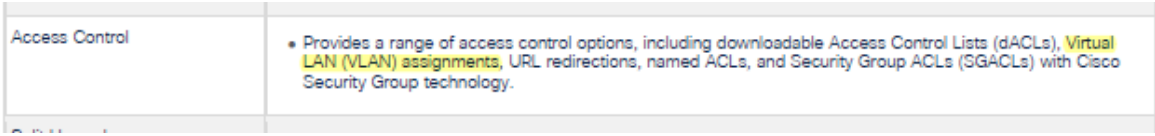
Access control lists (ACLs) are lists of access control entries (ACEs), which may be applied by a Policy Enforcement Point (for example, a switch) to a resource. Each ACE identifies the permissions allowed per user for that object, such as read, write, execute and more. For example, an ACL may be configured for use the Sales area of the network, with an ACE allowing Write permissions for the Sales group and a separate ACE allowing Read permissions for all other employees of the organization. With RADIUS protocol, ACLs grant authorization by filtering source and destination IP addresses, transport protocols, and additional parameters. Static ACLs reside on and are directly configured from the switch and can be applied in your authorization policies from the ISE GUI; downloadable ACLs (DACLs) can be configured, managed and applied in your authorization policies from the ISE GUI.

To implement DACLs in your network authorization policy in ISE:

1. Configure a new or existing DACL from **Policy** > **Policy Elements** > **Results** > **Downloadable ACLs**. For more information see Configure Permissions for Downloadable ACLs, on page 868.
2. Configure a new or existing authorization profile from **Policy** > **Policy Elements** > **Results** > **Authorization Profiles**, using any of the DACLs you already configured.
3. Implement the authorization profiles you have configured when creating and configuring new and existing policy sets from **Policy** > **Policy Sets**.

See also ISE 3.0 Admin Guide at 867-68.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

4. The method of claim 2, wherein configuring the access point includes assigning a VLAN.	Cisco ISE performs "[t]he method of claim 2, wherein configuring the access point includes assigning a VLAN" and induces others to do so. Cisco discloses that generally, ISE "provides a range of access control options, including . . . Virtual LAN (VLAN) assignments. ISE Data Sheet at 5.  By way of an example, Cisco discloses that its can perform dynamic VLAN assignment with a RADIUS server. Cisco, Configure Dynamic VLAN Assignment with ISE and Catalyst 9800 Wireless LAN Controller at 3, 25 (June 2022), https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/217043-configure-dynamic-vlan-assignment-with-c.pdf (last visited May 22, 2023).

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

Introduction

This document describes the concept of dynamic VLAN assignment and how to configure the Catalyst 9800 wireless LAN controller (WLC) and Cisco Identity Service Engine (ISE) to assign wireless LAN (WLAN) in order to accomplish this for the wireless clients.

Requirements

Cisco recommends that you have knowledge of these topics:

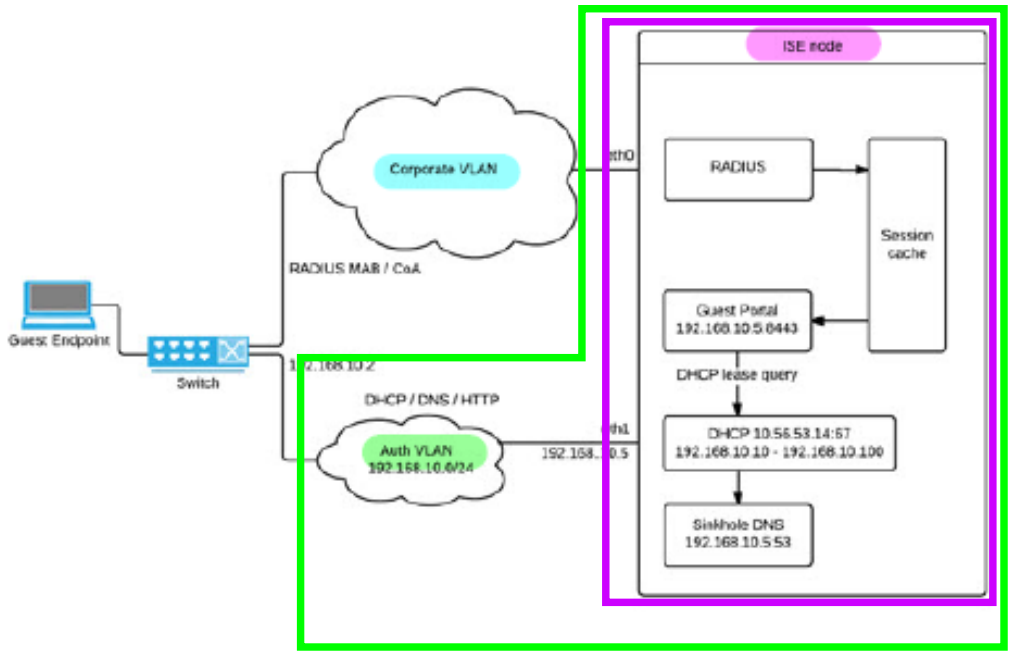
- Have basic knowledge of the WLC and Lightweight Access Points (LAPs).
- Have functional knowledge of the AAA server such as ISE.
- Have a thorough knowledge of wireless networks and wireless security issues.

Configure Dynamic VLAN Assignment with ISE at 1.

With respect to another example discussed above—both Cisco and third-party (i.e. non-Cisco) access points—it was established that Cisco ISE "applies a security policy," per claim element 1-d (citing ISE 3.0 Admin Guide at 803-06), and further that it "configures the access point," per claim 2. As can be shown in the schematics, once ISE "configures the access point," the device has access to the "Corporate VLAN" (in blue). Thus, "configuring the access point includes assigning a VLAN."

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

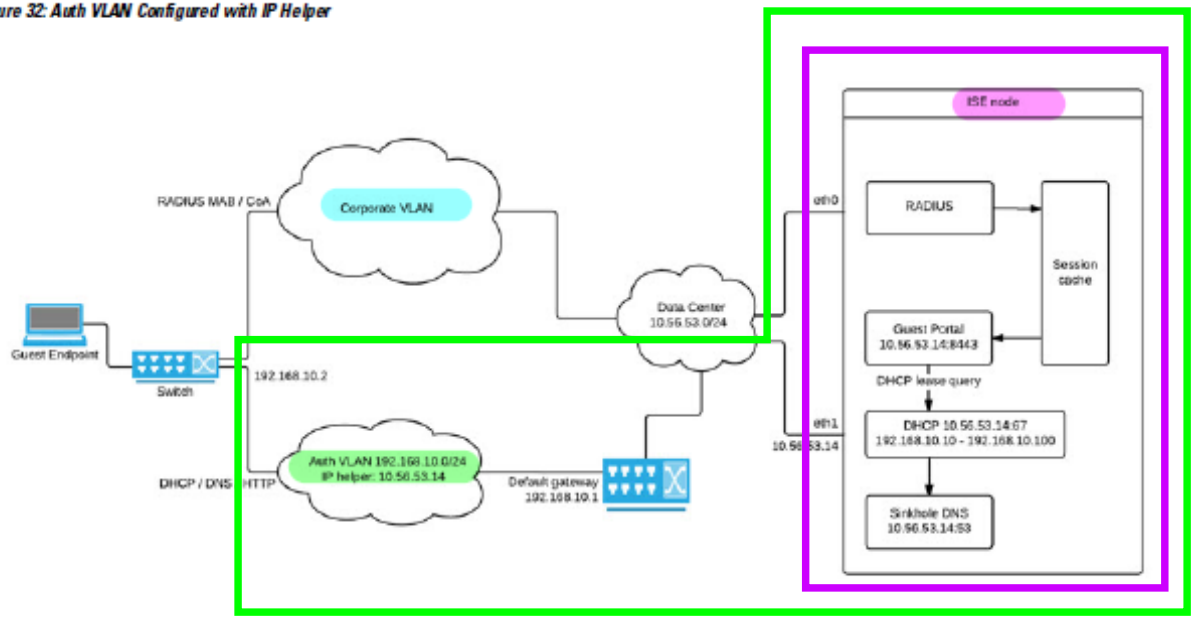
Figure 31: Auth VLAN Connected to Cisco ISE Node



The following diagram displays a network with Auth VLAN and an IP helper.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

Figure 32: Auth VLAN Configured with IP Helper



ISE 3.0 Admin Guide at 804-06.

By way of another example—Adaptive Network Control—Cisco describes how ISE can "quarantine" a user "essentially" by "mov[ing] an endpoint ***from its default VLAN*** to a ***specified Quarantine VLAN***." ISE 3.0 Admin Guide at 300. Similarly, ISE can "unquarantined" a user by "returning the endpoint to its original VLAN" and thus "permit[ting] full access to the network for an endpoint." By changing

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

VLANs (from quarantine back to original), Cisco "configure[es] the access point [b] assigning a VLAN."

Adaptive Network Control

Adaptive Network Control (ANC) is a service that runs on the Administration node. This service monitors and controls network access of endpoints. ANC is invoked by the ISE administrator on the admin GUI, and also can be invoked through pxGrid from third-party systems. ANC supports wired and wireless deployments and requires an Advantage License.

You can use ANC to change the authorization state without having to modify the overall authorization policy of the system. ANC allows you to set the authorization state when you quarantine an endpoint. As a result, the established authorization policies where authorization policies are defined to check for ANCPolicy to limit or deny network access. You can unquarantine an endpoint for full network access. You can also shut down the port on the network attached system (NAS) that disconnects the endpoint from the network.

There are no limits to the number of users that can be quarantined at one time. Also, there are no time constraints on the quarantine period length.

You can perform the following operations to monitor and control network access through ANC:

- Quarantine: Allows you to use Exception policies (authorization policies) to limit or deny an endpoint access to the network. You must create Exception policies to assign different authorization profiles (permissions) depending on the ANCPolicy. Setting to the Quarantine state essentially moves an endpoint from its default VLAN to a specified Quarantine VLAN. You must define the Quarantine VLAN previously that is supported on the same NAS as the endpoint.
- Unquarantine: Allows you to reverse the quarantine status that permits full access to the network for an endpoint. This happens by returning the endpoint to its original VLAN.
- Shutdown: Allows you to deactivate a port on the NAS and disconnect the endpoint from the network. Once the port is shut down on the NAS to which an endpoint is connected, manually reset the port on the NAS again. This allows an endpoint to connect to the network, which is not available for wireless deployments.

ISE 3.0 Admin Guide at 300.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

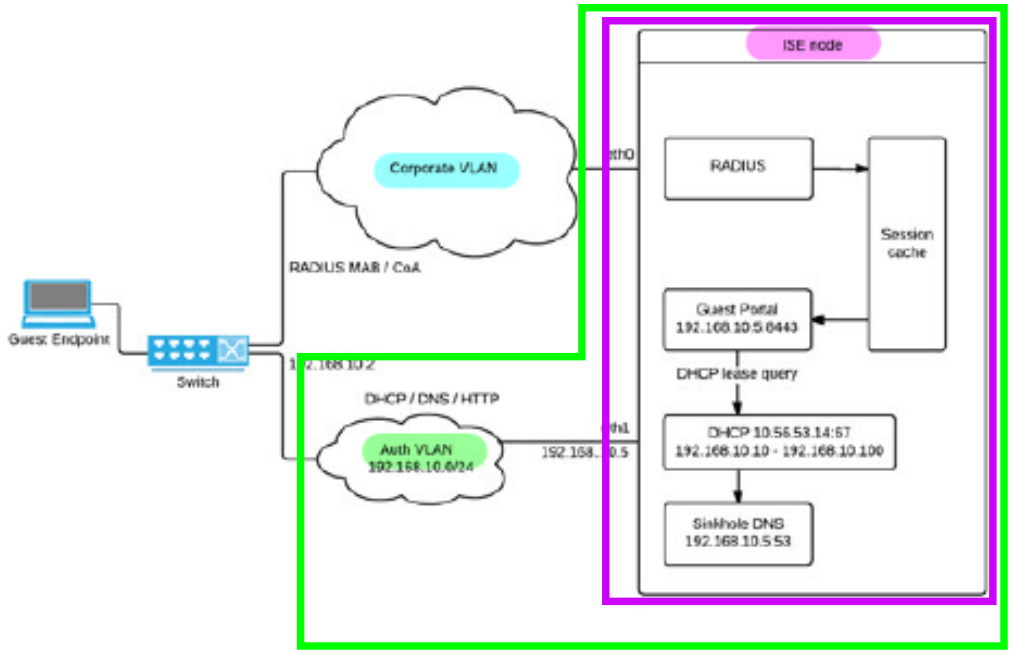
5. The method of claim 2, further comprising receiving, from the agent, updated audit data pertaining to the device after configuring the access point.	Cisco ISE performs "[t]he method of claim 2, further comprising receiving, from the agent, updated audit data pertaining to the device after configuring the access point" and induces others to do so. As discussed above with respect to claim elements 1-b & c, Cisco ISE has several agents running on the (endpoint) devices to which it can "send[] a request for audit data[.]" These include the AnyConnect agent, the AnyConnect Stealth Agent, the Cisco Temporal Agent, and the Cisco Web Agent. Cisco describes ***Continuous Endpoint Attribute Monitoring Mode.*** In this mode, the AnyConnect Agent operates (as is relevant to this claim) "[a]fter the initial posture" *see ISE* 3.0 Admin Guide at 1102-03—that is, after "applying a security policy . . ." (per claim element 1-d) and after "configuring the access point . . . (per claim 2). The AnyConnect Agent "scans the applications every X minute and ***sends the differences from the last scan to the server***. The server displays the complete list of running and installed applications." ISE 3.0 Admin Guide at 1102-03. These "differences from the last scan" constitute "updated audit data pertaining to the device." **Continuous Endpoint Attribute Monitoring** You can use the AnyConnect agent to continuously monitor different endpoint attributes to ensure that dynamic changes are observed during posture assessment. This improves the overall visibility of an endpoint and helps you create posture policies based on their behavior. The AnyConnect agent monitors applications that are installed and running on an endpoint. You can turn on and off the feature and configure how often the data should be monitored. By default, data is collected every 5 minutes and is stored in the database. During initial posture, AnyConnect reports a complete list of running and installed applications. After initial posture, the AnyConnect agent scans the applications every X minute and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications. ISE 3.0 Admin Guide at 1102-03.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

6. The method of claim 2, further comprising receiving, from the agent, updated audit data pertaining to the device while the device has access to a less-restricted subset of the network.	Cisco ISE performs "[t]he method of claim 2, further comprising receiving, from the agent, updated audit data pertaining to the device while the device has access to a less-restricted subset of the network" and induces others to do so. As discussed above with respect to claim 5, Cisco ISE's Continuous Endpoint Attribute Monitoring mode is a mode through which ISE "receiv[es], from the agent, updated audit data pertaining to the device after configuring the access point." In this mode, and at a time after which the access point has been "configured," the (endpoint) device also "has access to a less-restricted subset of the network." As was described above with respect to both Cisco and third party (i.e. non-Cisco) access points, once ISE "configures the access point," the device has access to the "Corporate VLAN" (blue). ISE 3.0 Admin Guide at 804-06; *see also above* with respect to claim element 2 (showing how Cisco's ISE's "appl[ication of] the security policy includes configuring the access point"). Thus, "the device has access to a less-restricted subset of the network."

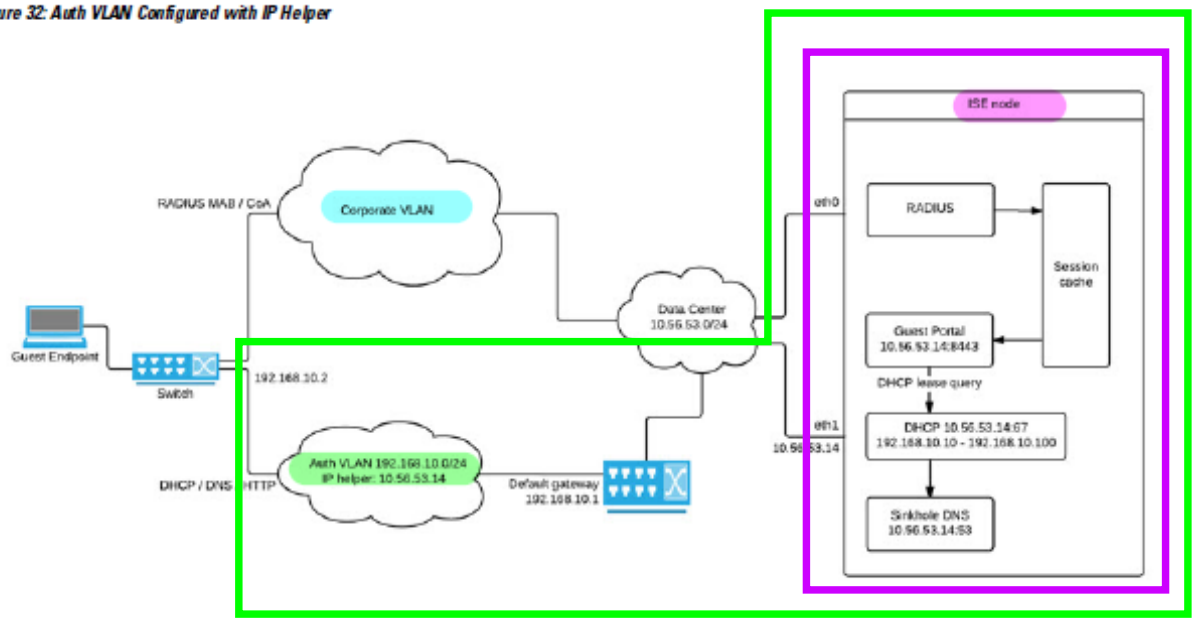
U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

Figure 31: Auth VLAN Connected to Cisco ISE Node



The following diagram displays a network with Auth VLAN and an IP helper.

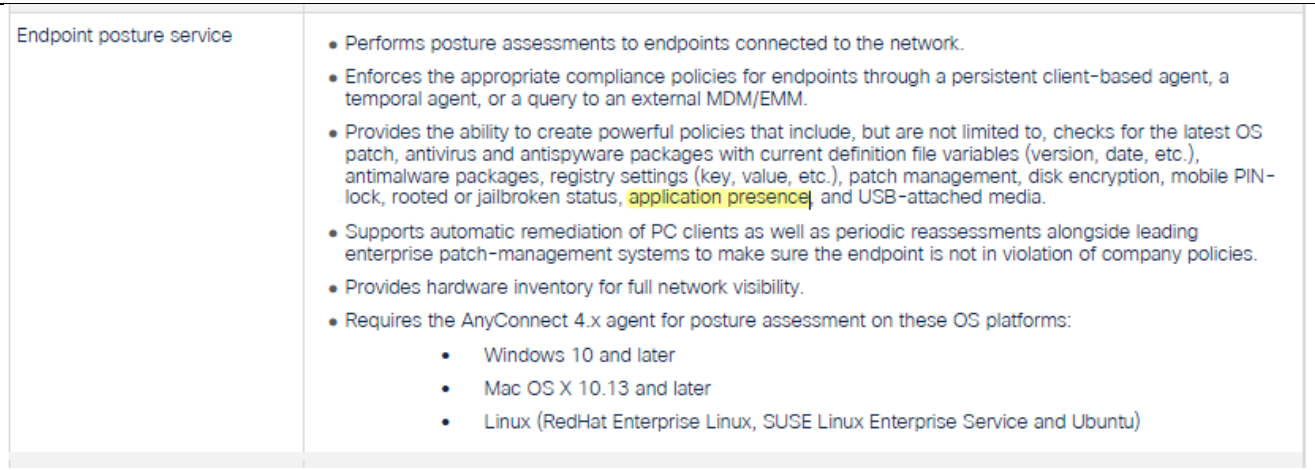
U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

	Figure 32: Auth VLAN Configured with IP Helper  ISE 3.0 Admin Guide at 804-06.
7. The method of claim 2, further comprising continuing to receive at the	Cisco ISE performs "[t]he method of claim 2, further comprising continuing to receive at the gatekeeper, from the agent, audit data pertaining to the device after the configuring of the access point" and induces others to do so. As was discussed above with respect to claim 5, Cisco ISE, through its Continuous Endpoint Attribute Monitoring mode, "receiv[es], from the agent, updated audit data pertaining to the device after

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

gatekeeper, from the agent, audit data pertaining to the device after the configuring of the access point.	configuring the access point." Furthermore, Cisco describes how in this mode, "[a]fter initial posture, the AnyConnect agent scans the applications every X minute and sends the differences from the last scan ***to the server***." By this, Cisco ISE "continu[es] to receive at the gatekeeper, from the agent, audit data . . ." Moreover, by ISE "send[ing]" this audit data to "the server," this audit data is "receive[d] at the gatekeeper. *See also above*, claim element 1-d (explaining the gatekeeper). **Continuous Endpoint Attribute Monitoring** You can use the AnyConnect agent to continuously monitor different endpoint attributes to ensure that dynamic changes are observed during posture assessment. This improves the overall visibility of an endpoint and helps you create posture policies based on their behavior. The AnyConnect agent monitors applications that are installed and running on an endpoint. You can turn on and off the feature and configure how often the data should be monitored. By default, data is collected every 5 minutes and is stored in the database. During initial posture, AnyConnect reports a complete list of running and installed applications. After initial posture, the AnyConnect agent scans the applications every X minute and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications. ISE 3.0 Admin Guide at 1102-03.
10. The method of claim 1, wherein the request includes a request for audit data pertaining to	Cisco ISE performs "[t]he method of claim 1, wherein the request includes a request for audit data pertaining to an application" and induces others to do so. Cisco states that it "[p]erforms posture assessments to endpoints connected to the network" and "enforces the appropriate compliance policies for [those] endpoints" through different mechanisms. ISE Data Sheet at 7. Such "security policies" "include, but are not limited to, checks for . . . application presence[,]" among other criteria. *Id.* Thus "the request includes a request for audit data pertaining to an application."

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

an application.	 ISE Data Sheet at 7. Cisco also describes "simple posture conditions," including "application conditions" on the client (the claimed "device"). ISE 3.0 Admin Guide at 1027. Thus "the request includes a request for audit data pertaining to an application."

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

Simple Posture Conditions

You can use the **Posture Navigation** pane to manage the following simple conditions:

- File Conditions: A condition that checks the existence of a file, the date of a file, and the versions of a file on the client.
- Registry Conditions: A condition that checks for the existence of a registry key or the value of the registry key on the client.
- Application Conditions: A condition that checks if an application or process is running or not running on the client.

Note If a process is installed and running, user is compliant. However, the Application condition works in reverse logic; If an application is not installed and not running, the end user is complaint. If an application is installed and running, the end user is non-complaint.

- Service Conditions: A condition that checks if a service is running or not running on the client.
- Dictionary Conditions: A condition that checks a dictionary attribute with a value.
- USB Conditions: A condition that checks for the presence of USB mass storage device.

Cisco also states—with respect to continuous endpoint attribute monitoring— "After initial posture [assessment], the AnyConnect agent scans ***the applications*** [on the endpoint, i.e. the "device"] every X minute and sends the differences from the last scan to the server. The server displays the ***complete list of running and installed applications***." ISE 3.0 Admin Guide at 1102-03. Thus "the request includes a request for audit data pertaining to an application."

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

	Continuous Endpoint Attribute Monitoring You can use the AnyConnect agent to continuously monitor different endpoint attributes to ensure that dynamic changes are observed during posture assessment. This improves the overall visibility of an endpoint and helps you create posture policies based on their behavior. The AnyConnect agent monitors applications that are installed and running on an endpoint. You can turn on and off the feature and configure how often the data should be monitored. By default, data is collected every 5 minutes and is stored in the database. During initial posture, AnyConnect reports a complete list of running and installed applications. After initial posture, the AnyConnect agent scans the applications every X minute and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications. ISE 3.0 Admin Guide at 1102-03.
11. The method of claim 1, wherein the received audit data includes audit data that pertains to an application on the device.	Cisco ISE performs "[t]he method of claim 1, wherein the received audit data includes audit data that pertains to an application on the device" and induces others to do so. As was discussed above with respect to claim 10, Cisco ISE performs "[t]he method of claim 1, wherein the request includes a request for audit data pertaining to an application" and induces others to do so. The examples of "audit data pertaining to an application" all concerned an application ***on the (endpoint) device*** — and thus Cisco ISE performs this step (and induces others to do so).
12. The method of claim 1,	Cisco ISE performs "[t]he method of claim 1, wherein the received audit data includes information that concerns operating system of the device" and induces others to do so.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

wherein the received audit data includes information that concerns operating system of the device.	Cisco states that ***hardware attributes*** (one type of "audit data" discussed with respect to claim element 1-b) can include "operating system types." ISE 3.0 Admin Guide at 175. • Status • Network Device Name • Location • UDID • IPv4 Address • Username • Hostname • OS Types • Anomalous Behavior • Endpoint Profile • Description • Endpoint Type ISE 3.0 Admin Guide at 175. Thus "the security policy audit is based at least in part on audit data collected by the agent concerning operating system of the device."

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

13. The method of claim 1, wherein the received audit data includes information that concerns antivirus software on the device.	Cisco ISE performs "[t]he method of claim 1, wherein the received audit data includes information that concerns antivirus software on the device" and induces others to do so. Cisco states that it "[p]erforms posture assessments to endpoints connected to the network" and "enforces the appropriate compliance policies for [those] endpoints" through different mechanisms. Such "security policies" "include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages . . . patch management . . . rooted or jailbroken status [and] application presence[,]" among others. **Endpoint posture service** • Performs posture assessments to endpoints connected to the network. • Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM. • Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media. • Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies. • Provides hardware inventory for full network visibility. • Requires the AnyConnect 4.x agent for posture assessment on these OS platforms: ◦ Windows 10 and later ◦ Mac OS X 10.13 and later ◦ Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu) ISE Data Sheet at 7. Thus, "the received audit data includes information that concerns antivirus software on the device."

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

14. The method of claim 1, wherein the received audit data includes information that concerns other devices coupled to the device.	Cisco ISE performs "[t]he method of claim 1, wherein the received audit data includes information that concerns other devices coupled to the device" and induces others to do so. Cisco states, with respect to "hardware attributes," that they include a field for "attached devices." ISE 3.0 Admin Guide at 174-75. Cisco further explains that "You can click the number in the ***Attached Devices*** column that corresponds to an endpoint to view the Name, Category, Manufacturer, Type, Product ID, and Vendor ID of the USB devices that are currently attached to the endpoint." *Id.*; *see also id.* at 1027 (USB Conditions), 1051 (USB Condition Settings), 1057 (USB_Block "[e]nsures that the endpoint device does not have any USB storage devices connected"). Thus, because Cisco's ISE can determine "attached devices" such as a USB (which are so attached to the endpoint), "the received audit data includes information that concerns other devices coupled to the device."
17. The method of claim 1, wherein the gatekeeper is configured to take part in bringing a software on the device up to date in response to applying the security policy.	Cisco ISE performs "[t]he method of claim 1, wherein the gatekeeper is configured to take part in bringing a software on the device up to date in response to applying the security policy" and induces others to do so. Cisco describes "Posture Remediation Options," and also "Custom Posture Remediation Actions," which include "a file, a link, an antivirus or antispyware ***definition updates***, launching programs, Windows ***updates***, or Windows Server ***Update*** Services (WSUS) remediation types." ISE 3.0 Admin Guide at 1059, 1061.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

Posture Remediation Options

The following table provides a list of posture remediation options that are supported by the Cisco ISE Posture Agents for Windows and Macintosh, and the Web Agent for Windows.

Table 162: Posture Remediation Options

ISE Posture Agent for Windows	ISE Posture Agent for Macintosh OS X
Message Text (Local Check)	Message Text (Local Check)
URL Link (Link Distribution)	URL Link (Link Distribution)
File Distribution	—
Launch Program	—
Antivirus Definition Update	Antivirus Live Update
Antispyware Definition Update	Antispyware Live Update
Patch Management Remediation (AC 4.1 - and ISE 1.4)	—
Windows Update	—
WSUS	—

Custom Posture Remediation Actions

A custom posture remediation action is a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) remediation types.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

	By "remediat[ing]" an endpoint, Cisco "bring[s] a software on the device up to date in response to applying the security policy." *See also* ISE 3.0 Admin Guide at 1061-64 ("Add an Antispyware Remediation: You can create an antispyware remediation, which ***updates clients*** with ***up-to-date file definitions for compliance after remediation***." and similar disclosures for Antivirus Remediation, File Remediation, Launch Program Remediation, Patch Management Remediation, and others). *See also* ISE 3.0 Admin Guide at 1029 (automatic updates in Windows clients): **Predefined Condition for Enabling Automatic Updates in Windows Clients** The pr_AutoUpdateCheck_Rule is a Cisco predefined condition, which is downloaded to the Compound Conditions window. This condition allows you to check whether the automatic updates feature is enabled on Windows clients. If a Windows client fails to meet this requirement, then the Network Access Control (NAC) Agents enforce the Windows client to enable (remediate) the automatic updates feature. After this remediation is done, the Windows client becomes posture compliant. The Windows update remediation that you associate in the posture policy overrides the Windows administrator setting, if the automatic updates feature is not enabled on the Windows client.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

and at 1048-50 (Patch Management Condition Settings):

Patch Management Condition Settings

The following table describes the fields in the **Patch Management Conditions** window. To view this window, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Conditions** > **Posture** > **Patch Management Condition**.

Table 157: Patch Management Condition

Field Name	Usage Guidelines
Name	Enter the name of the patch management condition.
Description	Enter a description for the patch management condition.
Operating System	Choose an operating system to check the installation of a patch management software on the endpoint, or check the latest patch management definition file updates to which the condition is applied. You can select the Windows OS or macOS. You can also select more than one version of an operating system to create the patch management condition.
Vendor Name	Choose a vendor from the **Vendor Name** drop-down list. Based on your selection, the patch management products and their supported versions, check type, and minimum compliant module support details are displayed in the **Products for Selected Vendor** table. The list in the table changes according to the selected operating system.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

Field Name	Usage Guidelines
Check Patches Installed	(Available only when you select the **Up To Date** check type) You can configure severity levels for missing patches, which are then deployed based on the severity. Choose one of the following options: • **Critical Only**: To check if critical software patches are installed on the endpoints in your deployment. • **Important and Critical**: To check if important and critical software patches are installed on the endpoints in your deployment. • **Moderate, Important, and Critical**: To check if moderate, important, and critical software patches are installed on the endpoints in your deployment. • **Low To Critical**: To check if low, moderate, important, and critical software patches are installed on the endpoints in your deployment. • **All**: To install the missing patches for all severity levels.

and also Randomized Changing MAC at 44 ("Cisco ISE performs the following functions with the external MDM server: . . . Handles device remediation: Endpoints are granted restricted access during remediation."); *and also* ISE Data Sheet at 4 ("Automated device-compliance checks for device-posture and ***remediation*** options using Cisco Secure Client (formerly Anyconnect agent), Temporal and Agentless options . . ." and 7 ("Supports automatic ***remediation*** of PC clients as well as periodic reassessments . . .")

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

Automated device-compliance checks for device-posture and remediation options using Cisco Secure Client (formerly Anyconnect agent), Temporal and Agentless options with custom scripts support. Cisco Secure Client Temporal and Agentless are two different ways to gather posture from endpoints beyond a full agent. Agentless option is supported from ISE 3.0 onwards Io Cisco Secure client also provide advanced VPN services for desktop and laptop checks. ISE also integrates with market-leading Mobile Device Management/Enterprise Mobility Management (MDM/EMM) vendors. MDM integration helps ensure that a mobile device is both secure and policy compliant before it is given access to the network.

. . .

Endpoint posture service	• Performs posture assessments to endpoints connected to the network.
	• Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM.
	• Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media.
	• Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies.
	• Provides hardware inventory for full network visibility.
	• Requires the AnyConnect 4.x agent for posture assessment on these OS platforms:
	  ◦ Windows 10 and later
	  ◦ Mac OS X 10.13 and later
	  ◦ Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu)

ISE Data Sheet at 4, 7.

Furthermore, the "gatekeeper is configured to take part in bringing a software on the device up to date in response to applying the security policy[.]" Cisco ISE's—which is a "a security policy management platform that provides secure access to network resources" (ISE 3.0 Release Notes at 1), which can "create[e] ***access control policies*** for the various network elements," (*id.*), and which is "an identity-

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

	based network access control and ***policy enforcement system*** [that] functions as a common policy engine that enables endpoint access control and network device administration" (ISE 3.0 Admin Guide at 1)—contains a gatekeeper. *See also above*, with respect to claim elements 1-c & d.
[22-preamble] A method for auditing a device, the method comprising:	Cisco infringes this claim by making, using, testing, offering for sale, and selling the ISE product and system and through performance of each of the claimed steps and/or providing instructions and data from its servers to third-parties to perform at least one of the claimed steps. Further, subsequent to Cisco's making, using, testing, offering for sale, and selling of the ISE, Cisco offers services to third-parties and customers with respect to the ISE. For example, these can include "Technical Services," "Advisory Services," and "Cisco Talos Incidence Response" services. (https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/ise-licensing-guide-og.html). For technical services, for example, Cisco encourages customers to purchase "Cisco Smart Net Total Care" for Cisco ISE physical appliances and Software Support (SWSS) contracts for Cisco ISE virtual machines. For advisory services, Cisco offers Expert Services to address "your business objectives with the technology we offer" (including ISE). *Id*. And for the Talos Incident Response, Cisco provides a full suite of proactive and emergency services to help third-parties prepare, respond, and recover from a cybersecurity breach. Cisco explains that third-parties can "order and transact Cisco Talos Incident Response when ordering Cisco ISE subscriptions." *Id*. Cisco ISE performs "[a] method for auditing a device" and induces others to do so. As explained above with respect to claim 1's preamble, Cisco's ISE meets this limitation.
[22-a] performing an authentication using an EPA	Cisco ISE "perform[s] an authentication using an EPA protocol from the device, the device being connected to an access point configured to use an 802.1x protocol [,]"and induces others to do so. As explained above with respect to claim element 1-a, Cisco ISE "perform[s] an authentication using an

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

protocol from the device, the device being connected to an access point configured to use an 802.1x protocol;	EAP protocol from the device, the device being connected via a computer network to an access point configured to use an 802.1x protocol[.]" Thus, Cisco's ISE meets this claim limitation.
[22-b] sending a request for audit data to an agent running on the device;	Cisco ISE "send[s] a request for audit data to an agent running on the device,]" and induces others to do so. As explained above with respect to claim element 1-b, Cisco's ISE meets this limitation.
[22-c] receiving the audit data at a gatekeeper configured to control access to a network, from the agent, the audit data	Cisco ISE "receiv[es] the audit data at a gatekeeper configured to control access to a network, from the agent, the audit data pertaining to the device and having been obtained by the agent[,]" and induces others to do so. As explained above with respect to claim element 1-c, Cisco's ISE meets this limitation.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

pertaining to the device and having been obtained by the agent;	
[22-d] applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication, the applying of the security policy taking place under control of the gatekeeper, where applying the	Cisco ISE "appl[ies] a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication, the applying of the security policy taking place under control of the gatekeeper, where applying the security policy includes configuring the access point[,]" and induces others to do so. As explained above with respect to claim element 1-d, Cisco ISE "appl[ies] a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication, the applying of the security policy taking place under control of the gatekeeper." Additionally, as explained above with respect to claim 2, "applying the security policy includes configuring the access point." Thus, Cisco's ISE meets this claim limitation.

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

security policy includes configuring the access point;	
[22-e] receiving, from the agent, updated audit pertaining to the device while the device has access to a less-restricted subset of the network; and **[22-f]** re-auditing the device in accordance to the security policy using the received	Cisco's ISE "receiv[es], from the agent, updated audit pertaining to the device while the device has access to a less-restricted subset of the network; and re-audit[s] the device in accordance to the security policy using the received updated audit data" and induces others to do so. As explained above with respect to claim 6, Cisco ISE "receiv[es], from the agent, updated audit data pertaining to the device while the device has access to a less-restricted subset of the network." Also as explained above, Cisco ISE has a ***Continuous Endpoint Attribute Monitoring Mode.*** In this mode, the AnyConnect Agent operates (as is relevant to this claim) "[a]fter the initial posture" *see ISE* 3.0 Admin Guide at 1102-03—that is, after "applying a security policy . . ." (per claim element 1-d) and "while the device has access to a less-restricted subset of the network." *See also above* with respect to claim 6. The AnyConnect Agent "scans the applications every X minute and ***sends the differences from the last scan to the server***. The server displays the complete list of running and installed applications." ISE 3.0 Admin Guide at 1102-03. These "differences from the last scan" constitute "updated audit data." Additionally, the ISE server "receives" this data and it can then "re-audit" the device. (Cisco describes ISE doing these re-audits "every X minute[s].")

U.S. Patent No. 8,578,444 (Cisco's Identity Services Engine)

updated audit data.	**Continuous Endpoint Attribute Monitoring** You can use the AnyConnect agent to continuously monitor different endpoint attributes to ensure that dynamic changes are observed during posture assessment. This improves the overall visibility of an endpoint and helps you create posture policies based on their behavior. The AnyConnect agent monitors applications that are installed and running on an endpoint. You can turn on and off the feature and configure how often the data should be monitored. By default, data is collected every 5 minutes and is stored in the database. During initial posture, AnyConnect reports a complete list of running and installed applications. After initial posture, the AnyConnect agent scans the applications every X minute and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications. ISE 3.0 Admin Guide at 1102-03. Thus, Cisco ISE "receiv[es], from the agent, updated audit pertaining to the device while the device has access to a less-restricted subset of the network; and re-audit[s] the device in accordance to the security policy using the received updated audit data" and induces others to do so.

EXHIBIT F-6

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

U.S. Patent No. 8,117,645	Cisco's Identity Services Engine
[Claim 1—preamble] A network access control system, comprising:	Cisco infringes this claim by making, using, testing, offering for sale, and selling the Identity Services Engine ("ISE")[1] product and system and through performance of each of the claimed steps and/or providing instructions and data from its servers to third-parties to perform at least one of the claimed steps. Further, subsequent to Cisco's making, using, testing, offering for sale, and selling of the ISE, Cisco offers services to third-parties and customers with respect to the ISE. For example, these can include "Technical Services," "Advisory Services," and "Cisco Talos Incidence Response" services. (https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/ise-licensing-guide-og.html). For technical services, for example, Cisco encourages customers to purchase "Cisco Smart Net Total Care" for Cisco ISE physical appliances and Software Support (SWSS) contracts for Cisco ISE virtual machines. For advisory services, Cisco offers Expert Services to address "your business objectives with the technology we offer" (including ISE). *Id*. And for the Talos Incident Response, Cisco provides a full suite of proactive and emergency services to help third-parties prepare, respond, and recover from a cybersecurity breach. Cisco explains that third-parties can "order and transact Cisco Talos Incident Response when ordering Cisco ISE subscriptions." *Id*. Additionally, and as set forth in InfoExpress's 3-1 disclosures, Cisco's ISE also includes Cisco's ISE (NAC) appliance. Specifically, these are Cisco-provided tangible hardware and "virtual

[1] Certain portions of the evidence cited herein identify and relate to the Cisco Identity Services Engine, Release version 3.0. We understand that each version of the Accused Technology is operationally and functionally the same with respect to and for the purposes of identifying infringement for each of the Asserted Claims.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	appliances" on which ISE can be deployed. A list of accused ISE (NAC) Appliances (also referred to as "hardware platforms") which ISE supports, are disclosed in InfoExpress's Disclosure of Asserted Claims and Infringement Contentions per Patent L.R. 3-1 and 3-2 at Section II.B.2. These ISE (NAC) Appliances are listed in Cisco's Identity Services Engine Administrator Guides, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0001603 to 0014308, and also their Release Notes for ISE Releases 1.04, 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014606 to 0015185. Cisco's ISE (NAC) appliances are directed to "[g]ranting and denying network access" and using "attributes related to users and their devices" in "determining authorized network access." https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/datasheet-c78-726524.html.[2] Cisco further explains that its NAC appliance (known in one example as "The Cisco Secure Network Server") "supports Cisco's powerful network access and control security applications." *Id*. Further, Cisco explains that the "Cisco Secure Network Server… is configured specifically to support the Cisco Identity Services Engine (ISE) security application." *Id*.

[2] Certain portions of the evidence cited herein identify and relate to the "Cisco Secure Network Server Data Sheet" for Cisco SNS-3715, SNS-3755, and SNS-3795 Secure Network Server. We understand that each other version of the Accused Technology relating to these Cisco ISE NAC appliances including ISE-3315-K9, ISE-3355-K9, and ISE-3395-K9; SNS-3415-K9 and SNS-3495-K9; SNS -3515-K9 and SNS-3595-K9; SNS-3615-K9, SNS-3655-K9, and SNS-3695-K9; and ISE Virtual Machine (S/M/L)-K9 are operationally and functionally the same with respect to and for the purposes of identifying infringement for each of the Asserted Claims.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	To the extent the preamble is limiting, Cisco's ISE is "an identity-based ***network access control*** and policy enforcement ***system*** " and thereby is a "network access control system." Cisco Identity Services Engine (ISE) is an identity-based network access control and policy enforcement system. It functions as a common policy engine that enables endpoint access control and network device administration for enterprises. You can leverage Cisco ISE to ensure compliance, enhance infrastructure security, and streamline service operations. A Cisco ISE administrator can gather real-time contextual data for a network, including users and user groups (who?), device type (what?), access time (when?), access location (where?), access type (wired, wireless, or VPN) (how?), and network threats and vulnerabilities. *See generally* Cisco Identity Services Engine Administrator Guide, Release 3.0 ("ISE 3.0 Admin Guide"), at 1, available at https://www.cisco.com/c/en/us/ td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf (last visited May 31, 2023). *See also* Release Notes for Cisco Identity Services Engine, Release 3.0 ("ISE 3.0 Release Notes") at 1, *available at* https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/release_notes/b_ise_30_rn.pdf (last visited May 31, 2023) describing Cisco ISE as a "security policy management platform that provides secure access to network resources").

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	Introduction to Cisco Identity Services Engine Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, Cisco Wireless Controllers, Virtual Private Network (VPN) gateways, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation. Cisco ISE is available on secure network server appliances with different performance characterizations, and also as software that can be run on a virtual machines (VMs). Note that you can add more appliances to a deployment for better performance. Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also enables the configuration and management of distinct personas and services, thereby giving you the ability to create and apply services, where needed, in a network, but operate the Cisco ISE deployment as a complete and coordinated system.
[1-a] an authentication module stored in memory and executable by a processor to authenticate a device seeking network access based at least on	Cisco's ISE comprises and includes "an authentication module stored in memory and executable by a processor to authenticate a device seeking network access based at least on authentication information received from the device." Cisco's ISE "uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods."

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

authentication information received from the device;	• **Bring Your Own Device (BYOD)**: Cisco ISE allows your employees and guests to securely use their personal devices on your enterprise network. BYOD feature end users can use configured pathways to add their devices, and provision predefined authentications and levels of network access. • **Asset Visibility**: Cisco ISE gives you visibility and control over who and what is on your network consistently, across wireless, wired, and VPN connections. Cisco ISE uses probes and device sensors to listen to the way devices connect to the network. The Cisco ISE profile database, which is extensive, then classifies the device. This gives the visibility and context you need to grant the right level of network access. • **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods. • **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation. *See generally* Cisco Identity Services Engine Administrator Guide, Release 3.0 ("ISE 3.0 Admin Guide"), at 2, available at https://www.cisco.com/c/en/us/ td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf (last visited May 31, 2023); *see also id.* (explaining that for the TACACS+ security protocol, "Network devices can be configured to query Cisco ISE for ***authentication and authorization of device administrator actions***."); *id.* (explaining that for ISE's bring-your-own-device (BYOD) feature, "end users can use configured pathways to add their devices, and ***provision predefined authentications and levels of network access***."); *see also id.* at 183 ("UTF-8 Credential Authentication"), 214 ("Wildcard Certificates for HTTPS and Extensible Authentication Protocol Communication"), 268 (Configure Cisco ISE to Use Certificates for Authenticating Personal Devices); 269 (Create a Certificate Authentication Profile for TLS-Based Authentication); 270 (Create an Identity Source Sequence for TLS-Based Authentication); (275 (Configure the ***Dot1X Authentication Policy*** Rule for TLS-Based Authentication); 276 ("Create

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	Authorization Profiles for ***CentralWeb Authentication*** and Supplicant-Provisioning Flows"); 278-79 ("This section lists the authorization profiles that you must create for enabling ***certificate-based authentication*** in Cisco ISE. You must have already created the ACLs (NSP-ACL and NSP-ACL-Google) on the wireless LAN controller (WLC)."); 280 (Cisco ISE CA Issues Certificates to [Adaptive Security Appliance ("ASA")] VPN Users) ("The ASA requests ***certificate-based authentication*** from the client. . . . The ASA proceeds to primary user ***authentication (AAA)*** using the username/ password and passes the information to the ***authentication server (ISE)***."); 354 (discussing exemplary "authentication method[s] that [are] used by the RADIUS protocol"); 428-29 (Guest Access Web Authentication Options); 429-30 (Network Access Devices with Central Web Authentication Process, "In this scenario, the network access device (NAD) makes a new authorization request to the Cisco ISE RADIUS server from an unknown endpoint connection. The endpoint then receives a url-redirect to Cisco ISE. . . . If the guest device is connected to a NAD, the guest service interaction takes the form of a MAC Authentication Bypass (MAB) request that leads to a Guest portal Central WebAuth login. The following is an outline of the subsequent ***Central Web Authentication (Central WebAuth)*** process, which applies to both wireless and wired network access devices."); 430-31 (Wireless LAN Controller with Local Web Authentication Process); 431 (Wired Network Access Device with Local Web Authentication Process); 433-34 (Device Registration Web Authentication Process); 512 ("In Cisco ISE, you can ***authenticate administrators*** via an external identity store such as Active Directory, LDAP, or RSA SecureID."); 513 (External Authentication and Authorization); 635 ("Cisco ISE can authenticate a subject (user or host) against an [Lightweight Directory Access Protocol ('LDAP')] identity source . . ."); 862 (Password-Based Authentication); 1183 (Enable Your Switch to Support StandardWeb Authentication); 1186 (Enable 802.1X Port-Based Authentication for Switch Ports and Enable EAP for Critical Authentications); 1188-90 (Enable Switch Ports for 802.1X and [MAC-Based Authentication ("MAB")]); 1232-38 ("Live Authentications: "You can monitor recent ***RADIUS authentications*** as they occur . . .").

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	Cisco also explains that its ISE uses "***policy sets*** [with which] you [] manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group ***authentication and authorization policies*** within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type, and similar parameters." Cisco further explains that "[w]hen creating policy sets, you can configure the rules (configured with condition and results in order to choose . . . the identity sources on the ***authentication policy*** level[.]" Cisco further explains that hierarchically, authentication policy rules are applied first and before local policy exceptions, global policy exceptions and authorization policy rules. ISE 3.0 Admin Guide at 856.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

Policy Sets

Cisco ISE is a policy-based, network-access-control solution, which offers network access policy sets, allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type, and similar parameters. When you install Cisco ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules.

When creating policy sets, you can configure these rules (configured with conditions and results) in order to choose the network access services on the policy set level, the identity sources on the authentication policy level, and network permissions on the authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE-supported dictionaries for different vendors. Cisco ISE allows you to create conditions as individual resuable policy elements.

The network access service to be used per policy set to communicate with the network devices is defined at the top level of that policy set. Network access services include:

- Allowed protocols—the protocols configured to handle the initial request and protocol negotiation.
- A proxy service—sends requests to an external RADIUS server for processing.

Note From the **Work Centers** > **Device Administration** , you can also select a relevant TACACS server sequence for your policy set. Use the TACACS server sequence to configure a sequence of TACACS proxy servers for processing.

Policy sets are configured hierarchically, where the rule on the top level of the policy set, which can be viewed from the **Policy Set** table, applies to the entire set and is matched before the rules for the rest of the policies and exceptions. Thereafter, rules of the set are applied in this order:

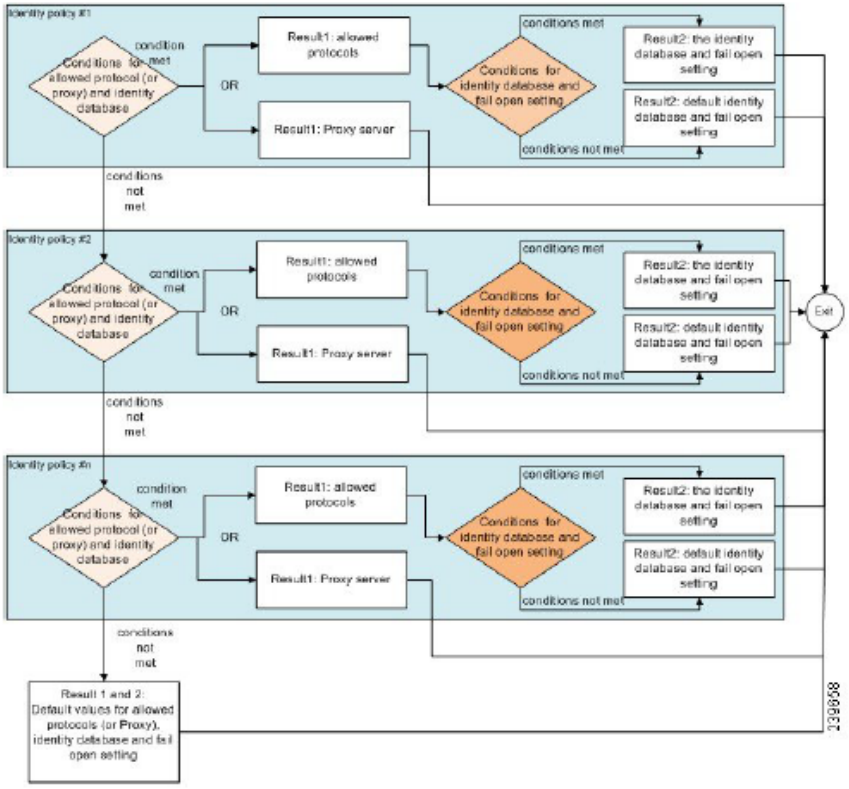
1. Authentication policy rules
2. Local policy exceptions
3. Global policy exceptions
4. Authorization policy rules

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	Cisco goes on to explain that "Each policy set can contain ***multiple authentication rules*** that together represent the authentication policy for that set. Priority of the authentication policies is determined based on the order to those policies as they appear within the policy set itself[.]" **Authentication Policies** Each policy set can contain multiple authentication rules that together represent the authentication policy for that set. Priority of the authentication policies is determined based on the order to those policies as they appear within the policy set itself (from the Set view page in the Authentication Policy area). Cisco ISE dynamically chooses the network access service (either an allowed protocol a server sequence) based on the settings configured on the policy set level, and thereafter checks the identity sources and results from the authentication and authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE dictionary. Cisco ISE allows you to create conditions as individual policy elements that can be stored in the Library and then can be reused for other rule-based policies. The identity method, which is the result of the authentication policy, can be any one of the following: . . .

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

Figure 40: Authentication Policy Flow



ISE 3.0 Admin Guide at 858-59; *see also id.* at 860 (Configure Authentication Policies: Define an authentication policy per policy set by configuring and maintaining multiple authentication rules, as necessary.").

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

Cisco also explains that with its mobile device management (MDM) server integration with ISE, one can authenticate using a Device Unique ID/Global Unique ID (DUID/GUID).

DUID/GUID data flow

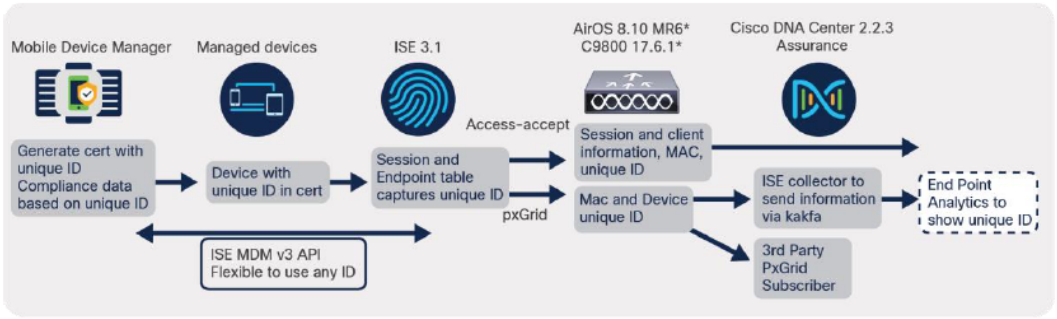


Figure 4.
DUID/GUID data flow

- This solution relies on the mobile device manager, also referred to as a device manager or unified endpoint manager (for example, Cisco Meraki, Airwatch, Intune, MobileIron, etc.), which manage devices in an enterprise infrastructure.
- ISE provides the provisioning of the device with the unique ID-based (DUID) certificates.
- The device presents this certificate during TLS-based authentication. ISE authorizes the devices and also reads the unique ID from the certificate.
- The DUID is used for compliance check with MDM servers and also a unique identifier of the device in the endpoint table.
- The randomized MAC address will not matter, as now the device will have a DUID using the ID in the certificate.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	Cisco, Randomized and Changing MAC Deployment Guide (2022) at 42, https://www.cisco.cowm/c/en/us/products/collateral/wireless/randomized-changing-mac-dg.pdf (last visited June 27, 2023). **Handle random and changing MAC addresses with an MDM server** To avoid issues caused by the use of the MAC address randomization method, configure Cisco ISE to identify endpoints that are connected to an MDM server by a unique device identifier instead of a MAC address. Mobile devices increasingly use random and changing MAC addresses for each SSID. This means that an endpoint presents different MAC addresses to the MDM server and to Cisco ISE. As a result, when the MDM server and Cisco ISE are integrated and an action is initiated for an endpoint, issues arise because the endpoint's identity is different in the two systems. In Cisco ISE, you can now work around this problem by configuring Cisco ISE to use a unique device identifier instead of MAC addresses. When an endpoint enrolls with an MDM server, the MDM server sends a certificate with a GUID value to the endpoint. The endpoint uses this certificate for authentication with Cisco ISE. Cisco ISE receives the GUID for the endpoint from the certificate. All communications between Cisco ISE and the MDM server now use the GUID to identify the endpoint, helping ensure accuracy and consistency between the two systems. Note that GUIDs are available only in certificate-based authentication methods. Basic authentication methods that use only a username and password will not be able to leverage the GUID-based solution. The Cisco ISE MDM APIs have been updated (Cisco ISE MDM APIs Version 3) to facilitate the gathering and management of GUID data. Currently, MobileIron supports Cisco ISE MDM APIs Version 3, and sends GUID information to Cisco ISE. Randomized and Changing MAC Deployment Guide at 48. • **Time Interval for Compliance Device ReAuth Query:** When an endpoint is authenticated or reauthenticated, Cisco ISE uses a cache to get the MDM variables for that endpoint. If the age of the cached value is higher than the value configured in this field, Cisco ISE sends a new device query to the MDM server to get new values. If the compliance status has changed, Cisco ISE triggers the appropriate CoA. Randomized and Changing MAC Deployment Guide at 50.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	Cisco further discloses "authentication information received from the device [seeking network access]." Examples of such "authentication information" include, but are not limited to: • Passwords (ISE 3.0 Admin Guide at 862); • In use cases involving certificate-based authentication, "certificate signing requests" from the devices (which Cisco terms "endpoints"). (*Id.* at 268); • In use cases where a device connects to the network through a Cisco Adaptive Security Appliance's ("ASA") VPN, "attributes such as the [device's] unique device identifier (for example, [International Mobile Equipment Identity ('IMEI')])" (*Id.* at 280-81); • "Endpoint attribute data" which is received "from multiple sources, such as Cisco Catalyst 9000 Series devices, CMBD connections, telemetry devices, and more" and which further includes "Attributes related to Random MAC addresses," (*Id.* at 874-75); • Source IP addresses, which Access Control Lists (ACL) use in conjunction with the RADIUS protocol to grant authorization by filtering those source IP addresses along with "destination IP addresses, transport protocols, and additional parameters." (*Id.* at 867); • IPv6 attributes, such as NAS-IPv6-Address, Framed-Interface-Id, Framed-IPv6-Prefix, Login-IPv6-Host, Framed-IPv6-Route, Framed-IPv6-Pool, Delegated-IPv6-Prefix, Framed-IPv6-Address, DNS-Server-IPv6-Address, Route-IPv6-Information, Delegated-IPv6-Prefix-Pool, Stateful-IPv6-Address-Pool. (*Id.* at 901). *See also id.* at 268 ("Configure Cisco ISE to Use Certificates for Authenticating Personal Devices"), 354 (discussing exemplary "authentication method[s] that [are] used by the RADIUS protocol"),

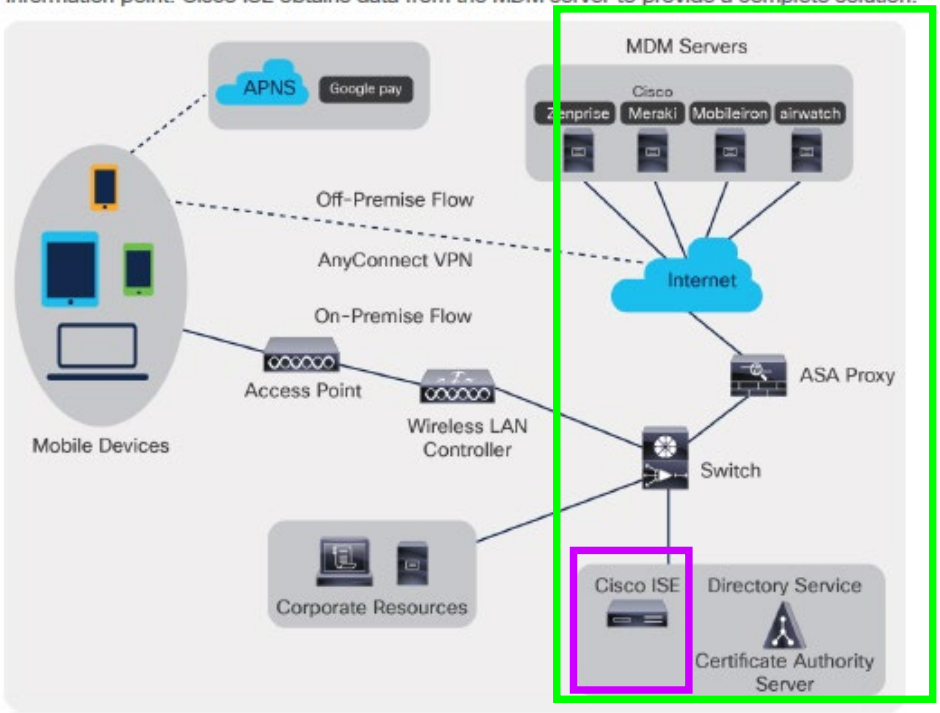
U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	934-35 ("RADIUS-Based EAP Authentication Flow"), 1186 ("Enable 802.1X Port-Based Authentication for Switch Ports"), 1186 ("Enable EAP for Critical Authentications"). By way of further example, the ISE includes "an authentication module stored in memory and executable by a processor" in the way it communicates with the following hardware devices: • Access points and switches. *See, e.g.*, ISE 3.0 Admin Guide at 867-68 ("Access control lists (ACLs) are lists of access control entries (ACEs), ***which may be applied by a Policy Enforcement Point (for example, a switch)*** to a resource. . . . Static ACLs reside on and are ***directly configured from the switch*** . . . downloadable ACLs (DACLs) can be configured, managed and applied in your authorization policies from the ISE GUI."); 874 ("Cisco AI Endpoint Analytics receives endpoint attribute data from multiple sources, ***such as Cisco Catalyst 9000 Series devices***."); 901 ("When an IPv6-enabled endpoint connects to the Cisco ISE network, it communicates with the ***Network Access Device (NAD)*** over an IPv6 network. The NAD conveys the accounting and profiling information from the endpoint (including IPv6 values) to Cisco ISE over an IPv4 network."); 1183 (Enable Your ***Switch*** to Support StandardWeb Authentication); 1186 (Enable 802.1X Port-Based Authentication for ***Switch Ports*** and Enable EAP for Critical Authentications); 1188-90 (Enable ***Switch Ports*** for 802.1X and [MAC-Based Authentication ("MAB")]); Randomized Changing MAC at 4 ("Catalyst 9800 WLCs and the ***Catalyst 9100 access points*** [are] the best in the enterprise-class market."); • Wireless LAN Controllers ("WLC"). *See, e.g.*, ISE 3.0 Admin Guide at 278-79 ("This section lists the authorization profiles that you must create for enabling certificate-based authentication in Cisco ISE. You must have already created the ACLs (NSP-ACL and NSP-ACL-Google) on the ***wireless LAN controller (WLC)***."); 430-31 ("***Wireless LAN Controller*** with Local Web Authentication Process"); Randomized Changing MAC at 4 ("***Catalyst***

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	9800 WLCs and the Catalyst 9100 access points [are] the best in the enterprise-class market."); and • Adaptive Security Appliances ("ASA"). *See, e.g.*, ISE 3.0 Admin Guide at 280-81 ("ISE CA issues certificates to client machines connecting over ***ASA VPN***. Using this feature, you can automatically provision certificates to end devices that connect over ASA VPN."); In use cases where a device connects over a Cisco Adaptive Security Appliance's ("ASA") VPN, "attributes such as the [device's] unique device identifier (for example, [International Mobile Equipment Identity ('IMEI')]" (*Id.* at 280-81); These hardware devices include those made by both Cisco and also third-parties. Cisco also describes ISE-compatible third-party devices in its ISE 3.0 Admin Guide at 806-07, including those made by Aruba, Motorola, HP, Ruckus, Alcatel, Brocade, and Juniper.
[1-b-i] a gatekeeper stored in memory and executable to: formulate an audit request,	Cisco's ISE comprises "a gatekeeper stored in memory." Cisco explains that "ISE is the enforcement point . . . [that] then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points."

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

[1-b-ii] send the audit request to the device,	In the following illustration, Cisco ISE is the enforcement point and the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution.  Figure 5. Cisco ISE and MDM servers Randomized and Changing MAC Deployment Guide at 43.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	You can configure Cisco ISE to interoperate with one or more external MDM servers. By setting up this type of third-party connection, you can use the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. It then applies the appropriate access control policies to switches, access routers, wireless access points, and other network access points. The policies give you greater control of the remote devices that are accessing the Cisco ISE-enabled network. Randomized and Changing MAC Deployment Guide at 43. Cisco explains how the ISE is executable to: formulate an audit request, [and] send the audit request to the device in that: "ISE allows you to check for compliance, also known as ***posture***, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services." ISE 3.0 Admin Guide at 2. Cisco goes on to explain these posture agents in greater depth:

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

Posture Types

The following posture agents monitor and enforce Cisco ISE posture policies:

- **AnyConnect**: Deploys the AnyConnect agent to monitor and enforce Cisco ISE posture policies that require interaction with the client. The AnyConnect agent stays on the client. For more information about using AnyConnect in Cisco ISE, see Cisco AnyConnect Secure Mobility, on page 1099.
- **AnyConnect Stealth**: Runs posture as a service, with no user interface. The agent stays on the client.

  When you choose the AnyConnect Stealth posture type in the posture requirement, some of the conditions, remediations, or attributes in a condition are disabled (grayed out). For example, when you enable AnyConnect Stealth requirement, the Manual Remediation Type is disabled (grayed out) because this action requires client-side interaction.

  When you map the posture profile to the AnyConnect configuration, and then map the AnyConnect configuration to the Client Provisioning window for AnyConnect Stealth mode deployment:

  - AnyConnect can read the posture profile and set it to the intended mode.
  - AnyConnect can send information related to the selected mode to Cisco ISE during the initial posture request.
  - Cisco ISE can match the right policy, based on the mode and other factors, such as identity group, OS, and compliance module.

. . . .

- **Temporal Agent**: When a client attempts to access the trusted network, Cisco ISE opens the Client Provisioning portal. The portal instructs the user to download and install the agent, and run the agent. The temporal agent checks the compliance status, and sends the status to Cisco ISE. Cisco ISE acts based on the results. The temporal agent removes itself from the client after compliance processing completes. The temporal agent does not support custom remediation. The default remediation supports only message text.

. . . .

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

- **Agentless Posture**—Agentless posture provides posture information from clients, and completely removes itself when finished. No action is required from the end user. Unlike the Temporal agent, Agentless Posture connects to the client as an administrative user. For more information about using Agentless Posture in Cisco ISE, see Agentless Posture, on page 1012.

ISE 3.0 Admin Guide at 1010-11.

Furthermore, Cisco's ISE "formulate[s] an audit request, [and] send[s] th[at] audit request to the device [seeking network access.]" Cisco describes how ISE, generally, "enables [the user] to validate and maintain security capabilities on any client machine that accesses the protected network." ISE 3.0 Admin Guide at 1057. ISE does this by formulating and sending requests for certain information to the devices seeking network access. ISE can execute these requests by, for example, agents that reside on the device seeking network access:

Client Posture Assessment

To ensure that the imposed network security measures remain relevant and effective, Cisco ISE enables you to validate and maintain security capabilities on any client machine that accesses the protected network. By employing posture policies that are designed to ensure that up-to-date security settings or applications are available on client machines, the Cisco ISE administrator can ensure that any client machine that accesses the network meets, and continues to meet, the defined security standards for enterprise network access. Posture compliance reports provide Cisco ISE with a snapshot of the compliance level of the client machine at the time of user login, as well as any time a periodic reassessment occurs.

Posture assessment and compliance occurs using one of the following agent types available in Cisco ISE:

- AnyConnect ISE Agent: A persistent agent that can be installed on Windows or Mac OS X client to perform posture compliance functions.
- Cisco Temporal Agent: A temporary executable file that is run on the client to check the compliance status. The agent is removed from the client machine after the login session is terminated. By default, the agent resides in the Cisco ISE ISO image, and is uploaded to Cisco ISE during installation.

ISE 3.0 Admin Guide at 1057.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

Posture Types

The following posture agents monitor and enforce Cisco ISE posture policies:

- **AnyConnect**: Deploys the AnyConnect agent to monitor and enforce Cisco ISE posture policies that require interaction with the client. The AnyConnect agent stays on the client. For more information about using AnyConnect in Cisco ISE, see Cisco AnyConnect Secure Mobility, on page 1099.
- **AnyConnect Stealth**: Runs posture as a service, with no user interface. The agent stays on the client.

  When you choose the AnyConnect Stealth posture type in the posture requirement, some of the conditions, remediations, or attributes in a condition are disabled (grayed out). For example, when you enable AnyConnect Stealth requirement, the Manual Remediation Type is disabled (grayed out) because this action requires client-side interaction.

  When you map the posture profile to the AnyConnect configuration, and then map the AnyConnect configuration to the Client Provisioning window for AnyConnect Stealth mode deployment:

  - AnyConnect can read the posture profile and set it to the intended mode.
  - AnyConnect can send information related to the selected mode to Cisco ISE during the initial posture request.
  - Cisco ISE can match the right policy, based on the mode and other factors, such as identity group, OS, and compliance module.

. . . .

- **Temporal Agent**: When a client attempts to access the trusted network, Cisco ISE opens the Client Provisioning portal. The portal instructs the user to download and install the agent, and run the agent. The temporal agent checks the compliance status, and sends the status to Cisco ISE. Cisco ISE acts based on the results. The temporal agent removes itself from the client after compliance processing completes. The temporal agent does not support custom remediation. The default remediation supports only message text.

ISE 3.0 Admin Guide at 1010-11.

Another way by which Cisco's ISE can execute these audit requests is by "agentless posture[, which] ***provides posture information from clients***, and completely removes itself when finished,

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	until invoked by Cisco ISE again." ISE 3.0 Admin Guide at 1012. Cisco further describes how in agentless posture mode, "Posture evaluation runs on the client, and sends the status to Cisco ISE." *Id.* at 1013. *See also and also* Cisco Community, *How To: Agentless Posture Configuration, Validation & Troubleshooting* (Oct. 15, 2020), *available at* https://community.cisco.com/t5/security-knowledge-base/how-to-agentless-posture-configuration-validation-amp/ta-p/4152763 (last visited May 31, 2023). **Agentless Posture** Agentless posture provides posture information from clients, and completely removes itself when finished, until invoked by Cisco ISE again. No action is required from the end user. **Requirements** • The client must be reachable by its IP address, and that IP address must be available in RADIUS accounting. IPv6 is not supported. • Windows and Mac clients are currently supported. • For Windows clients, port 5985 to access Powershell on the client must be open. Powershell must be version 5.1 or later. The client must have cURL version 7.34 or later. • For macOS clients, port 22 to access SSH must be open to access the client. The client must have cURL version 7.34 or later. . . . .

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	Agentless Posture Process Flow 1. The client connects to the network. 2. Cisco ISE detects if agentless posture is enabled in the authorization profile used by client. 3. If so, Cisco ISE sends an agentless posture job request to the Cisco ISE Messaging queue. 4. Cisco ISE gets the job from the messaging queue, and starts the agentless posture flow. 5. Cisco ISE connects to the client via power shell or SSH. 6. Cisco ISE pushes the certificate, if it's not already in the client's trust certificate authority store. 7. Cisco ISE runs the client provisioning policy. 8. Cisco ISE pushes the agentless plug-in to the client and launches the plug-in. 9. Posture evaluation runs on the client, and sends the status to Cisco ISE. 10. Cisco ISE removes the agentless plug-in from the client. Logs of the posture flow remain on the client for 24 hours, or until the client deletes them. Cisco describes certain "default posture policies" within ISE. These policies "check" for certain information on the device seeking network access—the presence of antimalware software, the presence of certain applications, the presence of a firewall program, and that the device "does not have any USB storage devices connected." ISE 3.0 Admin Guide at 1056-57; *see also id.* at 1058 (Posture Assessment Options).

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

Default Posture Policies

The Cisco ISE software comes with a number of pre-configured posture policies that make it easier for you to create the posture policies and profiles. These policies are disabled by default. You can enable these policies based on your requirements. Following are some of the default posture policies.

Rule Name	Description	Requirements
Default_Antimalware_Policy_Mac	Checks if endpoints have any of the supported vendor's antimalware software (that is recognized by AnyConnect) installed and running in their devices.	Any_AM_Installation
Default_Antimalware_Policy_Win	Checks if endpoints have any of the supported vendor's antimalware software (that is recognized by AnyConnect) installed and running in their devices.	Any_AM_Installation_Win
Default_AppVis_Policy_Mac	Gathers information and reports all the applications that are installed on a given endpoint.	Default_AppVis_Requirement_Mac

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

Rule Name	Description	Requirements
Default_AppVis_Policy_Win	Gathers information and reports all the applications that are installed on a given endpoint.	Default_AppVis_Requirement_Win
Default_Firewall_Policy_Mac	Checks if endpoints have any of the supported vendor's Firewall program (that is recognized by AnyConnect) installed.	Default_Firewall_Requirement_Mac
Default_Firewall_Policy_Win	Checks if endpoints have any of the supported vendor's Firewall program (that is recognized by AnyConnect) installed.	Default_Firewall_Requirement_Win
Default_USB_Block_Win	Ensures that the endpoint device does not have any USB storage devices connected.	USB_Block

By checking for that information on the devices seeking network access, Cisco's ISE thereby " "formulate[s] an audit request, [and] send[s] th[at] audit request to the device [seeking network access.]"

Finally, and by way of another example—Easy Connect Enforcement Mode—Cisco describes how ISE, among other steps, "collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event." Thus, it "formulate[s] an audit request, [and] send[s] th[at] audit request to the device [seeking network access.]" ISE 3.0 Admin Guide at 580-82.

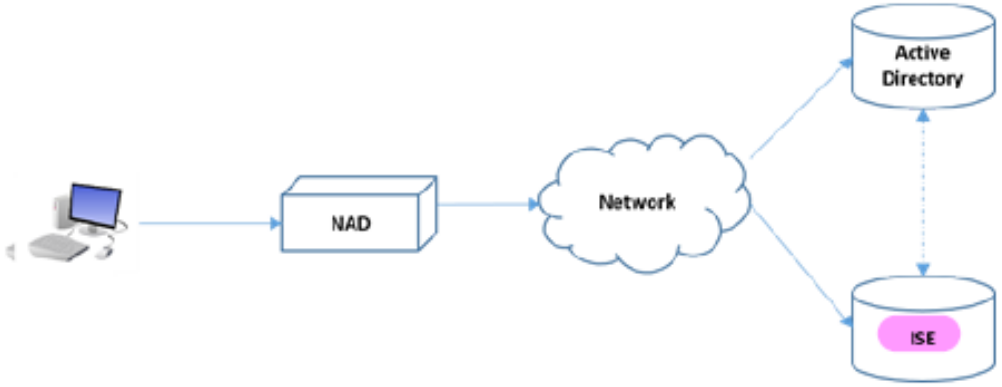
U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

Easy Connect Enforcement Mode Process Flow

The Easy Connect Enforcement mode process is as follows:

1. The user connects to the NAD from a wired endpoint (such as a PC for example).
2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD.
3. The user logs in to the domain and a security audit event is sent to Cisco ISE.
4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event.
5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy.

Figure 20: Easy Connect Enforcement Mode Basic Flow



51080352.4

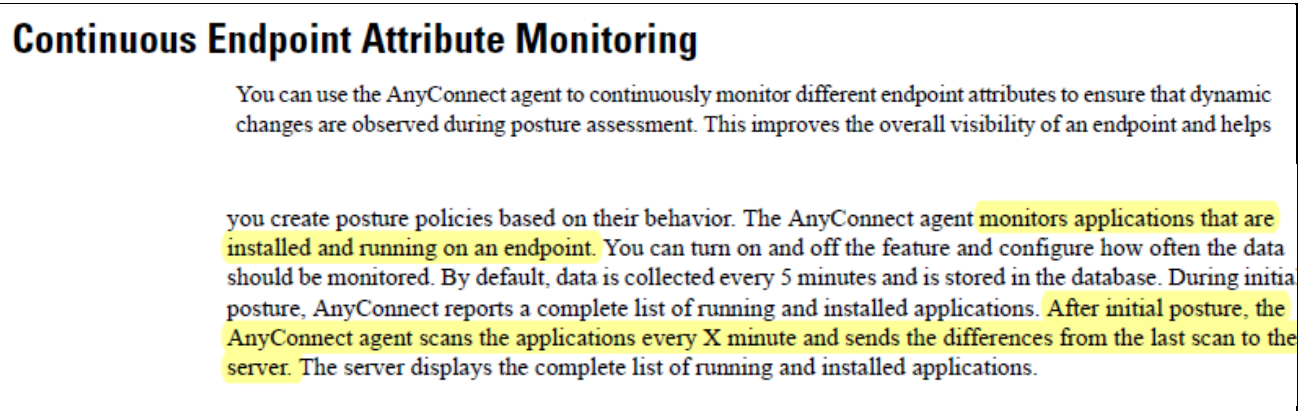
U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

[1-b-iii] evaluate device information received from the device in response to the audit request, and **[1-b-iv]** approve the device based on evaluation of the device information; and	Cisco's ISE "evaluate[s] device information received from the device in response to the audit request, and approve[s] the device based on evaluation of the device information[.]" Cisco explains how ISE "uses contextual data about network devices and endpoints" and thereby "evaluate[s] device information received from the device in response to the audit request[.]" ISE 3.0 Admin Guide at 2. Cisco goes on to explain that ISE "facilitate[s] network segmentation" and "enables secure network segmentation" and thereby "approves the device [seeking network access] based on evaluation of the device information[.]" *Id.* Similarly, Cisco's ISE "check[s] for compliance, also known as posture, of endpoints," and thereby "evaluate[s] device information received from the device in response to the audit request[.]" *Id.* It further explains that it "check[s] for compliance . . . of endpoints[] before allowing them to connect to your network[,]" and thereby "approve[s] the device based on evaluation of the device [.]" *Id.* • **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods. • **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation. • **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services. ISE 3.0 Admin Guide at 2.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	With respect to the "posture agents monitor and enforce Cisco ISE posture policies" described as to the preceding claim element, Cisco describes how the AnyConnect agent "monitor[s] and enforce[s] ISE posture policies that require interaction with the client." ISE 3.0 Admin Guide at 1010. Cisco further explains how "[d]uring initial posture, AnyConnect reports a complete list of running and installed applications" on the device seeking network connection (which Cisco terms an "endpoint"). ISE 3.0 Admin Guide at 1103. Thus, with this information regarding running and installed applications ("device information received from the device in response to an audit request"), ISE can then evaluate that information and "approve the device based on evaluation of the device information[.]" Moreover, Cisco describes a "Continuous Endpoint Attribute Monitoring" mode whereby "the AnyConnect agent scans the applications every X minute and sends the differences from the last scan to the server." These "differences from the last scan" also meet the claimed "device information received from the device in response to an audit request[.]" Thus, with this information, ISE can then evaluate that it and "approve the device based on evaluation of the device information[.]" **Posture Types** The following posture agents monitor and enforce Cisco ISE posture policies: • **AnyConnect**: Deploys the AnyConnect agent to monitor and enforce Cisco ISE posture policies that require interaction with the client. The AnyConnect agent stays on the client. For more information about using AnyConnect in Cisco ISE, see Cisco AnyConnect Secure Mobility, on page 1099. • **AnyConnect Stealth**: Runs posture as a service, with no user interface. The agent stays on the client. ISE 3.0 Admin Guide at 1010.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)



Continuous Endpoint Attribute Monitoring

You can use the AnyConnect agent to continuously monitor different endpoint attributes to ensure that dynamic changes are observed during posture assessment. This improves the overall visibility of an endpoint and helps you create posture policies based on their behavior. The AnyConnect agent monitors applications that are installed and running on an endpoint. You can turn on and off the feature and configure how often the data should be monitored. By default, data is collected every 5 minutes and is stored in the database. During initia posture, AnyConnect reports a complete list of running and installed applications. After initial posture, the AnyConnect agent scans the applications every X minute and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications.

ISE 3.0 Admin Guide at 1102-03.

By way of another example—Cisco Web Agent—it checks the posture on the device seeking network access (which Cisco terms a "client machine"). ISE 3.0 Admin Guide at 1103. Cisco checks the device for information such as "processes, applications and services" and then "sends a report back to the ISE server." This "report" comprises "device information received from the device in response to the audit request," which ISE can then "evaluate." Cisco further states that "[i]f requirements are met on the client machine, the user is allowed network access"—that is, ISE "approve[s] the device based on evaluation of the device information."

By way of another example—Agentless Posture—Cisco describes how it "provides posture information from clients[.]" ISE 3.0 Admin Guide at 1012. This posture information (i.e. "posture conditions") can include information such as "file conditions," "service conditions," "application conditions," and others.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

Agentless Posture

Agentless posture provides posture information from clients, and completely removes itself when finished, until invoked by Cisco ISE again. No action is required from the end user.

Requirements

- The client must be reachable by its IP address, and that IP address must be available in RADIUS accounting. IPv6 is not supported.
- Windows and Mac clients are currently supported.
  - For Windows clients, port 5985 to access Powershell on the client must be open. Powershell must be version 5.1 or later. The client must have cURL version 7.34 or later.
  - For macOS clients, port 22 to access SSH must be open to access the client. The client must have cURL version 7.34 or later.

. . .

Supported Posture Conditions

- File conditions, except the conditions that use the USER_DESKTOP and USER_PROFILE file paths
- Service conditions, except System Daemon and Daemon or User Agent checks on macOS
- Application conditions
- External Data Source conditions
- Compound conditions
- Anti-malware conditions
- Patch management condition, except the **Enabled** and **Up To Date** condition checks
- Firewall conditions
- Disk encryption conditions, except the encryption location-based condition check
- Registry conditions, except the conditions that use HCSK as root key

ISE 3.0 Admin Guide at 1012.

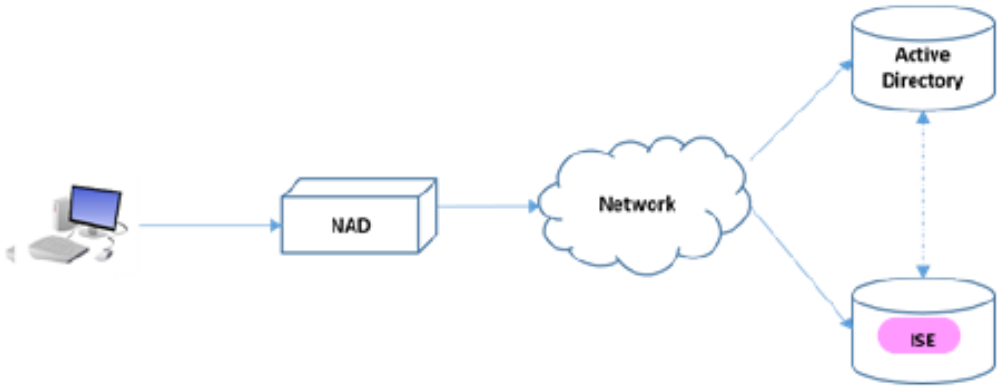
U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	Cisco further describes that in Agentless Posture mode, "Posture evaluation runs on the client, and sends the status to Cisco ISE." Any of this information, including the "status information," meets the "device information received from the device in response to the audit request," which ISE can then "evaluate." ISE then "approve[s] the device based on evaluation of the device information." **Agentless Posture Process Flow** 1. The client connects to the network. 2. Cisco ISE detects if agentless posture is enabled in the authorization profile used by client. 3. If so, Cisco ISE sends an agentless posture job request to the Cisco ISE Messaging queue. 4. Cisco ISE gets the job from the messaging queue, and starts the agentless posture flow. 5. Cisco ISE connects to the client via power shell or SSH. 6. Cisco ISE pushes the certificate, if it's not already in the client's trust certificate authority store. 7. Cisco ISE runs the client provisioning policy. 8. Cisco ISE pushes the agentless plug-in to the client and launches the plug-in. 9. Posture evaluation runs on the client, and sends the status to Cisco ISE. 10. Cisco ISE removes the agentless plug-in from the client. Logs of the posture flow remain on the client for 24 hours, or until the client deletes them. ISE 3.0 Admin Guide at 1012. Finally, with respect to the example of Easy Connect Enforcement Mode, Cisco describes how ISE, among other steps, "collects" information such as "the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event." ISE 3.0 Admin Guide at 580-82. "[A]ll data is collected and merged in the session directory[.]" *Id.* This information meets the "device information received from the device in response to the audit request[.]" Furthermore, Cisco ISE "issues a CoA to the

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	[network access device ("NAD")] (based on the appropriate policy managed in the policy service node)"—and thus "evaluates" this information. And finally, Cisco states, "the user ***is provided access by the NAD to the network*** based on that policy"—and thus ISE "approve[s] the device based on evaluation of the device information." **Easy Connect Enforcement Mode Process Flow** The Easy Connect Enforcement mode process is as follows: 1. The user connects to the NAD from a wired endpoint (such as a PC for example). 2. The NAD (which is configured for MAB) sends an access request to Cisco ISE. Cisco ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP, and AD. 3. The user logs in to the domain and a security audit event is sent to Cisco ISE. 4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event. 5. After all data is collected and merged in the session directory, Cisco ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node), and the user is provided access by the NAD to the network based on that policy.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	Figure 20: Easy Connect Enforcement Mode Basic Flow  ISE 3.0 Admin Guide at 580-81.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

[1-c] an extensible authentication protocol (EAP) server layer (SL) stored in memory and executable to:	Cisco's ISE contains "an extensible authentication protocol (EAP) server layer (SL) stored in memory[.]" Cisco describes how ISE uses several different EAP protocols, including Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), and Protected Extensible Authentication Protocol (PEAP). ISE 3.0 Admin Guide at 903. Cisco's ISE therefore contains "an extensible authentication protocol (EAP) server layer (SL) stored in memory." **Policy Set Protocol Settings** You must define global protocol settings in Cisco ISE before you can use these protocols to create, save and implement a policy set. You can use the Protocol Settings page to define global options for the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), and Protected Extensible Authentication Protocol (PEAP) protocols, which communicate with the other devices in your network. **Supported Network Access Policy Set Protocols** The following is a list of protocols that you can choose while defining your Network Access Policy Set policy: • Password Authentication Protocol (PAP) • Protected Extensible Authentication Protocol (PEAP) • Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2) • Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) • Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) • Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) • Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) • Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS) ISE 3.0 Admin Guide at 903.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

Cisco goes on to describe the guidelines for each of these EAP types. ISE 3.0 Admin Guide at 903-06 (EAP-FAST); 906-07 (EAP-TTLS); 907-08 (EAP-TLS); 908-09 (PEAP); 919-25 (allowed protocols in ISE include EAP-MD5, EAP-TLS, LEAP, PEAP, EAP-FAST, EAP-TTLS, Tunnel Extensible Authentication Protocol (TEAP).

Cisco also describes several RADIUS-based EAP protocols in ISE:

RADIUS-Based EAP Protocols

EAP provides an extensible framework that supports various authentication types. This section describes the EAP methods supported by Cisco ISE and contains the following topics:

Simple EAP Methods

- EAP-Message Digest 5
- Lightweight EAP

EAP Methods That Use Cisco ISE Server Certificate for Authentication

- PEAP/EAP-MS-CHAPv2
- PEAP/EAP-GTC
- EAP-FAST/EAP-MS-CHAPv2
- EAP-FAST/EAP-GTC

Apart from the methods listed above, there are EAP methods that use certificates for both server and client authentication.

ISE 3.0 Admin Guide at 934.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

RADIUS-Based EAP Authentication Flow

Whenever EAP is involved in the authentication process, the process is preceded by an EAP negotiation phase to determine which specific EAP method (and inner method, if applicable) should be used. EAP-based authentication occurs in the following process:

1. A host connects to a network device.
2. The network device sends an EAP Request to the host.
3. The host replies with an EAP Response to the network device.
4. The network device encapsulates the EAP Response that it received from the host into a RADIUS Access-Request (using the EAP-Message RADIUS attribute) and sends the RADIUS Access-Request to Cisco ISE.
5. Cisco ISE extracts the EAP Response from the RADIUS packet and creates a new EAP Request, encapsulates it into a RADIUS Access-Challenge (again, using the EAP-Message RADIUS attribute), and sends it to the network device.
6. The network device extracts the EAP Request and sends it to the host.

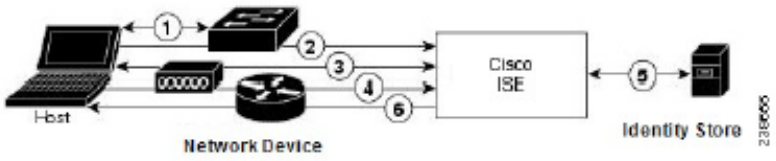
In this way, the host and Cisco ISE indirectly exchange EAP messages (transported over RADIUS and passed through the network device). The initial set of EAP messages that are exchanged in this manner negotiate the specific EAP method that will subsequently be used to perform the authentication.

The EAP messages that are subsequently exchanged are then used to carry the data that is needed to perform the actual authentication. If it is required by the specific EAP authentication method that is negotiated, Cisco ISE uses an identity store to validate user credentials.

After Cisco ISE determines whether the authentication should pass or fail, it sends either an EAP-Success or EAP-Failure message, encapsulated into a RADIUS Access-Accept or Access-Reject message to the network device (and ultimately also to the host).

ISE 3.0 Admin Guide at 934.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	The following figure shows a RADIUS-based authentication with EAP. *Figure 47: RADIUS-Based Authentication with EAP*  ISE 3.0 Admin Guide at 935; *see also id.* at 935-37 (EAP-MD5, LEAP, PEAP advantages and protocol flow, EAP-FAST benefits and protocol flow); 940-41 (EAP-FAST is used within Cisco's TrustSec architecture).
[1-c-i] receive the authentication information from the device using an EAP encryption protocol, and	Cisco's ISE "receive[s] the authentication information from the device using an EAP encryption protocol[.]" Cisco refers to this "authentication information [received] from the device as "attributes." It explains with respect to several specific EAP methods. By way of one example, with respect to EAP-FAST, Cisco explains how "ISE supports retrieval attributes and groups for both machine and user in EAP-FAST chaining only for AD. For LDAP and Internal DB ISE uses only the last identity attributes." These "attributes" comprise the "authentication information" received from the device. • When Cisco ISE is configured for chaining and AC for single mode then AC response with IdentityType TLV to ISE. However, the second identity authentication fails. You can see from this conversation that client is suitable to perform chaining but currently is configured for single mode. • Cisco ISE supports retrieval attributes and groups for both machine and user in EAP-FAST chaining only for AD. For LDAP and Internal DB ISE uses only the last identity attributes. ISE 3.0 Admin Guide at 904.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	By way of another example-EAP-TTLS—Cisco explains that "Phase 1 builds the secure tunnel and derives the session keys used in Phase 2 to securely tunnel ***attributes and inner method data*** between the server and the client. You can use the ***attributes*** tunneled during Phase 2 to perform additional authentications using a number of different mechanisms." **Using EAP-TTLS as Authentication Protocol** EAP-TTLS is a two-phase protocol that extends the functionality of EAP-TLS protocol. Phase 1 builds the secure tunnel and derives the session keys used in Phase 2 to securely tunnel attributes and inner method data between the server and the client. You can use the attributes tunneled during Phase 2 to perform additional authentications using a number of different mechanisms. ISE 3.0 Admin Guide at 906. In another example, Cisco's explains how in ISE's RADIUS-based EAP authentication, "The EAP messages that are subsequently exchanged are then ***used to carry the data that is needed to perform the actual authentication***." Thus, ISE "receive[s] the authentication information from the device using an EAP encryption protocol[.]" In this way, the host and Cisco ISE indirectly exchange EAP messages (transported over RADIUS and passed through the network device). The initial set of EAP messages that are exchanged in this manner negotiate the specific EAP method that will subsequently be used to perform the authentication. The EAP messages that are subsequently exchanged are then used to carry the data that is needed to perform the actual authentication. If it is required by the specific EAP authentication method that is negotiated, Cisco ISE uses an identity store to validate user credentials. After Cisco ISE determines whether the authentication should pass or fail, it sends either an EAP-Success or EAP-Failure message, encapsulated into a RADIUS Access-Accept or Access-Reject message to the network device (and ultimately also to the host). ISE 3.0 Admin Guide at 934.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

[1-c-ii] configure an access point in response to approval of the device by the gatekeeper.	Cisco's ISE comprises "an extensible authentication protocol (EAP) server layer (SL) stored in memory and executable to: . . . configure an access point in response to approval of the device by the gatekeeper." Generally, Cisco describes how ISE "uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access[.]" ISE 3.0 Admin Guide at 2. A list "access points"—including switches, routers, and remote access devices (i.e. firewalls)— is disclosed in InfoExpress's Disclosure of Asserted Claims and Infringement Contentions per Patent L.R. 3-1 and 3-2 at Section II.B ("Accused Technology"). These hardware products are listed in Cisco's Identity Services Engine Network Component Compatibility documents, for Releases 2.0, 2.2, 2.4, 2.6, 2.7, 3.0, 3.1, 3.2, and 3.3, which have been produced as INFOEX-CSCO_0014309 to INFOEX-CSCO_0014605. These Cisco documents describe "Cisco Identity Services Engine (ISE) validated compatibility with switches, wireless LAN controllers, and other policy enforcement devices as well as operating systems with which Cisco ISE interoperates." INFOEX-CSCO_0014586 at 14586 They further state, with respect to "Validated Network Access Devices," that "Cisco ISE supports interoperability with any Cisco or non-Cisco RADIUS client network access device (NAD) that implements common RADIUS behavior (similar to Cisco IOS 12.x) for ***standards-based authentication***." INFOEX-CSCO_0014586 at 14587. By way of one example—RADIUS-based EAP—Cisco states that "After Cisco ISE determines whether the authentication should pass or fail, it sends either an ***EAP-Success or*** EAP-Failure ***message***, encapsulated into a ***RADIUS Access-Accept*** or Access-Reject message to the network device (and ***ultimately also to the host***)." Thus, ISE's EAP-Success and RADIUS Access-Accept messages are sent in respons to approval of the device by the gatekeeper. Furthermore, Cisco states that these EAP-Success and RADIUS Access-Accept are sent to the host (that is, the "access point"). And finally, these messages "configure" that access point.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	In this way, the host and Cisco ISE indirectly exchange EAP messages (transported over RADIUS and passed through the network device). The initial set of EAP messages that are exchanged in this manner negotiate the specific EAP method that will subsequently be used to perform the authentication. The EAP messages that are subsequently exchanged are then used to carry the data that is needed to perform the actual authentication. If it is required by the specific EAP authentication method that is negotiated, Cisco ISE uses an identity store to validate user credentials. After Cisco ISE determines whether the authentication should pass or fail, it sends either an EAP-Success or EAP-Failure message, encapsulated into a RADIUS Access-Accept or Access-Reject message to the network device (and ultimately also to the host). ISE 3.0 Admin Guide at 934. By way of another example—that involving both Cisco and third-party (that is, non-Cisco) access points, Cisco states that once a device (which Cisco terms "a guest endpoint user") logs in for authentication (for example, by an EAP), "11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the [change of authorization ("CoA")], authorizes the endpoint, and bypasses the sink hole." Then, at step 12, "The guest user ***receives the appropriate access based on the CoA***[.]" Thus, in this case, the change of authorization ("CoA") "configures" the access point.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

Admin Guide at 804-06.

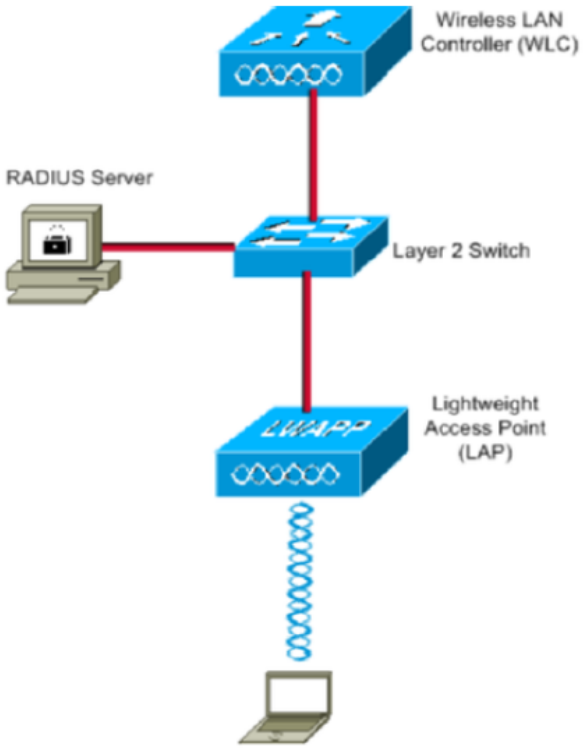
In another example, Cisco's ISE can perform dynamic VLAN assignment with a RADIUS server. Cisco describes how its Wireless LAN controllers (WLCs) use 802.1x with PEAP as the security mechanism. Cisco, Configure Dynamic VLAN Assignment with ISE and Catalyst 9800 Wireless LAN Controller at 3, 25 (June 2022), https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/217043-configure-dynamic-vlan-assignment-with-c.pdf (last visited May

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	22, 2023). Thus, ISE comprises "an extensible authentication protocol (EAP) server layer (SL) stored in memory[.]"

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

This document uses this network setup:



These are the configuration details of the components used in this diagram:

- The IP address of Cisco ISE (RADIUS) server is 10.10.1.24.
- The Management Interface address of the WLC is 10.10.1.17.
- The internal DHCP server on the controller is used to assign the IP address to wireless clients.
- This document uses 802.1x with PEAP as the security mechanism.

Configure Dynamic VLAN Assignment at 3.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

```
       [64]     6  VLAN                    [13]
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Tunnel-Medium-Type
[65]     6  ALL_802                 [6]
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  EAP-Message
[79]     6  ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Message-
Authenticator[80]    18  ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Tunnel-Private-
Group-Id[81]     6  "102"
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  EAP-Key-Name
 [102]    67  *
2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:   MS-MPPE-Send-Key
[16]     52  *
2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:   MS-MPPE-Recv-Key
[17]     52  *
2021/03/21 22:22:45.238 {wncd_x_R0-0}{1}: [eap-auth] [25253]: (info): SUCCESS for EAP method
name: PEAP on handle 0x0C000008
```

Configure Dynamic VLAN Assignment at 25.

Furthermore, Cisco explains how ISE uses ***dynamic VLAN assignment*** to "place a wireless user into a specific VLAN based on the credentials supplied by the user."

> Dynamic VLAN assignment is one such feature that places a wireless user into a specific VLAN based on the credentials supplied by the user. The task to assign users to a specific VLAN is handled by a RADIUS authentication server, such as Cisco ISE. This can be used, for example, to allow the wireless host to remain on the same VLAN as it moves within a campus network.
>
> Therefore, when a client attempts to associate to a LAP registered with a controller, the WLC passes the credentials of the user to the RADIUS server for validation. Once the authentication is successful, the RADIUS server passes certain Internet Engineering Task Force (IETF) attributes to the user. These RADIUS attributes decide the VLAN ID that must be assigned to the wireless client. The SSID of the client does not matter because the user is always assigned to this predetermined VLAN ID.

Configure Dynamic VLAN Assignment at 25.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	ISE does this VLAN assignment "once the authentication is successful," and performs it on the switches in the system (that is, the claimed "access points"). *E.g., id.* at 25, 8 ("Configure the Switch for Multiple VLANs"). Therefore, ISE comprises "an extensible authentication protocol (EAP) server layer (SL) stored in memory and executable to: . . . configure an access point in response to approval of the device by the gatekeeper." *See also* Change of Authorization with RADIUS (CoA) on MR Access Points, https://documentation.meraki.com/MR/Encryption_and_Authentication/Change_of_Authorization_with_RADIUS_(CoA)_on_MR_Access_Points (last visited May 31, 2023) ("RADIUS CoA (Change of Authorization) is a feature that allows a RADIUS server to adjust an active client session.") (further describing EAP). In addition to making, using, offering for sale, and selling the ISE, Cisco also induces third-parties to infringe this claim as set forth in InfoExpress's 3-1 disclosures under 35 USC 271(b). For this claim, the underlying direct infringement is caused by the third-parties including Cisco's customers, subscribers, users and developers. And Cisco's acts of induced infringement including the following: as set forth herein, the Release Notes, Admin Guide, Randomized and Changing MAC Deployment Guide and Data Sheets for the ISE are all provided by Cisco to third-parties which provide deliberate and specific instruction and guidance for third-parties to use the ISE in a manner infringed by this claim. In addition, Cisco's Identity Services Engine Administrator Guide ("ISE AG) explains also provide such specific guidance of infringement to third-parties explaining that "[a]dministrators can use the admin portal to: Manage deployments, help desk operations, and network devices, and node monitoring and troubleshooting; Manage Cisco ISE services, policies, administrator accounts, and system configuration and operations." https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/admin_guide/b_ise_admin_3_3/b_ISE_admin_33_overview.html

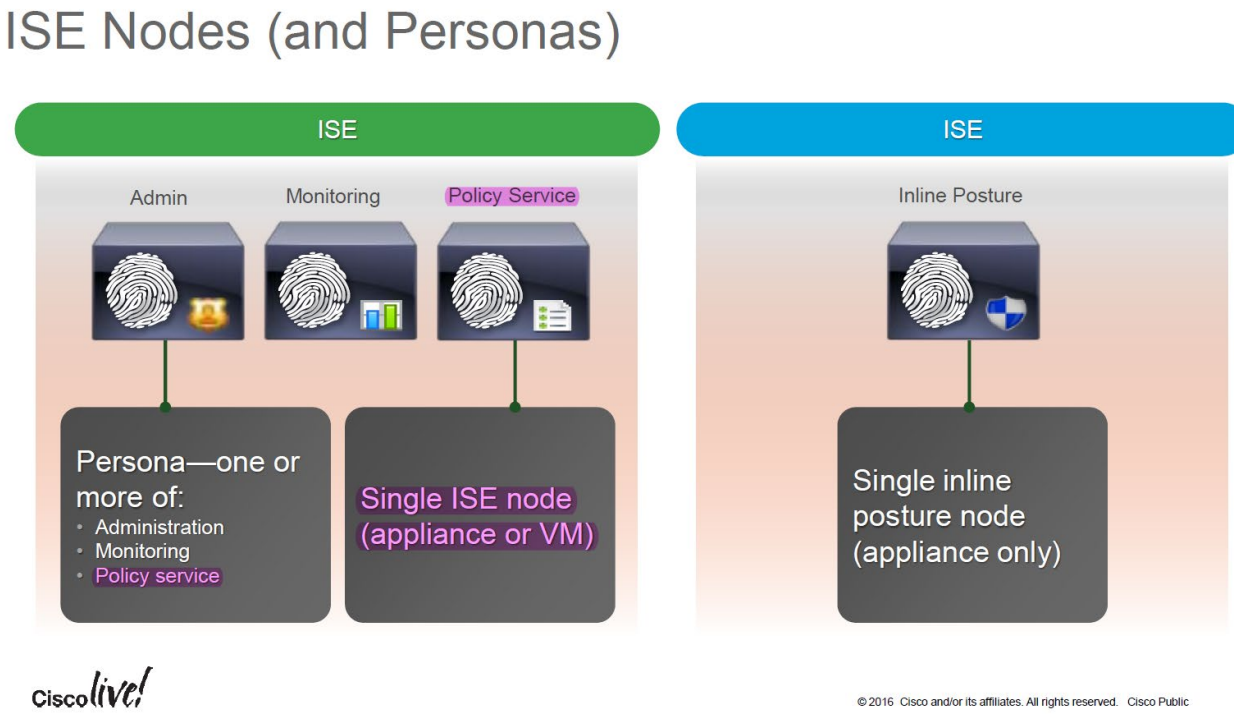
U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	For example, the Admin Guide explains that its audience can be third party administrators ("Cisco ISE administrators can perform various administrative tasks based on the administrative group to which they belong. These administrators are critical. Grant administrative access only to users who are authorized to administer Cisco ISE in your network" ISE 3.0 Admin Guide at 13); developers ("On Facebook, create a Facebook application: a) Log on to http://developers.facebook.com and sign up as a developer," ISE 3.0 Admin Guide at. 397), and it instructs these third-parties on configuring the ISE, for example, with respect to the claimed authentication, compliance, and access point reconfiguration. With respect to this claim, the Admin Guide instructs third-parties how to "Create a Certificate Authentication Profile for TLS-Based Authentication." ISE 3.0 Admin Guide at 269-270. In particular, Cisco instructs these third-parties how to "use certificates for authenticating endpoints that connect to your network" and "defin[ing] a certificate authentication profile in Cisco ISE…" *Id.* In another example, the Cisco's Admin guide instructs third-parties how to apply and/or configure security policies. For example, Cisco explains that the third-parties can "globally configure the Admin portal for posture services." ISE 3.0 Admin Guide at 1015. There, Cisco's Admin guide instructs third-parties how to "download updates automatically to the Cisco ISE through the web from Cisco. *Id.* Further, Cisco explains the various steps for how to "create a posture requirement." Id.. at. 1015-17; *see also id.* at 1066 (Cisco instructing third-parties on "Create[ing] Client Posture Requirements"); *id* at 1067 ("Posture Reassessment Configuration Settings"); *id.* at 1023 ("You can use the Posture Update window to download updates dynamically from the web."); *id.* at 1072 ("Creat[ing] a Posture Condition", "Creat[ing] Posture Remediation."); *id.* at 1073 ("Create Posture Policy"). The ISE AG provides third-parties with an "Administration Portal" which provides third-parties "Policy windows include[ing] tools for managing network security in the areas of authentication, authorization, profiling, posture, and client provisioning."

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

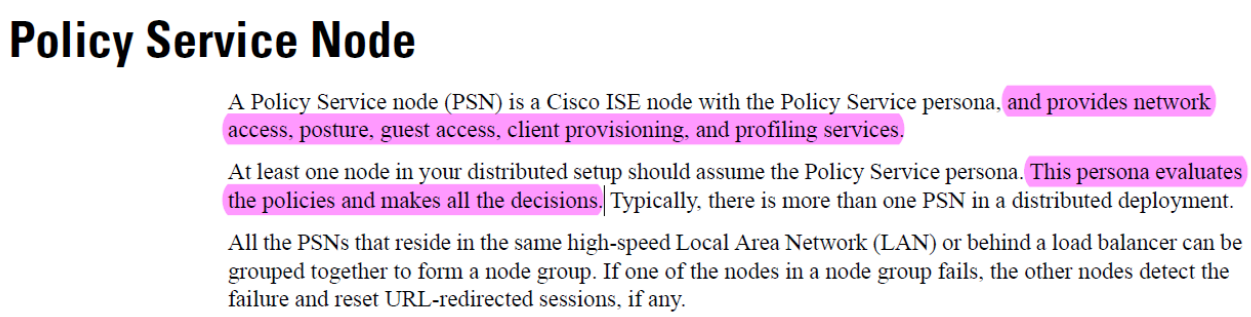
	https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/admin_guide/b_ise_admin_3_3/b_ISE_admin_33_basic_setup.html#reference_D93EF6652C8D4EB8B56EC6B857DA6F9A. Further, the ISE AG permits third-parties to create "Posture conditions" by following the following field path at the Administration Portal: "Policy -> Policy Elements -> Conditions -> Posture windows." Id. In another example, Cisco's Admin guide instructs third-parties with respect to "Quarantine [for] a Vulnerable Endpoint." ISE 3.0 Admin Guide at 1127. Specifically, Cisco explains that "You can choose to quarantine the endpoint, provide limited access (redirect to a different portal), or reject the request" and then provides three steps for doing so. *Id*.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

2. The network access control system of claim 1, wherein the gatekeeper is hosted at the same computing device as the EAPM, ESL, and SF.	Cisco ISE comprises and includes ""[t]he network access control system of claim 1, wherein the gatekeeper is hosted at the same computing device as the EAPM, ESL, and SF." Cisco describes deployments of its ISE NAC systems as having different ***personae***, including one for ***policy service***. Thus is hosted at a single ISE node (termed a ***policy service node*** or "PSN"). 

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

Cisco, Demystifying Cisco Identity Services Engine (ISE) Architecture and Enterprise Security (July 2016) ("Demystifying ISE") at 14, *available at* https://www.ciscolive.com/c/dam/r/ciscolive/global/docs/2016/CP-1014.pdf (last visited October 1, 2023); *see also* ISE 3.0 Admin Guide at 137 ("A Policy Service node (PSN) . . . provides network access, posture, guest access, client provisioning, and profiling services. At least one node in your distributed setup should assume the Policy Service persona. This persona ***evaluates the policies and makes all the decisions***."



Policy Service Node

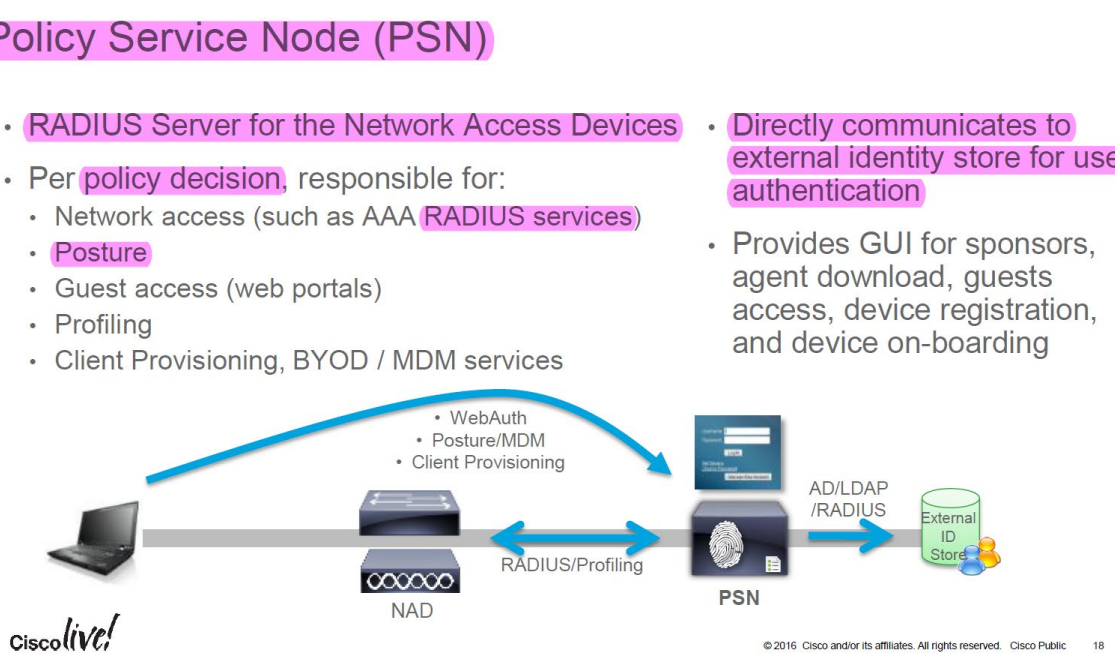
A Policy Service node (PSN) is a Cisco ISE node with the Policy Service persona, and provides network access, posture, guest access, client provisioning, and profiling services.

At least one node in your distributed setup should assume the Policy Service persona. This persona evaluates the policies and makes all the decisions. Typically, there is more than one PSN in a distributed deployment.

All the PSNs that reside in the same high-speed Local Area Network (LAN) or behind a load balancer can be grouped together to form a node group. If one of the nodes in a node group fails, the other nodes detect the failure and reset URL-redirected sessions, if any.

ISE 3.0 Admin Guide at 137.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)



Demystifying ISE at 18.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	Cisco ISE's PSN: • Assesses posture (Demystifying ISE at 18; ISE 3.0 Admin Guide at 137), and thereby contains the gatekeeper. • Has a mechanism for relaying responses for audit (posture) information to the gatekeeper, and for relaying authentication information to the EAPM. It thus contains a mechanism for "filtering" information to its proper destination—and thus it contains a server filter (SF).; • "Directly communicates to external identity store for user authentication provides GUI" and is "responsible for . . . RADIUS services" (Demystifying ISE at 18), and thereby contains an EAP Module (EAPM).; and • Is "responsible for . . . RADIUS services" (Demystifying ISE at 18), and thereby contains an EAP Server Layer (ESL). Moreover, Demystifying ISE shows the gatekeeper, EAPM, ESL, and SF all located at the same network component—the PSN node in the figure). Thus, in Cisco ISE "the gatekeeper is hosted at the same computing device as the EAPM, ESL, and SF." *See also* ISE 3.2 Administrator Guide at 1149 ("ISE 3.2 Admin Guide"), avialable at https://www.cisco.com/c/en/us/td/docs/security/ise/3-2/admin_guide/b_ise_admin_3_2.html (last visited October 2, 2023) (describing EAP-TLS and PEAP authentication protocols in conjunction with a posture agent.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	Given below are the steps you perform to provision an endpoint without redirection for different networks. Dot1X EAP-TLS 1. Connect the Cisco ISE network with provisioned certification. 2. Open a browser window and type in the provisioning URL: provisioning.cisco.com. 3. Log into the CP portal via internal user, AD, LDAP, or SAML. Agent performs posture. The endpoint moves to the right network based on posture compliance. Dot1X PEAP 1. Connect the Cisco ISE network with User Name and Password through NSP 2. Open a browser window and type in the provisioning URL: provisioning.cisco.com. 3. Log into the CP portal via internal user, AD, LDAP, or SAML Agent performs posture. The endpoint moves to the right network based on posture compliance. ISE 3.2 Admin Guide at 1149.

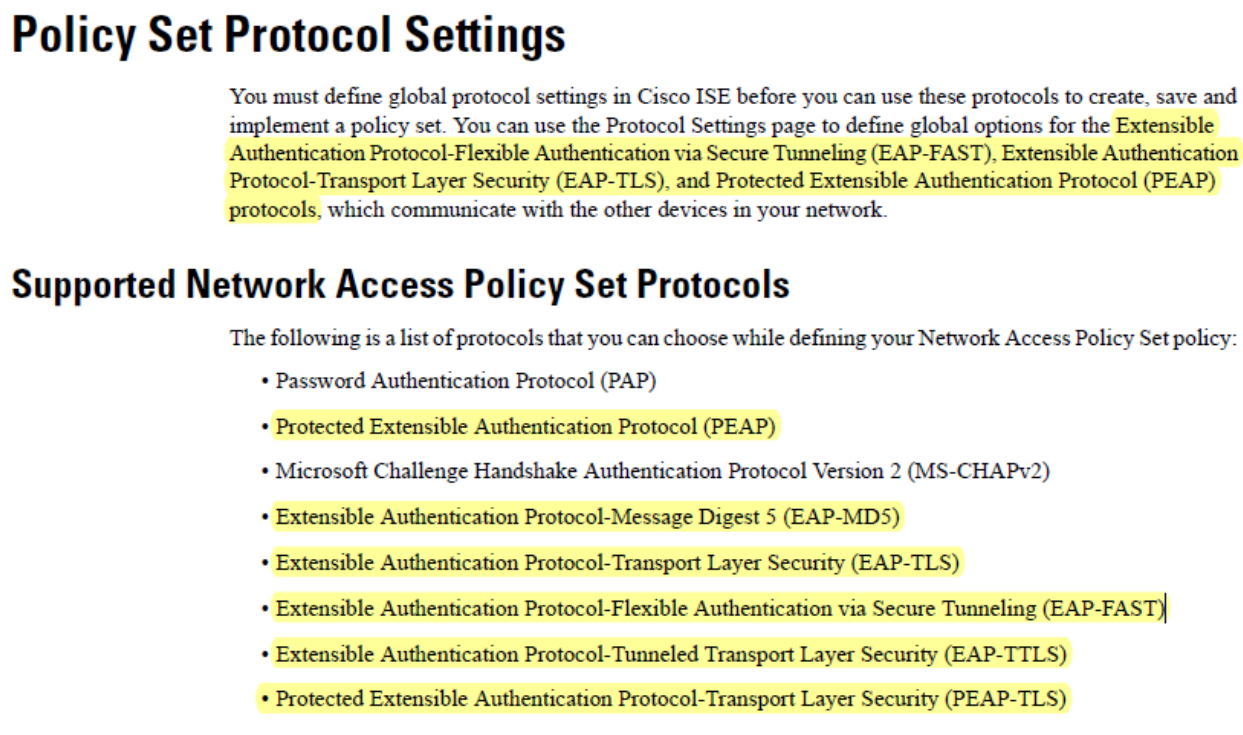
U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

5. The network access control system of claim 1, wherein the SF is part of the ESL.	Cisco ISE comprises and includes "[t]he network access control system of claim 1, wherein the SF is part of the ESL." As demonstrated above with respect to claim 2, in ISE the "gatekeeper is hosted at the same computing device as the EAPM, ESL, and SF. Also as explained above, ISE contains a server filter (SF) for filtering posture information and authentication from one another, and sending those types of information respectively to the gatekeeper and EAP module (EAPM). Additionally, the EAP server layer is the component of the RADIUS server that receives the EAP packet. Thus, it must contain as a part of it some apparatus for filtering packets to their proper destinations—and thus in ISE, "the SF is part of the ESL."

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

6. The network access control system of claim 1, wherein the EAPM includes a plurality of authentication modules configured to perform different authentication operations.	Cisco's Identity Services Engine ("ISE") comprises "[t]he network access control system of claim 1, wherein the EAPM includes a plurality of authentication modules configured to perform different authentication operations." Cisco describes how ISE contains several different EAP protocols, and thus "includes a plurality of [EAP] authentication modules configured to perform different authentication operations." These EAP protocols include Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), and Protected Extensible Authentication Protocol (PEAP). ISE 3.0 Admin Guide at 903. Cisco's ISE therefore contains "an extensible authentication protocol (EAP) server layer (SL) stored in memory."

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)



Policy Set Protocol Settings

You must define global protocol settings in Cisco ISE before you can use these protocols to create, save and implement a policy set. You can use the Protocol Settings page to define global options for the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), and Protected Extensible Authentication Protocol (PEAP) protocols, which communicate with the other devices in your network.

Supported Network Access Policy Set Protocols

The following is a list of protocols that you can choose while defining your Network Access Policy Set policy:

- Password Authentication Protocol (PAP)
- Protected Extensible Authentication Protocol (PEAP)
- Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2)
- Extensible Authentication Protocol-Message Digest 5 (EAP-MD5)
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)
- Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS)
- Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)

ISE 3.0 Admin Guide at 903.

Cisco goes on to describe the guidelines for each of these EAP types. ISE 3.0 Admin Guide at 903-06 (EAP-FAST); 906-07 (EAP-TTLS); 907-08 (EAP-TLS); 908-09 (PEAP); 919-25 (allowed protocols in ISE include EAP-MD5, EAP-TLS, LEAP, PEAP, EAP-FAST, EAP-TTLS, Tunnel Extensible Authentication Protocol (TEAP).

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

	Cisco also describes several RADIUS-based EAP protocols in ISE: **RADIUS-Based EAP Protocols** EAP provides an extensible framework that supports various authentication types. This section describes the EAP methods supported by Cisco ISE and contains the following topics: **Simple EAP Methods** • EAP-Message Digest 5 • Lightweight EAP **EAP Methods That Use Cisco ISE Server Certificate for Authentication** • PEAP/EAP-MS-CHAPv2 • PEAP/EAP-GTC • EAP-FAST/EAP-MS-CHAPv2 • EAP-FAST/EAP-GTC Apart from the methods listed above, there are EAP methods that use certificates for both server and client authentication. ISE 3.0 Admin Guide at 934.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

RADIUS-Based EAP Authentication Flow

Whenever EAP is involved in the authentication process, the process is preceded by an EAP negotiation phase to determine which specific EAP method (and inner method, if applicable) should be used. EAP-based authentication occurs in the following process:

1. A host connects to a network device.
2. The network device sends an EAP Request to the host.
3. The host replies with an EAP Response to the network device.
4. The network device encapsulates the EAP Response that it received from the host into a RADIUS Access-Request (using the EAP-Message RADIUS attribute) and sends the RADIUS Access-Request to Cisco ISE.
5. Cisco ISE extracts the EAP Response from the RADIUS packet and creates a new EAP Request, encapsulates it into a RADIUS Access-Challenge (again, using the EAP-Message RADIUS attribute), and sends it to the network device.
6. The network device extracts the EAP Request and sends it to the host.

In this way, the host and Cisco ISE indirectly exchange EAP messages (transported over RADIUS and passed through the network device). The initial set of EAP messages that are exchanged in this manner negotiate the specific EAP method that will subsequently be used to perform the authentication.

The EAP messages that are subsequently exchanged are then used to carry the data that is needed to perform the actual authentication. If it is required by the specific EAP authentication method that is negotiated, Cisco ISE uses an identity store to validate user credentials.

After Cisco ISE determines whether the authentication should pass or fail, it sends either an EAP-Success or EAP-Failure message, encapsulated into a RADIUS Access-Accept or Access-Reject message to the network device (and ultimately also to the host).

ISE 3.0 Admin Guide at 934.

U.S. Patent No. 8,117,645 (Cisco's Identity Services Engine)

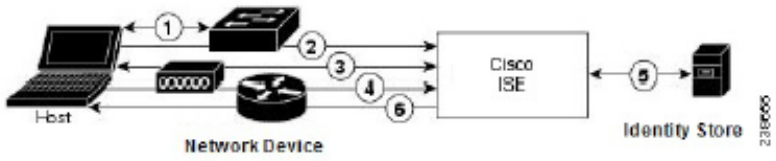
	The following figure shows a RADIUS-based authentication with EAP. *Figure 47: RADIUS-Based Authentication with EAP*  ISE 3.0 Admin Guide at 935; *see also id.* at 935-37 (EAP-MD5, LEAP, PEAP advantages and protocol flow, EAP-FAST benefits and protocol flow); 940-41 (EAP-FAST is used within Cisco's TrustSec architecture).

EXHIBIT W

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC. and FORTINET, INC.,
Petitioners,

v.

INFOEXPRESS INC.,
Patent Owner.

IPR2024-00675
U.S. Patent No. 7,523,484

PATENT OWNER PRELIMINARY RESPONSE

TABLE OF CONTENTS

PAGE

I. Introduction....1

II. The '484 Patent....1

A. Date of Invention....1
B. Person of Ordinary Skill in the Art (POSITA)....1
C. Overview of the '484 Patent....1

III. Claim Construction....5

A. "Access Control Configured To Reconfigure The Communication Device … If The Audit Results In A Determination That The Access Device Meets The Requitements Of The At Least One Security Policy"....5

IV. Petitioners' References....11

A. Krantz....12
B. Herrmann....14

V. Krantz Alone (Ground 1) or the Combination of Krantz and Herrmann (Ground 2) Fail to Render Obvious Any of the Challenged Claims....16

A. Ground 1: Krantz Is Missing Claimed Limitations....16

1. Krantz Does Not Disclose "An Access Control Configured To Reconfigure The Communication Device Such That Data Sent From The Access Device Is Received By The Less-Restricted Subset Of The Protected Network … If The Audit Results In A Determination That The Access Device Meets The Requirements Of The At Least One Security Policy"....17
2. Krantz Fails To Disclose "A Policy Auditor Configured To Audit The Access Device Using The At Least One Security Policy"....22

B. Ground 2: Krantz in Combination with Herrmann Fails To Render Obvious The Challenged Claims....27

VI. All Grounds: Neither Reference Constitutes Prior Art 30

A. Legal Standard.....31
B. The Inventors Conceived of the Claimed Inventions Prior to the Critical Dates of Both Krantz and Herrmann.....32
C. The Inventors Exercised Reasonably Continuous Diligence Up and Through Constructive Reduction to Practice. 34
D. The Inventors Exercised Achieved a Constructive Reduction to Practice by the Filing of U.S. Provisional Patent Application Serial No. 60/513,080, Which Was Filed on October 21, 2003 43

VII. Conclusion 44

TABLE OF AUTHORITIES

FEDERAL CASES

ATI Techs. v. Iancu, 920 F.3d 1362 (Fed. Cir. 2019) 31, 35, 43

Bey v. Kollonitsch, 806 F.2d 1024 (Fed. Cir. 1986) 32

Monsanto Co. v. Mycogen Plant Sci., Inc., 261 F.3d 1356 (Fed. Cir. 2001) 31, 35

Globus Med., Inc. v. Depuy Synthes Prods., LLC, No. IPR2015-00107 (P.T.A.B. May 1, 2015) 33

LG Elecs., Inc. v. Wi-LAN Inc., No. IPR2018-00704, Paper No. 14 (P.T.A.B. Sept. 5, 2018) 30, 31

Perfect Surgical Techniques, Inc. v. Olympus Am., Inc., 841 F.3d 1004 (Fed. Cir. 2016) 31, 32

Polaris Indus., Inc. v. Arctic Cat, Inc., 882 F.3d 1056 (Fed. Cir. 2018) 30

SAS Institute Inc. v. Iancu, 138 S.Ct. 1348 (2018) 33

Sequenom v. Leland Stanford Junior Univ., No. IPR2013-00390 (P.T.A.B. Nov. 25, 2014) 31

Tyco Healthcare Grp. v. Ethicon Endo-Surgery, Inc., 774 F.3d 968 (Fed. Cir. 2014) 31

FEDERAL STATUTES

35 U.S.C. § 102(e) 31, 32

35 U.S.C. §§ 119(e) & 112, ¶ 1 43

STATE STATUTES

ECL 39

EXHIBIT LIST

Exhibit Number	Description
2001	Declaration of Dr. Eric Cole
2002	Curriculum Vitae of Dr. Eric Cole
2003	Declaration of Stacey C. Lum
2004	Diligence Calendar
2005	U.S. Provisional App. No. 60/505,582
2006	U.S. Provisional App. No. 60/513,080
2007	Declaration of Hugh Smith, Ph.D.
2008	Curriculum Vitae of Hugh Smith, Ph.D.
2009	Conception of the '484 Patent
2010	Constructive Reduction to Practice of the '484 Patent
2011	LAN Based Policy Enforcement Engineering Specification
2012	Metadata for Exhibit 2011
2013	CyberGatekeeper Policy Manager
2014	Metadata for Exhibit 2013
2015	Internal InfoExpress Correspondence
2016	Internal InfoExpress Correspondence
2017	Internal InfoExpress Correspondence
2018	Internal InfoExpress Correspondence
2019	Internal InfoExpress Correspondence
2020	Internal InfoExpress Correspondence
2021	Internal InfoExpress Correspondence
2022	Correspondence with Globe Tech
2023	Email attachment to Exhibit 2022
2024	Internal InfoExpress Correspondence
2025	Correspondence with Meetinghouse
2026	Draft Meetinghouse Agreement
2027	Internal InfoExpress Correspondence
2028	Draft Meetinghouse Agreement
2029	Internal InfoExpress Correspondence
2030	Draft Meetinghouse Agreement
2031	Draft Meetinghouse Agreement
2032	Internal InfoExpress Correspondence
2033	Draft Meetinghouse Agreement
2034	Draft Meetinghouse Agreement
2035	Draft Meetinghouse Agreement

Exhibit Number	Description
2036	Internal InfoExpress Correspondence
2037	Draft Meetinghouse Agreement
2038	Draft Meetinghouse Agreement
2039	Internal InfoExpress Correspondence
2040	Draft Meetinghouse Agreement
2041	Draft Meetinghouse Agreement
2042	Draft Meetinghouse Agreement
2043	Draft Meetinghouse Agreement
2044	Internal InfoExpress Correspondence
2045	Draft Meetinghouse Agreement
2046	Draft Meetinghouse Agreement
2047	Internal InfoExpress Correspondence
2048	Correspondence with Globe Tech
2049	Correspondence with Globe Tech
2050	Internal InfoExpress Correspondence
2051	Correspondence with Globe Tech
2052	Correspondence with Globe Tech
2053	Correspondence with Globe Tech
2054	Correspondence with Globe Tech
2055	Correspondence with Globe Tech
2056	Draft Globe Tech Agreement
2057	Draft Globe Tech Agreement
2058	Draft Globe Tech Agreement
2059	Draft Globe Tech Agreement
2060	Draft Globe Tech Agreement
2061	Draft Globe Tech Agreement
2062	Draft Globe Tech Agreement
2063	Correspondence with Globe Tech
2064	Draft Globe Tech Agreement
2065	Correspondence with Globe Tech
2066	Network Device Configuration API Engineering Specification
2067	Correspondence with Globe Tech
2068	Correspondence with Globe Tech
2069	Network Device Configuration API Engineering Specification
2070	Network Device Configuration API Engineering Specification
2071	Correspondence with Globe Tech
2072	Network Device Configuration API Engineering Specification

Exhibit Number	Description
2073	Network Device Configuration API Engineering Specification
2074	Correspondence with Globe Tech
2075	Correspondence with Globe Tech
2076	Correspondence with Globe Tech
2077	Correspondence with Globe Tech
2078	Correspondence with Globe Tech
2079	Email attachment to Exhibit 2078
2080	Correspondence with Globe Tech
2081	Correspondence with Globe Tech
2082	Correspondence with Globe Tech
2083	Correspondence with Globe Tech
2084	Correspondence with Globe Tech
2085	Correspondence with Globe Tech
2086	Correspondence with Globe Tech
2087	Correspondence with Globe Tech
2088	Correspondence with Globe Tech
2089	Correspondence with Globe Tech
2090	Correspondence with Globe Tech
2091	Correspondence with Globe Tech
2092	Correspondence with Globe Tech
2093	Correspondence with Globe Tech
2094	Correspondence with Globe Tech
2095	Correspondence with Globe Tech
2096	Correspondence with Globe Tech
2097	Correspondence with Globe Tech
2098	Correspondence with Globe Tech
2099	Correspondence with Globe Tech
2100	Correspondence with Globe Tech
2101	Correspondence with Globe Tech
2102	Correspondence with Globe Tech
2103	Correspondence with Globe Tech
2104	Correspondence with Globe Tech
2105	Correspondence with Globe Tech
2106	Correspondence with Globe Tech
2107	Correspondence with Globe Tech
2108	Internal InfoExpress Correspondence
2109	Correspondence with Globe Tech

Exhibit Number	Description
2110	Correspondence with Globe Tech
2111	Correspondence with Globe Tech
2112	Correspondence with Globe Tech
2113	Internal InfoExpress Correspondence
2114	Correspondence with Globe Tech
2115	Email attachment to Exhibit 2114
2116	Correspondence with Globe Tech
2117	Internal InfoExpress Correspondence
2118	Correspondence with Globe Tech
2119	Correspondence with Globe Tech
2120	Correspondence with Globe Tech
2121	Correspondence with Globe Tech
2122	Correspondence with Globe Tech
2123	Correspondence with J. Ong
2124	Correspondence with Globe Tech
2125	Correspondence with Globe Tech
2126	Correspondence with Globe Tech
2127	Correspondence with Globe Tech
2128	Correspondence with Globe Tech
2129	Correspondence with Globe Tech
2130	Correspondence with Globe Tech
2131	Correspondence with Globe Tech
2132	Correspondence with Globe Tech
2133	Correspondence with Globe Tech
2134	Correspondence with Globe Tech
2135	Correspondence with Globe Tech
2136	Correspondence with Globe Tech
2137	Correspondence with Globe Tech
2138	Correspondence with Globe Tech
2139	Correspondence with Globe Tech
2140	Correspondence with Globe Tech
2141	Correspondence with Globe Tech
2142	Correspondence with Globe Tech
2143	Correspondence with Globe Tech
2144	Correspondence with Globe Tech
2145	Correspondence with Globe Tech
2146	Correspondence with Globe Tech

Exhibit Number	Description
2147	Correspondence with Globe Tech
2148	Correspondence with J. Ong
2149	Correspondence with Globe Tech
2150	Correspondence with J. Ong
2151	Correspondence with Globe Tech
2152	Correspondence with J. Ong
2153	Correspondence with Globe Tech
2154	Correspondence with Globe Tech
2155	Correspondence with Globe Tech
2156	Correspondence with Globe Tech
2157	Correspondence with Globe Tech
2158	Correspondence with Globe Tech
2159	Correspondence with Globe Tech
2160	Correspondence with Globe Tech
2161	Correspondence with J. Ong
2162	Correspondence with Globe Tech
2163	Correspondence with C. Tsai
2164	Correspondence with Globe Tech
2165	Correspondence with Globe Tech
2166	Correspondence with Globe Tech
2167	Correspondence with Globe Tech
2168	Correspondence with Globe Tech
2169	Correspondence with Globe Tech
2170	Correspondence with Globe Tech
2171	Correspondence with Globe Tech
2172	Correspondence with Globe Tech
2173	Correspondence with Globe Tech
2174	Correspondence with Globe Tech
2175	Correspondence with Globe Tech
2176	Correspondence with Globe Tech
2177	Correspondence with Globe Tech
2178	Correspondence with Globe Tech
2179	Correspondence with Globe Tech
2180	Correspondence with Globe Tech
2181	Correspondence with Globe Tech
2182	Correspondence with Globe Tech
2183	Correspondence with Globe Tech

Exhibit Number	Description
2184	Correspondence with Globe Tech
2185	Correspondence with Globe Tech
2186	Correspondence with Globe Tech
2187	Correspondence with Globe Tech
2188	Correspondence with Globe Tech
2189	Correspondence with C. Tsai
2190	Correspondence with Globe Tech
2191	Correspondence with Globe Tech
2192	Correspondence with Globe Tech
2193	Correspondence with Globe Tech
2194	Correspondence with Globe Tech
2195	Correspondence with Globe Tech
2196	Correspondence with Globe Tech
2197	Correspondence with Globe Tech
2198	Correspondence with J. Ong
2199	Correspondence with C. Tsai
2200	Correspondence with J. Ong
2201	Cisco Switch Feature Support Matrix
2202	Correspondence with M. Banin
2203	Correspondence with A. Lee
2204	Correspondence with M. Banin
2205	Correspondence with M. Banin
2206	Correspondence with M. Banin
2207	Correspondence with M. Banin
2208	Correspondence with M. Banin
2209	Correspondence with M. Banin
2210	Correspondence with M. Banin
2211	Correspondence with patent counsel
2212	Correspondence with patent counsel
2213	Correspondence with patent counsel
2214	Correspondence with patent counsel
2215	Correspondence with patent counsel
2216	Correspondence with patent counsel
2217	Correspondence with patent counsel
2218	Correspondence with patent counsel
2219	Correspondence with patent counsel
2220	Correspondence with patent counsel

Exhibit Number	Description
2221	Correspondence with patent counsel
2222	Correspondence with patent counsel
2223	Correspondence with patent counsel
2224	Correspondence with patent counsel
2225	Correspondence with patent counsel
2226	Correspondence with patent counsel
2227	Correspondence with patent counsel
2228	Correspondence with patent counsel
2229	Correspondence with patent counsel
2230	Correspondence with patent counsel
2231	Correspondence with patent counsel
2232	Correspondence with patent counsel
2233	Correspondence with patent counsel
2234	Correspondence with patent counsel
2235	Correspondence with patent counsel
2236	Correspondence with patent counsel
2237	Correspondence with patent counsel
2238	Correspondence with patent counsel
2239	Correspondence with patent counsel
2240	Correspondence with patent counsel
2241	Correspondence with patent counsel
2242	Correspondence with patent counsel
2243	Correspondence with patent counsel
2244	Correspondence with patent counsel
2245	Correspondence with patent counsel
2246	Correspondence with patent counsel
2247	Correspondence with patent counsel
2248	Correspondence with patent counsel
2249	Correspondence with patent counsel
2250	Correspondence with patent counsel
2251	Correspondence with patent counsel
2252	Correspondence with patent counsel
2253	Correspondence with patent counsel
2254	Correspondence with patent counsel
2255	Correspondence with patent counsel
2256	Correspondence with patent counsel
2257	Correspondence with patent counsel

Exhibit Number	Description
2258	Correspondence with patent counsel
2259	Correspondence with patent counsel
2260	Correspondence between S. Lum and A. Lee
2261	Correspondence between S. Lum and A. Lee
2262	Correspondence with patent counsel
2263	Correspondence with patent counsel
2264	Correspondence with patent counsel
2265	Correspondence with patent counsel
2266	Correspondence with patent counsel
2267	Correspondence with patent counsel
2268	Correspondence with patent counsel
2269	Correspondence with patent counsel
2270	Correspondence with patent counsel
2271	Correspondence with patent counsel
2272	Intentionally Left Blank
2273	Correspondence between S. Lum, J. Ong, C. Tsai and A. Lee
2274	Correspondence between S. Lum, C. Tsai and A. Lee
2275	Internal Notes
2276	Correspondence between C. Tsai, J. Ong and S. Lum
2277	Correspondence between C. Tsai, J. Ong and S. Lum
2278	Correspondence between C. Tsai, J. Ong and S. Lum
2279	Correspondence between C. Tsai, J. Ong and S. Lum
2280	Correspondence between C. Tsai and S. Lum
2281	Correspondence between T. Nakano and S. Lum
2282	Draft Meetinghouse Agreement
2283	Correspondence with Globe Tech
2284	Intentionally Left Blank
2285	Correspondence between S. Lum and corporate counsel
2286	Intentionally Left Blank
2287	Correspondence with Globe Tech
2288	Correspondence with Globe Tech
2289	Correspondence with Globe Tech
2290	Correspondence with Globe Tech
2291	Correspondence with Globe Tech
2292	Correspondence with Globe Tech
2293	Correspondence with Globe Tech
2294	Correspondence with Globe Tech

Exhibit Number	Description
2295	Correspondence with Globe Tech
2296	Correspondence with Globe Tech
2297	Correspondence with Globe Tech
2298	Correspondence between S. Lum and J. Ong
2299	Correspondence between S. Lum and J. Ong
2300	Correspondence with Globe Tech
2301	Correspondence with Globe Tech
2302	Correspondence between M. Banin and S. Lum
2303	Correspondence with Globe Tech
2304	Correspondence with Globe Tech
2305	Correspondence with Globe Tech
2306	Correspondence with Globe Tech
2307	Correspondence with Globe Tech
2308	Correspondence with Globe Tech
2309	Correspondence with Globe Tech
2310	Correspondence with Globe Tech
2311	Correspondence with Globe Tech
2312	Correspondence with Globe Tech
2313	Correspondence with Globe Tech
2314	Correspondence with Globe Tech
2315	Correspondence with Globe Tech
2316	Correspondence with Globe Tech
2317	Correspondence with Globe Tech
2318	Correspondence with Globe Tech
2319	Correspondence with Globe Tech
2320	Correspondence with Globe Tech
2321	Correspondence with Globe Tech
2322	Correspondence with Globe Tech
2323	Correspondence with Globe Tech
2324	Correspondence with Globe Tech
2325	Correspondence with Globe Tech
2326	Correspondence with Globe Tech
2327	Draft Patent Application
2328	Draft Patent Application
2329	CyberGatekeeper Enforcement Modes
2330	CyberGatekeeper Enforcement Modes
2331	Correspondence with Globe Tech

Exhibit Number	Description
2332	Correspondence with Globe Tech
2333	Correspondence with Globe Tech
2334	Correspondence with Globe Tech
2335	Correspondence with Globe Tech
2336	Correspondence with Globe Tech
2337	Correspondence with Globe Tech
2338	Correspondence with Globe Tech
2339	Correspondence with Globe Tech
2340	Internal InfoExpress Correspondence
2341	Intentionally Left Blank
2342	Internal InfoExpress Correspondence
2343	Correspondence with Globe Tech
2344	Correspondence with Globe Tech
2345	Correspondence with Globe Tech
2346	Correspondence with Globe Tech
2347	Correspondence with Globe Tech
2348	Correspondence with Globe Tech
2349	Correspondence with Globe Tech
2350	Correspondence with Globe Tech
2351	Correspondence with Globe Tech
2352	Correspondence with Globe Tech
2353	Correspondence with Globe Tech
2354	Correspondence with Globe Tech
2355	Correspondence with Globe Tech
2356	Correspondence with Globe Tech
2357	Correspondence with Globe Tech
2358	Correspondence with Globe Tech
2359	Correspondence with Globe Tech
2360	Correspondence with Globe Tech
2361	Correspondence with Globe Tech
2362	Correspondence with Globe Tech
2363	Correspondence with Globe Tech
2364	Correspondence with Globe Tech
2365	Correspondence with Globe Tech
2366	Correspondence with Globe Tech
2367	Correspondence with Globe Tech
2368	Correspondence with Globe Tech

Exhibit Number	Description
2369	Correspondence with Globe Tech
2370	Correspondence with Globe Tech
2371	Correspondence with Globe Tech
2372	Correspondence with Globe Tech
2373	Correspondence with Globe Tech
2374	Correspondence with Globe Tech
2375	Correspondence with Globe Tech
2376	Correspondence with Globe Tech
2377	Correspondence with Globe Tech
2378	Correspondence with Globe Tech
2379	Correspondence with Globe Tech
2380	Correspondence with Globe Tech
2381	Correspondence with Globe Tech
2382	Correspondence with Globe Tech
2383	Intentionally left blank
2384	Correspondence with Globe Tech
2385	Correspondence with Globe Tech
2386	Internal InfoExpress Correspondence
2387	Correspondence with Globe Tech
2388	Correspondence with Globe Tech
2389	Internal InfoExpress Correspondence
2390	Correspondence with Globe Tech
2391	Intentionally left blank
2392	Intentionally left blank
2393	Intentionally left blank
2394	Intentionally left blank
2395	Correspondence with Globe Tech
2396	Internal InfoExpress Correspondence
2397	Correspondence with Globe Tech
2398	Intentionally left blank
2399	Correspondence with Globe Tech
2400	Correspondence with Globe Tech
2401	Correspondence with Globe Tech
2402	Correspondence with Globe Tech
2403	Correspondence with Globe Tech
2404	Correspondence with Globe Tech
2405	Correspondence with Globe Tech

Exhibit Number	Description
2406	Correspondence with Globe Tech
2407	Correspondence with Globe Tech
2408	Correspondence with Globe Tech
2409	Correspondence with Globe Tech
2410	Correspondence with Globe Tech

I. Introduction

Patent Owner submits this Patent Owner Preliminary Response to the Petition related to claims 1-5, 11, 12, 16-19 and 23-25 (the "Challenged Claims") of U.S. Patent 7,523,484. Patent Owner requests the Board reject the Petition because the Grounds presented and art relied on fail to render any of the Challenged Claims unpatentable because the art fails to render obvious all of the claimed limitations, because the art does not qualify as prior art.

II. The '484 Patent

A. Date of Invention

For the reasons discussed in section VII, the date of invention for each of the Challenged Claims is no later than December 2, 2002.

B. Person of Ordinary Skill in the Art (POSITA)

A POSITA would have a working knowledge of computer network security art. A POSITA would have a bachelor's degree in computer science, computer engineering, or electrical engineering, and at least three years of experience in networking operating systems and cybersecurity, or a person with a master's degree in one of the foregoing and at least two years of experience in the aforementioned fields.

C. Overview of the '484 Patent

The patent is directed to a novel security solution for controlling access to a protected network. Before Patent Owner's inventions, network security required a

"gatekeeper" between each client/user and the network. EX1501, Fig. 1, 1:53-60; EX2001, ¶¶ 44-45. But as the patent explains, access control is improved by evaluation of accessing device's hardware and software, *e.g.*, virus protection, before the gatekeeper granted such access—thus consuming substantial network resources and creating bottlenecks. EX1501, 1:41-52.

An example of the prior art architecture is shown in annotated FIG. 1.

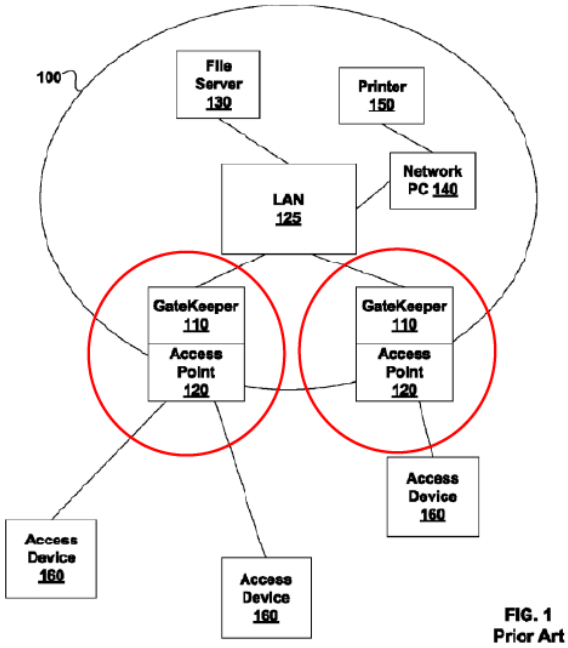


FIG. 1
Prior Art

The protected network 100 includes two Gatekeepers 110, each associated with a different instance of an Access Point 120. All devices attempting to access the protected network are required to be evaluated by a gatekeeper. With large corporate networks including many access points, the "use of one instance of GateKeeper 110 to support numerous instances of Access Device 160 is limited by bandwidth and

required sophistication (e.g., cost) of GateKeeper 110." EX1501, 2:31-34. The gatekeeper then becomes a limiting bottleneck. *Id*.

The patent addressed this previously unidentified problem with a novel and non-obvious approach relieving computer resources by configuring an access point in response to approval of a device by the gatekeeper. By configuring the access point to allow devices vetted by the gatekeeper to meet both authentication requirements and device compliance (auditing), to access the protected network, subsequent evaluation of the user/device by the gatekeepers when the previously evaluated device accesses the network again is obviated.

The patent discloses a protected network including a restricted subset with a gatekeeper and less-restricted subsets.

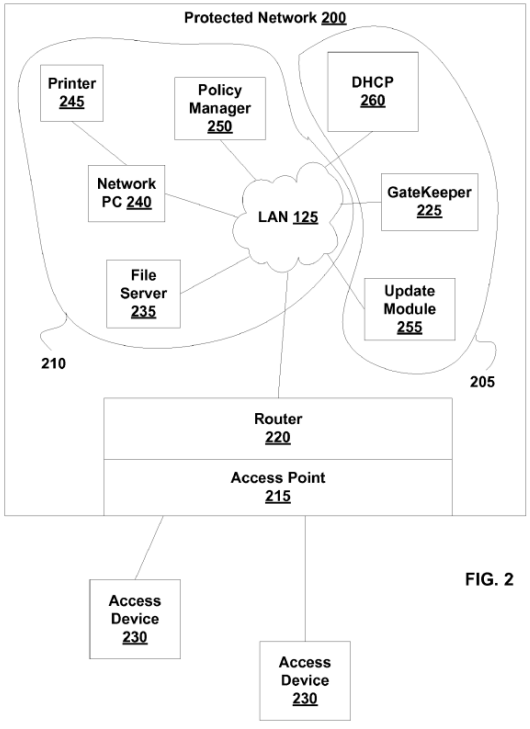


FIG. 2

52697138.1

EX1501, Fig. 2. Before a device is granted access to a less-restricted subset 210, its request is passed to the restricted subset (indicated as 205). EX1501, 2:52-56, 5:51-54. A gatekeeper in the restricted subset audits the device against security policies pertaining to device configurations (e.g., virus protection software). EX1501, 6:34-48; 7:42-45. Determining whether the user/device is authenticated (e.g., username, password, MAC address) to access the protected network may also be performed. *E.g.*, EX1501, 6:41-49. In this embodiment, if the device passes both the audit and authentication, it is granted access to a less-restricted subset of the protected network. EX1501, 11:10-67, 12:1-43.

An improvement over the earlier approaches is that rather than require all device communications to pass through the gatekeeper, the access point itself is configured in response to approval of the device by the gatekeeper. The patent explains:

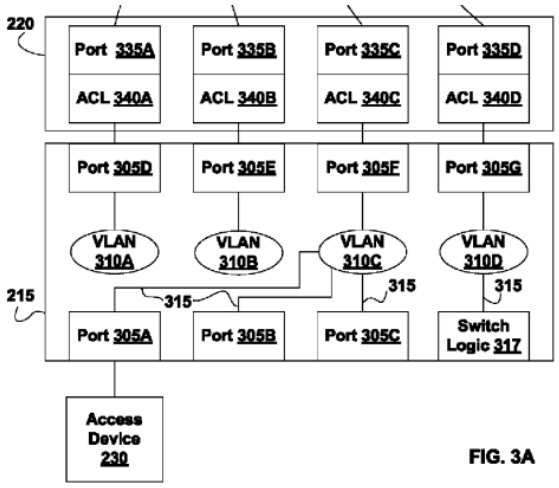


FIG. 3A

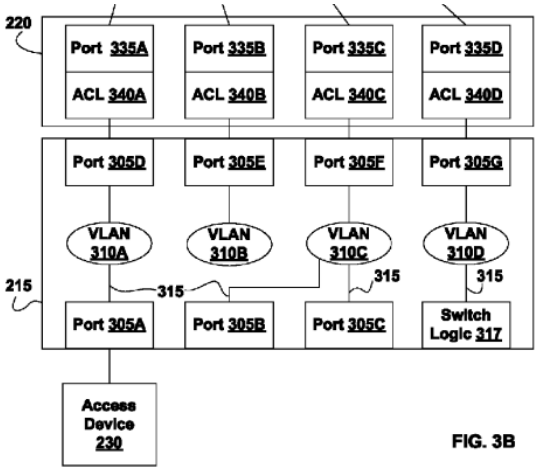


FIG. 3B

> Switch Logic 317 is configured for configuring and reconfiguring members of Ports 305A-305G responsive to received commands. For example, by receiving an appropriate command, Switch Logic 317 is configured to reconfigure Port 305A to be associated with VLAN 310A, as illustrated in FIG. 3B below. In this configuration, data received at Port 305A is directed to Port 305D via VLAN 310A, rather than to Port 305F.

EX1501, 8:16-23.

By configuring the access point in response to approval of the device, network traffic for previously approved devices passes to the less-restricted subset without passing through the gatekeeper, thereby alleviating the burden on computer resources.

III. Claim Construction

Petitioners assert the claims should be given their ordinary as understood by a POSITA. Pet. at 7. Petitioners avoid providing any explanation and then deviate from the ordinary meaning by way of their arguments regarding how the cited references supposedly meet the claimed limitations.

Patent Owner contends the claims should be given their ordinary meaning in the context of the intrinsic evidence, as discussed herein. Patent Owner provides the following context for certain claim terms to properly frame the appropriate ordinary meaning.

A. "Access Control Configured To Reconfigure The Communication Device … If The Audit Results In A Determination That The Access Device Meets The Requitements Of The At Least One Security Policy "

The Challenged Claims require "an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network … if the audit results in a determination that the access device meets the requirements of the at least one security policy…." EX1501 at 16:11-17. The ordinary meaning of this limitation requires reconfiguration **of a *communication device***—not merely a change to the user device (i.e., "access device") or to user identification data. The claimed "reconfiguration" is also required to be "if the audit results" in the device being qualified. As discussed herein, this "audit" pertains to whether the device includes the software/hardware necessary to comply with a security policy – a distinct evaluation from authentication.

One must first look to the words of the claim. "Configure" means to arrange something.[1] "Reconfigure" just means to change an existing configuration.

Further, reconfiguration must be of the "communication device." And, this reconfiguring must be in response to approval of a device based on an audit request.

The specification is consistent with this plain meaning, and teaches: "[t]o grant access, the gatekeeper sends commands to the access point in order to reconfigure a communication port to which the access device is connected. The

[1] *See* https://www.merriam-webster.com/dictionary/configure.

reconfiguration typically includes assigning the communication port from the restricted VLAN to the less-restricted VLAN." EX1501, 3:20-25. The specification provides an example of configuring the "access point" 215 involving reassigning ports.

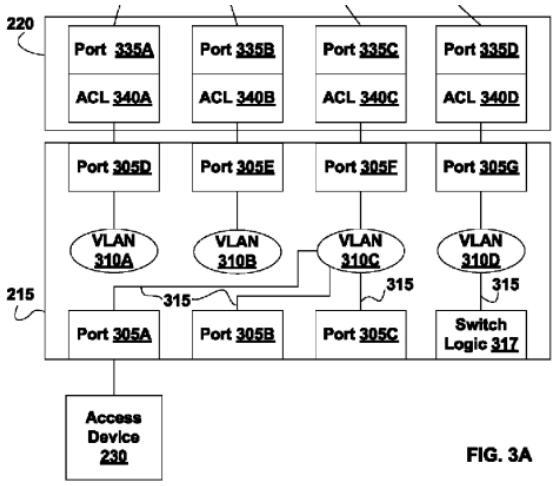


FIG. 3A

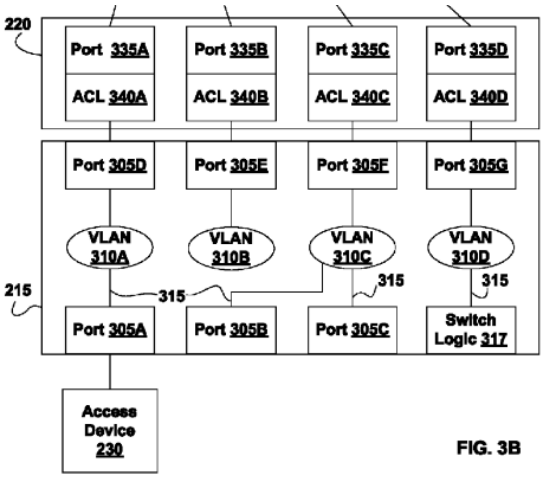


FIG. 3B

> Switch Logic 317 is configured for configuring and reconfiguring members of Ports 305A-305G responsive to received commands. For example, by receiving an appropriate command, Switch Logic 317 is configured to reconfigure Port 305A to be associated with VLAN 310A, as illustrated in FIG. 3B below. In this configuration, data received at Port 305A is directed to Port 305D via VLAN 310A, rather than to Port 305F.

EX1501, 8:16-26.

> Switch Logic 317 is controlled by an Access Control 320 included in GateKeeper 225. Access Control 320 is configured to send commands to Switch Logic 317 in order to reconfigure members of Ports 305A-305G. This reconfiguration includes modifying the association of members of Ports 305A-305G with different members of VLANs 310A-310D.

Id., 9:20-25.

> Access Control 320 is responsive to a Policy Auditor 325 included in GateKeeper 225. Policy Auditor 325 is configured to receive a request for access to Less-Restricted Subset 210 from Access Device 230, to determine which of Security Policy 330A or optional Security Policy 330B applies to the current request, to perform a security audit of Access Device 230 based on the appropriate member of Security Policies 330A-330B, and to notify Access Control 320 if the audit is passed. This notice typically causes Access Control 320 to reconfigure a member of Ports 305A-305G using Switch Logic 317. For example, in some embodiments, if Security Policy 330A applies and if Access Device 230 satisfies requirements of Security Policy 330A, then Policy Auditor 325 provides a notice to Access Control 320. In response, Access Control 320 sends appropriate commands to Switch Logic 317. These commands cause changes in Port 305A, such that communication from Access Device 230 is no longer blocked by ACL 340C and can now be received by elements of Less-restricted Subset 310.
>
> FIG. 3B is a block diagram showing further details of Access Point 215, Router 220 and GateKeeper 225 of FIG. 2, after access has been granted to elements of Less-Restricted Subset 210, according to various embodiments of the invention. Port 305A has been reconfigured to be associated with VLAN 310A rather than VLAN 310C.

Id., 9:30-62.

Thus, ordinary meaning for "an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network … if the audit results in a determination that the access device meets the requirements of the at least one security policy…" is a network component that rearranges the communication device, such as the ports of an access point itself, in response to auditing of the device.

A further part of the limitation deserved of discussion is the requirement that the reconfiguration occurs "if the audit results in a determination that the access device meets the requirements of the at least one security policy." Of particular relevance are "audit" and "security policy."

The specification, which is the best guide for determining the meaning of claim terms, is clear. A security policy can include authentication, i.e., identification, which pertains to confirmation that the user or user's device is what they or it purports to be. A security policy can also include determining whether the device complies with software/hardware requirements of the network. As such, the claimed audit and determination that the device meets the requirement of a security policy means the device's hardware/software meets network device requirements. Notably, "auditing" is not authentication.

> Various embodiments of the invention include a network gatekeeper comprising at least one security policy including requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network, ***a policy auditor configured to audit an access device using the at least one security policy***, in response to a request to access the less-restricted subset of the protected network, ***the request being sent from the access device to the gatekeeper via a communication device, and an access control configured to reconfigure the communication device*** such that data sent from the access device can be received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, ***if the audit results in a determination that the access device meets the requirements of the at least one security policy***, the restricted subset of the protected network including the gatekeeper.

EX1501, 3:60-67, 4:1-9.

> Access Control 320 is responsive to a Policy Auditor 325 included in GateKeeper 225. ***Policy Auditor 325 is configured to receive a request for access to Less-Restricted Subset 210 from Access Device 230, to determine which of Security Policy 330A or optional Security Policy 330B applies to the current request, to perform a security audit of Access Device 230 based on the appropriate member of Security Policies 330A-330B, and to notify Access Control 320 if the audit is passed***. This notice typically causes Access Control 320 to reconfigure a member of Ports 305A-305G using Switch Logic 317.

EX1501, 9:30-43.

The specification also establishes "auditing" and "authentication" are two different evaluations: "[r]eliance on mere user authentication includes several disadvantages. For example, there are no provisions to assure that an access device used by the authenticated user meets network security policies." EX1501, 1:41-44. The specification also distinguishes between the claimed "audit " and "authentication":

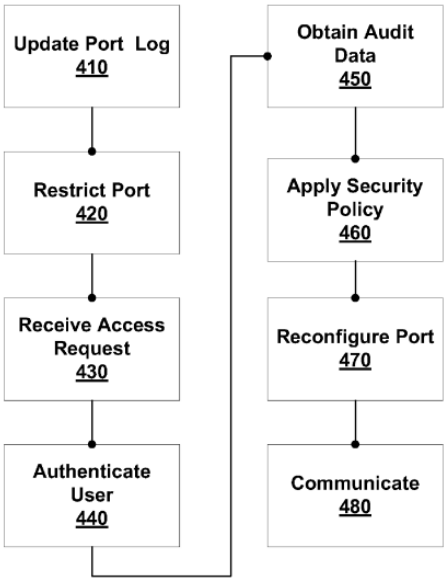


FIG. 4

… Update Port Log Step 410 and a Restrict Port Step 420 are used to prepare an open (unused) communication port on Access Point 215 for receiving a request for access to Less-Restricted Subset 210. This request is received from Access Device 230 in a Receive Access Request Step 430. ***In response, GateKeeper 225 authenticates a user, obtains audit data, and applies a security policy in an Authenticate User Step 440, an Obtain Audit Data Step 450 and an Apply Security Policy Step 460, respectively. If the security policy is satisfied, then in a reconfigure Port Step 470, GateKeeper 225 reconfigures the communication port of Access Point 215 to which Access Device 230 has connected.***

EX1501, 10:26-40.

IV. Petitioners' References

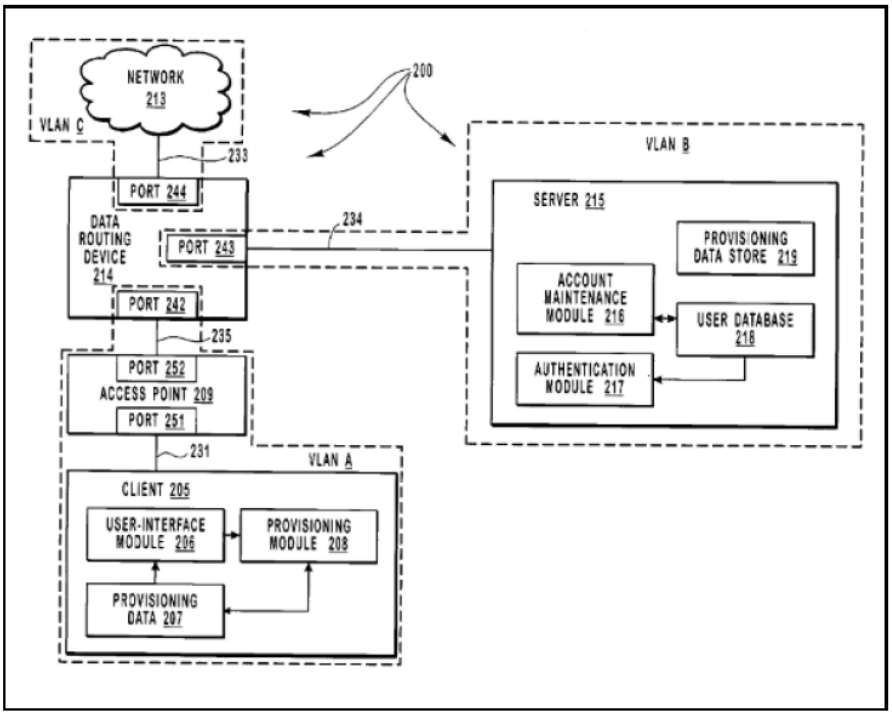
Krantz and Herrmann are not prior art. Krantz and Herrmann are also readily distinguished from the Challenged Claims, and merely illustrate examples of the earlier network security approaches improved upon by the '484 Patent.

A. Krantz

Krantz is described as follows:

> A computer system attempts to authenticate with a server to gain authorization to access a first network. It is determined by the server that the computer system is not authorized to access the first network. The computer system is given authorization to access a second network for at least the purpose of downloading files (e.g., signup and configuration files) needed to access the first network. A user-interface for receiving user-entered signup information is automatically presented at the computer system. A first schema-based document including user-entered information is transferred to the server. If the server determines that the user-entered information is appropriate, a second-schema document, which includes an indication of authorization to access the first network (e.g., a user-identifier and password), is received. A third schema-based document is executed at the computer system to compatible configure the computer system for accessing the first network.

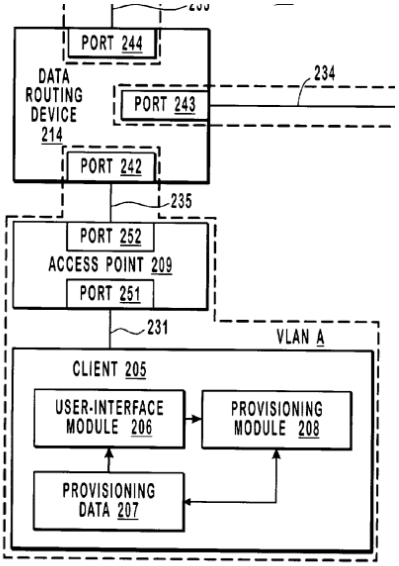
EX1505, Abstract. Krantz discloses the concept wherein upon the failure of a computer system to **authenticate a user** to one network, the user can access a second network for the limited purpose of downloading files by a server. EX2001, ¶¶47-49. This authentication by Krantz is further explained below.



A server includes the functionality to authorize clients to access a second network (e.g., the Internet). The server can be located on a first network that is separate from the second network or can be located on the second network. A client sends credentials to the server to attempt to authenticate with the server. Based on the credentials, the server may authorize the client for at least partial access to the second network and/or may deny access to the second network and authorize the client for at least partial to access to the first network. The server can be a Remote Authentication Dial-In User Service ("RADIUS") server that is located on the first network. Clients can be provided partial access to the first or second network at least for the purposes of authenticating with the server and downloading provisioning files used to gain full access to the second network. Thus, computer systems that are not currently able to access resources located on the second network may be able to electronically download provisioning files for gaining access to those resources.

EX1505, [0016]. As shown, in the excerpted portion of Fig. 2, an access point 209 is identified and the client communicates via access point 209 through port 251. *See*

id., [0063]. The access point 209 then sends data to data routing device 214 via port 252. This data routing device directs data through either port 244 or port 243.



There is no teaching of arranging or rearranging the access point 209 in response to approval of a device (including both user authentication and device security policy compliance) by a gatekeeper. EX2001, ¶¶ 49, 64. Krantz does not teach arranging the access point in response to anything, let alone in response to evaluating a user or device attempting to access a network. Ports 251 and 252 are never arranged in response to any evaluation by a gatekeeper. EX2001, ¶¶ 59-60. Instead, Krantz teaches only modifying data on the user device.

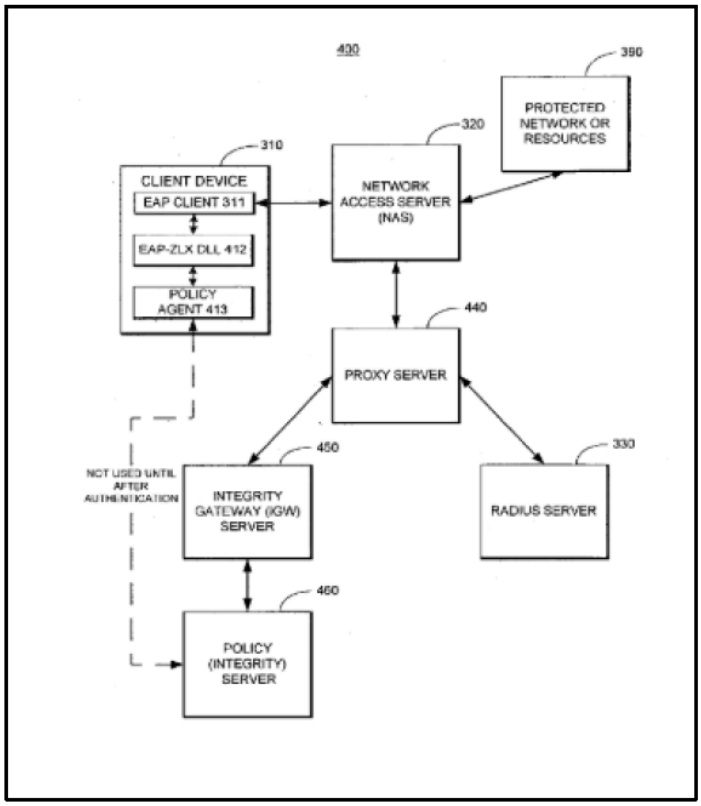
B. Herrmann

Herrmann describes a system as follows:

> A system and methodology for policy enforcement during authentication of a client device for access to a network is described. A first authentication module establishes a session with a client device

> requesting network access for collecting information from the client device and determining whether to authenticate the client device for access to the network based, at least in part, upon the collected information. A second authentication module participates in the session with the client device for supplemental authentication of the client device for access to the network. The supplemental authentication of the client device is based, at least in part, upon the collected information and a policy required as a condition for network access.

EX1506, Abstract. Like the prior art discussed in the '484 Patent, Herrmann utilizes servers between the client device and the protected network, and all attempts to access the protected network must first be checked for security policy compliance by at least a Network Access Server (NAS), which would create the bottleneck problems. EX2001, ¶ 53; *see also id.*, ¶ 62.



52697138.1

EX1506, Fig. 4, *compare id. to* EX1501, Fig. 1. Unlike the '484 Patent, Herrmann requires all data from client device 310 to pass through the NAS 320. There is no disclosure where the client device is ever able to access the protected network without going through the NAS. Nor, is there any teaching of configuring an access point in response to an access device having satisfied an audit.

V. Krantz Alone (Ground 1) or the Combination of Krantz and Herrmann (Ground 2) Fail to Render Obvious Any of the Challenged Claims

Ground 1 asserts invalidity based on Krantz alone, and Ground 2 asserts invalidity based on Krantz in combination with Herrmann. For both Grounds, key claim limitations are missing. Institution must be denied.

A. Ground 1: Krantz Is Missing Claimed Limitations

Krantz fails to disclose at least the following limitations: (1) "an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network … if the audit results in a determination that the access device meets the requirements of the at least one security policy"; and (2) "a policy auditor configured to audit the access device using the at least one security policy." Accordingly, the petition based on Ground 1 should be denied.

1. Krantz Does Not Disclose "An Access Control Configured To Reconfigure The Communication Device Such That Data Sent From The Access Device Is Received By The Less-Restricted Subset Of The Protected Network … If The Audit Results In A Determination That The Access Device Meets The Requirements Of The At Least One Security Policy"

The Challenged Claims require "an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network … if the audit results in a determination that the access device meets the requirements of the at least one security policy." Krantz does not disclose this. EX2001, ¶¶ 58-60. Rather, Krantz only discloses inserting "tag headers" ***into client data***; not changing ***the communication device***.

The patent explains configuring a communication device so that data is sent to a less-restricted subset of the protected network "typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN." EX1501, 3:22-25. Thus, there are changing pathway assignments for the ports of *the "access point."*

Indeed, as discussed in § II(C), configuration of an access point in response to approval of a device by the gatekeeper involves changing the VLAN to which a port may communicate.

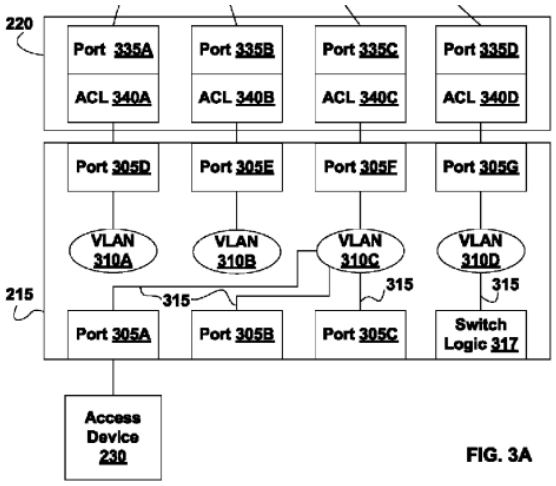


FIG. 3A

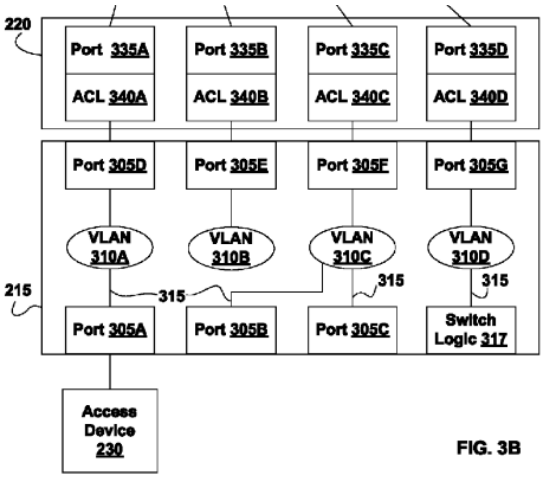


FIG. 3B

> Communication received at one member of Ports 305A-305G is directed internally to another member of Ports 305A-305G via a member of VLANs 310A-310D. VLANs 310A-310D are logical associations between members of Ports 305A-305G. Typically, any members of Ports 305A-305G that are configured to be associated with the same member of VLANs 310A-310D are in bi-directional communication with each other. These associations are illustrated in FIGS. 3A and 3B by Lines 315.

EX1501, 7:62-67, 8:1-3.

> Switch Logic 317 is configured for configuring and reconfiguring members of Ports 305A-305G responsive to received commands. For example, by receiving an appropriate command, Switch Logic 317 is configured to reconfigure Port 305A to be associated with VLAN 310A, as illustrated in FIG. 3B below. In this configuration, data received at Port 305A is directed to Port 305D via VLAN 310A, rather than to Port 305F.
>
> *Id.*, 8:16-23.

Petitioners strain to argue Krantz supposedly discloses the subject limitation by way of "tag header" insertion into client data. Pet. at 41-48. Adding a tag header

to client data is not the claimed configuring of an access point. If anything, it is modification of client information.

Petitioners assert Krantz's "access point 209" is "the communication device." Pet. at 40-42. Petitioners then argue Krantz discloses the claimed reconfiguration of the access point: "Krantz discloses "[w]hen client 205 is authorized to access resources located on VLAN C, access point 209 may enable protocols that are currently blocked for port 251 and may insert Tag Headers indicating that data from client 205 is to be transferred to VLAN C []. Server 215 can send commands to access point 209 to cause access point 209 to enable protocols and cause access point 209 to insert appropriate Tag Headers." Pet. at 48. Petitioners also argue port 251 is "reconfigur[ed]" in a way "such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network" because it facilitates the transfer of data between client 205 ("the access device") and ultimately VLAN C (the "less-restricted subset of the network.") as depicted below." Pet. at 44-46.

Petitioners arguments fall flat. Krantz discloses configuration or reconfiguration of client data, not the communication device. The '484 Patent is clear: "[t]he reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN." EX1501, 2:22-25. Ss shown in FIG. 3A, port 305A of the access point 215 sends data to VLAN 310C (as

shown by line 315). In FIG. 3B, however, that same port 305A is "configured" to send data to VLAN 310A. Krantz has no reconfiguration of the communication device. Instead, the Krantz ports in access point 209 send data to the same location (e.g. port 243 to VLAN B and port 244 to VLAN C). Krantz's only teaching is adding identification data to client information.

> A tagged data frame is a data frame that includes an indication, such as, for example, a Tag Header, that identifies a VLAN and/or frame classification associated with the tagged data frame. A Tag Header can be inserted into a data frame by a VLAN aware device to indicate to data routing device 214 a VLAN ID of the VLAN from which a tagged data frame was received. For example, ***access point 209 can insert a Tag Header into data from client 205 to indicate to data routing device 214 that the data was received from VLAN A***.

EX1505, [0061].

> ***Data routing device 214 can process the inserted Tag Header*** and transfer the EAPOL packet onto VLAN B. Server 215 can receive the EAPOL packet, which is transferred to authentication module 217 for authentication. Alternately, access point 209 access point 209 and/or data routing device 214 may strip the 802.1X encapsulation and instead encapsulate the EAP-Response/Identity message within an EAP-RADIUS message that is transferred onto VLAN B. … When credentials are sent to server 215, authentication module 217 can receive the credentials (e.g., user-identifier and password) and compare the credentials to entries in user database 218. If credential information matches an entry in user database 218, the identity of a user is authenticated (i.e., server 215 believes that the user represented by the user-identifier is the user who entered the credential information).

EX1505, [0073]-[0076]. It is undeniable Krantz fails to disclose **any** reconfiguration of access point 209. EX2001, ¶ 63. While Krantz's "data routing device 214" directs the traffic to either the VLAN B or VLAN C based on consideration of the user's

identification information and may redirect the data based on the user's tagged identification information, there is no "reconfiguring" ***of the access point 209***, which Petitioners argue is the claimed "communication device."

Further, Krantz explains it is not the access point, but rather, the data routing device 214 which directs the traffic to VLAN B or VLAN C. EX1505, [0060]; EX2001, ¶59. Even this, however, depends on configuration of client data, not the data routing device itself.

Lastly, as a fallback, Petitioners argue it would have been obvious for one to combine the access point 209 and the data routing device 214. Pet. at 52-55. Regardless of whether access point 209 could be combined with data routing device 214, configuring client data with tag headers is not configuring of the access point – it is only manipulating "data from client 205." EX1505 at, *e.g.*, [0061]. As such, the different data paths of Krantz still require the data routing device to check user identification information, namely, the tag header.

Further, Krantz recites separate access point 209 and data routing device 214. Arbitrarily combining these distinct components finds no support in Krantz. To the contrary, Krantz expressly teach access point 209 and a different component, namely a data routing device 214. EX1505, [0073] ("[A]ccess point 209 and/or data routing device 214 may strip the 802.1X encapsulation and instead encapsulate the EAP-Response/Identity messages within an EAP-RADIUS message that is transferred

onto VLAN B."). Krantz further confirms any configuration is of user identification data, not an access point as claimed, because "EAP-Response/Identity messages" expressly relate to user authentication.[2] Even if it were possible to combine access point 209 and data routing device 214, this would not resolve the bottleneck problem with the prior art, such as Krantz. Instead, all traffic would still go through access point 209 and data routing device 214. See EX1505, [0060].

Krantz's failure to disclose the reconfiguration of the communication device alone requires denial of institution.

2. Krantz Fails To Disclose "A Policy Auditor Configured To Audit The Access Device Using The At Least One Security Policy"

The Challenged Claims recite "a policy auditor configured to audit the access device using the at least one security policy." Despite Petitioners' attempts to conflate authentication with auditing, Krantz lacks ***any*** device ***auditing***.

Petitioners argue Krantz discloses the claimed "policy auditor" as "server 215." Pet. at 32-36.

[2] This understanding is consistent with how a POSITA understands EAP-Response/Identity. *See*, https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485048062.htm.

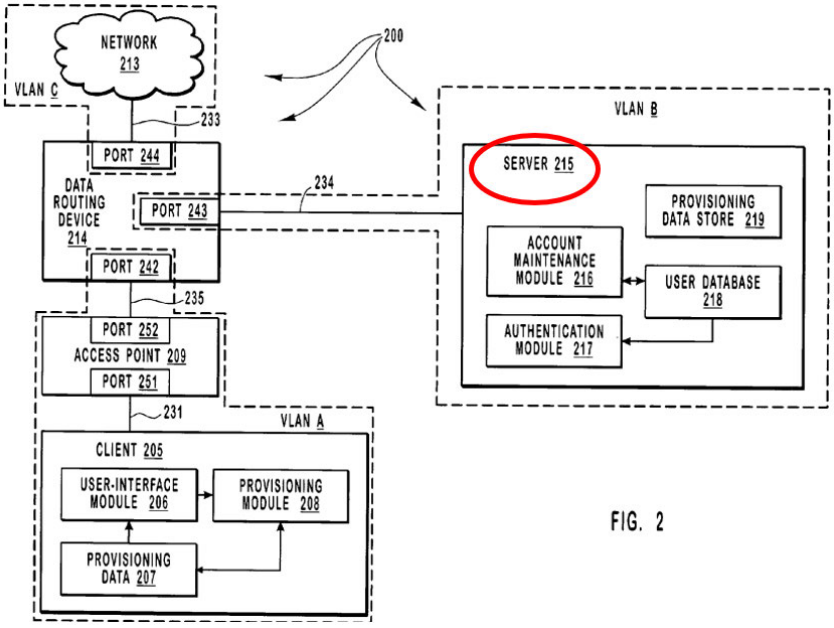


FIG. 2

But the Krantz server 215 is only for authentication. By contrast, the Challenged Claims recite a "policy ***auditor***." As discussed, the correct construction of a policy audit is an evaluation of device information related to whether it complies with software/hardware requirements of the network. Krantz fails to disclose any evaluation of the "device information." Petitioners rely on Krantz's disclosures regarding client ***authentication***, which, as discussed is a different evaluation from device auditing. Indeed, Krantz's disclosure is clearly limited to client authentication and silent on device auditing.

The '484 Patent expressly distinguishes between evaluating "authentication" information and "auditing" a device. The '484 Patent explains auditing relates to evaluating data about the device's software and/or hardware that is necessary to comply with a security policy, such as "operating system status (version, updates,

etc.), antivirus software status, information concerning devices connected to Access Device 230, Windows registry information, MAC address, IP addresses, cookies, status of applications executing on Access Device 230[.]" EX1501, 11:45-47. In contrast, authentication merely confirms identity. EX1501, 1:31-37 ("A first level of access control is achieved by requiring authentication of a user. This may be accomplished by requiring the user to enter a username and password or by reading a MAC address or other identifying information from an access device. ")

Authentication is a different technical concept, process, and implementation from the claimed "evaluate device information received from the device in response to the audit request." Indeed, a user can be properly authenticated, but if the access device does not have the proper antivirus software, then the network can be at risk. EX1501, 6:41-48.

Yet, Krantz only discloses user authentication, and fails to disclose anything about "evaluat[ing] device information in response to the audit request":

- "Krantz discloses that . . . '**authentication module 217** can receive the credentials (e.g. user-identifier and password) and compare the credentials to entries in the user database 218.'" Pet. at 40-41.
- "If an **authenticated user** of client 205 . . . is authorized to access resources…" EX1505, [0076] (cited in Pet. at 26-27, 35, 40, 49).
- "Krantz discloses that the 'method 300 includes [the act of client 205] sending credentials to a server to **authenticate** . . . ." Pet. at 28.

- "If credentials do not authorize full access to the second network (e.g., credentials cannot be **authenticated**, credentials are guest credentials, or an **authenticated user is not authorized**) . . ." EX1505, [0019].

With no evidence for Krantz of auditing a device—checking the device for compliance with network security policies—Petitioners repeatedly cite to user authentication protocols and incorrectly conclude this is "device information" or an "audit request." *See* Pet. at 56-59. As Dr. Cole explains, such device authentication is different from device auditing. *See* EX2001, ¶¶ 49, 58-59.

Petitioners claim that Krantz discloses "receiving audit data" because it "sends credentials to the server":

> [Krantz] discloses that the "server (based at least in part on received credentials) may authorize the client for at least partial access to the single network.

Pet. at 32. Petitioner's "credentials" argument fails immediately. The '484 Patent explains user authentication data and audit data are different. *Compare* EX1501, 1:33-42 (authentication) *with* 11:48-54 (audit data). Next, the Krantz "credentials" are the "user-identifier[s] and password[s]" which the '484 Patent expressly explains relate to authentication; they are not audit data. *See* Pet. at 33; EX1501, 1:33-37. Indeed, a user may access different devices using the same username and password. Third, Petitioners claim credentials also "can include sending an Extensible Authentication Protocol ('EAP') Response/Identity message…" Pet. at 33. EAP is for authentication. In fact, it is an acronym that stands for Extensible **Authentication**

Protocol. EX1501, 8:29-30. EX2001, ¶ 57. Fourth, Petitioners assert "authentication module 217 can receive the credentials (e.g. user-identifier and password) and compare the credentials to entries in user database 218. If credential information matches an entry in user database 218, the identity of the user is authenticated[.]" Pet. at 35. Again, on its face, this is user data unrelated to audit data for the device. EX2001, ¶¶ 57-58.

Additionally, Petitioners baldly claim Krantz's disclosures are "consistent with the disclosure of the 484 Patent that describes security policies having requirements related to user identification and passwords or configuration requirements related to the access device (such as aspects of the operating system), … or to authenticate an access device or user." Pet. at 27. This is wrong for several reasons. First, this is not what the '484 Patent says. Rather, the '484 Patent explains that **in addition to** conducting a security policy audit for a device, the authentication of the user can be conducted along with the same process. *See* EX1501, Fig. 4, 10:26-44. Nowhere does it say that audit data is the same thing as authentication information. Second, the claim requires "a policy auditor configured to audit the access device." Not to "authenticate a ***user***" which is a distinct type of evaluation.

Petitioners' secondary reference, Herrmann, even confirms authentication is distinct from security policy compliance. "One problem that is not addressed by current NAS and RADIUS [authentication] technology is ensuring that all devices

that connect to a network comply with and enforce applicable security policies." EX1506, [0011].

The '484 Patent also expressly distinguishes between authenticating a user and the separate security evaluation for the device based on "device information":

> [A]n AP (e.g., a switch or wireless access point (WAP) which is used to connect end points to the corporate network) may be programmed to prohibit access by the PC (e.g., notebook, desktop PC, PDA, or similar computing device) to the corporate network until authentication with the **authentication server passes AND an audit with the software agent** with the GK (e.g., software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria) passes, while still supporting the existing encryption and authentication functionality. **The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol.**

EX1501, 13:57-67, 14:1-3 (ALL CAPS emphasis of "AND" in original).

Accordingly, Krantz fails to disclose or suggest this claim limitation.

B. Ground 2: Krantz in Combination with Herrmann Fails To Render Obvious The Challenged Claims

Petitioners argue, to the extent Krantz is deemed not to disclose certain claim limitations, a POSITA would have found it obvious to and been motivated to incorporate Herrmann with Krantz.

Ground 2 fails first because even the asserted combination of Krantz and Herrmann fails to disclose at least the "access control configured to reconfigure the communication device such that data sent from the access device is received by the

less-restricted subset of the protected network … if the audit results in a determination that the access device meets the requirements of the at least one security policy " limitation.[3] Regardless of whether one considers Krantz alone or in combination with Herrmann, this specifically required limitation of the Challenged Claims is missing.

In addition, the Petition relies on Krantz alone for several of the claimed limitations of claim 1. With respect to the limitations Petitioners identify as 1.1-1.3, Petition cherry-picks portions of Herrmann to fill them. Petitioners' contentions regarding these limitations still fail. Also, the motivation to combine isolated teachings from Herrmann with Krantz argued in the Petition do not pass muster.

The Petition argues, "[t]o the extent [] one asserts [] Krantz does not disclose 'at least one security policy including requirements that must be satisfied," it would have been obvious in view of Herrmann. Pet. at 65-66. But Petitioners' application of Herrmann continues to conflate authentication and auditing just as with Krantz. Petitioners argue "[c]hecking for anti-virus software would merely be an additional item for server 215 ("gatekeeper") to ***evaluate in the authentication process*** already disclosed by Krantz[.]" Pet. at 70.

[3] Notably, Petitioners do not argue that Herrmann teaches the "configure an access point in response to approval of the device by the gatekeeper" limitation.

Thus, Petitioners claim that Herrmann's "policy requiring that a specific virus protection program is operational on each client device that is connected to a network" would be evaluated through Krantz "authentication process," and that doing such would "merely be an additional item for server 215." Pet. at 66. Petitioners' conclusory assertion of the ease of including the separate auditing evaluation with the authentication process is contrary to the evidence. The '484 Patent expressly says: "The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol." EX1501, 14:1-3. The '484 Patent then provides a specific explanation for exactly how to do this complicated process. *See, e.g.*, EX1501, 14:42-45 ("The ECL calls the corresponding CF to perform authentication… If the SF receives a success response from the server EAPM… the SF changes to the audit state and calls GK to obtain audit requests to send back to the client. In this state, the SF returns specifically formatted audit requests to the ESL…"). None of this is suggested by Krantz or Herrmann, and this is clearly not simply a matter of "merely be an additional item" (Pet. at 66) to add to the authentication process.

Petitioners argue a POSITA would have modified Krantz based on the generalized notion that Krantz is "specifically focused on network authentication and security." Pet. at 66-67. Krantz, however, is limited to authentication and includes nothing about device auditing. EX2001, ¶¶ 57-59. Indeed, the lack of any

recognition in Krantz of auditing demonstrates the argument to merely be impermissible hindsight. *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1068 (Fed. Cir. 2018) (cautioning that hindsight "often overlooks that the genius of invention is often a combination of known elements which in hindsight seem preordained" and disparages looking to "what a skilled artisan would have been ***able*** to do, rather than what a skilled artisan would have been ***motivated*** to at the time of the invention.") (emphasis in original, internal citations omitted). Krantz's lack of recognition of security policy compliance highlights the smoke and mirrors of the Petition's reliance on Krantz's paragraph [0019] for Krantz's purported goal of "security." Petitioners even go so far as to rely on the '484 Patent for a motivation to combine by stating that "[t]he 484 Patent itself confirms that a POSITA would recognize the need for the server/authentication module of Krantz to check for up-to-date and approved antivirus programs." In so doing, Petitioner expressly rely on the patent to provide a roadmap for combining references, which is quintessential impermissible hindsight. *Ruiz v. AB Chance Company*, 357 F.3d 1270, 1275 (Fed. Cir. 2004).

VI. All Grounds: Neither Reference Constitutes Prior Art

The Board has previously found antedating prior art references is sufficient grounds for denying *inter partes* review institution. *LG Elecs., Inc. v. Wi-LAN Inc.*, No. IPR2018-00704, Paper No. 14 at 20 (P.T.A.B. Sept. 5, 2018) ("[W]e determine

that Patent Owner has provided sufficient evidence to antedate ZTE . . . [and therefore] Petitioner has not demonstrated a reasonable likelihood of prevailing[.]").

Neither Krantz nor Herrmann are prior art because the InfoExpress inventors conceived of the invention before the effective dates and exercised reasonably continuous diligence in reducing to the claimed inventions to practice.

A. Legal Standard

A reference is prior art only if filed before the date of "the invention by the [patent owner]." 35 U.S.C. § 102(e) (pre-AIA). *See, e.g.*, *Sequenom v. Leland Stanford Junior Univ.*, No. IPR2013-00390, at 5 (P.T.A.B. Nov. 25, 2014).

To antedate a reference, a Patent Owner must show that there was conception prior to the critical date and "reasonably continuous diligence" throughout the critical period from just before the effective date of the prior art until reduction to practice. *E.g., ATI Techs. v. Iancu*, 920 F.3d 1362, 1369 (Fed. Cir. 2019); *Tyco Healthcare Grp. v. Ethicon Endo-Surgery, Inc.*, 774 F.3d 968, 975 (Fed. Cir. 2014).

Under the reasonably continuous diligence standard, an inventor is not required to work on reducing the invention to practice every day during the critical period, and periods of inactivity within the critical period do not automatically vanquish a claim of reasonable diligence. *ATI*, 920 F.3d at 1369; *Monsanto Co. v. Mycogen Plant Sci., Inc.*, 261 F.3d 1356, 1369 (Fed. Cir. 2001); *Perfect Surgical Techniques, Inc. v. Olympus Am., Inc.*, 841 F.3d 1004, 1009 (Fed. Cir. 2016).

Additionally, an attorney's work preparing a patent application can demonstrate diligence. *Perfect Surgical*, 841 F.3d at 1009-1012; *Bey v. Kollonitsch*, 806 F.2d 1024, 1030 (Fed. Cir. 1986).

Inventor declarations submitted to establish conception and diligence must be corroborated. *Perfect Surgical*, 841 F.3d at 1007. The "rule of reason" analysis governs whether corroboration is sufficient to establish diligence. *Id.* at 1009. "A variety of activities may corroborate an inventor's testimony of reasonable diligence, and such corroborating evidence is considered 'as a whole.'" *Id.* at 1007-08 (quoting *Brown v. Barbacid*, 436 F.3d 1376, 1380 (Fed. Cir. 2006)). The patent owner need not corroborate every contested factual issue, but instead merely needs to produce sufficient independent circumstantial evidence to support the testimony. *Perfect Surgical*, 841 F.3d at 1009.

The purpose of diligence is to show that the invention was not abandoned, set aside, or unreasonably delayed, not to "scour the patent owner's corroborating evidence in search of intervals of time where the patent owner has failed to substantiate some sort of activity." *Id.*

B. The Inventors Conceived of the Claimed Inventions Prior to the Critical Dates of Both Krantz and Herrmann.

Petitioner asserts that Krantz has an effective date of December 6, 2002 (Pet. at 7) and Herrmann has an effective date of March 13, 2003.[4] *Id*. at 10. InfoExpress conceived of the claimed invention before that.

On November 14, 2002, the InfoExpress inventors had the "CyberGatekeeper LAN Based Policy Enforcement Engineering Specification" (EX2011: "LAN Engineering Specification") prepared demonstrating that the claimed inventions were conceived of at least as of that date. EX2012; EX2003 (Lum Declaration), ¶ 12. This conception is demonstrated in the claim chart mapping by Dr. Smith showing the LAN Engineering Specification mapped to the challenged claims as set forth in EX2009. EX2007.

Indeed, leading up to the November 14, 2002 LAN Engineering Specification, InfoExpress had started diligently working.

On October 7, 2002, inventor Stacey Lum told the InfoExpress team that:

> "All, It may be possible to use 802.1x to audit [enforce] a system rather than switching them between VLANs. There's an authentication specific component in 802.1x, so we might be able to use that instead of VLANs." EX2015; EX2016.

[4] Herrmann's provisional date is listed as December 2, 2002. Petitioners waived any right to establish this provisional date as the §102(e) date because they failed to submit, mention, or analyze its provisional filing in the Petition. *SAS Institute Inc. v. Iancu*, 138 S.Ct. 1348, 1355 (2018) (the petition must define the boundaries of the IPR); *Globus Med., Inc. v. Depuy Synthes Prods., LLC*, No. IPR2015-00107, at *3 (P.T.A.B. May 1, 2015). Notwithstanding, the Herrmann provisional date is still later in time than the November 14, 2002 conception of the claimed inventions and thus would not be prior art regardless.

This was groundbreaking because preexisting security technologies did not include the implementation of auditing support functionality over authentication protocols such as 802.1x. Mr. Lum and the InfoExpress team diligently worked in October 2002 and November 2002 to produce the LAN Engineering Specification of November 14, 2002. EX2021; EX2056; EX2061; EX2273; EX2274; EX2275; EX2342.

C. The Inventors Exercised Reasonably Continuous Diligence Up and Through Constructive Reduction to Practice.

Before and after the November 14, 2002 LAN Engineering Specification, InfoExpress exercised reasonably continuous diligence up and through at least the filing of U.S. Patent Application No. 60/513,080 on October 21, 2003. The filing of this application constitutes constructive reduction to practice of the claimed inventions. EX2007, EX2010.

The InfoExpress inventors, employees, and team members diligently pursued reducing the claimed invention to practice from conception until constructive reduction to practice on at least October 21, 2003. This diligence is shown by substantial InfoExpress evidence including:

i. emails (e.g., EX2015-EX2065; EX2067; EX2068; EX2071; EX2074-EX2200; EX2202-EX2271; EX2273; EX2274; EX2276-EX2283; EX2285; EX2287-EX2326; EX2331-EX2340; EX2342-EX2382; EX2384-EX2390; EX2395-EX2397; EX2399-EX2410);

ii. technical specifications and analyses (e.g., EX2011-EX2014; EX2066; EX2069; EX2070; EX2072; EX2073; EX2201; EX2275; EX2329; EX2330);

iii. source code (e.g., EX2113; EX2114; EX2121; EX2129; EX2138; EX2178; EX2191; EX2197; EX2206; EX2298; EX2303; EX2314; EX2339; EX2348; EX2352; EX2359; EX2364; EX2384; EX2399; EX2404; EX2405); and

iv. the inventor declaration of InfoExpress CEO Stacey Lum (EX2003).

As further detailed in the diligence calendar submitted herewith (EX2004), InfoExpress worked consistently to reduce the claimed invention to practice. This evidence leaves no doubt that the InfoExpress inventors conceived of and diligently pursued reduction to practice during the critical period. *See ATI*, 920 F.3d at 1373 (Court finding that Patent Owner's evidence did "not point to the remotest suggestion of abandonment or setting aside" where the Patent Owner provided a calendar demonstrating that designated activity on the majority of days in the diligence period, and a declaration summarizing various documents in support of diligence); *Monsanto*, 261 F.3d at 1369 (Court finding substantial diligence evidence where the Patent Owner identified record evidence showing activity multiple times per month during the critical period, and there was no reason to doubt that the activity was relevant in reducing the invention to practice).

December 2002:

- [redacted]

- See EX2003, ¶¶6-7, 30, 33, 37, 49 (Lum Declaration).

January 2003:

- [redacted]

- Mr. Lum spoke with eventual patent counsel to clear conflicts. EX2212.
- See EX2003, ¶¶6-7, 30, 33, 37, 49) (Lum Declaration).

February 2003:

- [redacted]

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- [redacted]
- *See* EX2003, ¶¶32-33, 38, 40-43, 50-51, 56-57 (Lum Declaration).

March 2003:

- [redacted]
- [redacted]

- See EX2003, ¶¶44, 52, 58 (Lum Declaration)

April 2003:

-

- See EX2003, ¶¶44, 52 (Lum Declaration).

May 2003:

-

- [redacted]

- See EX2003, ¶¶44-45, 52 (Lum Declaration).

June 2003:

- [redacted]

[redacted]

- See EX2003, ¶53 (Lum Declaration).

July 2003:

- [redacted]
  - [redacted]
  - [redacted]
- [redacted]
- *See* EX2003, ¶¶52, 59-61 (Lum Declaration).

August 2003

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]

- [redacted]

- *See* EX2003, ¶52 (Lum Declaration).

September 2003

- [redacted]

- *See* EX2003, ¶¶53, 62-63 (Lum Declaration).

October 2003

- [redacted]

- *See* EX2003, ¶¶14, 23, 25, 64-66 (Lum Declaration).

D. The Inventors Exercised Achieved a Constructive Reduction to Practice by the Filing of U.S. Provisional Patent Application Serial No. 60/513,080, Which Was Filed on October 21, 2003

As set forth in EX2010 and discussed by Prof. Smith (EX2007), the '080 Provisional provides written description support for the Challenged Claims in accordance with pre-A.I.A. 35 U.S.C. §§ 119(e) & 112, ¶ 1.

The evidence discussed above demonstrates diligence on the part of the inventors towards reducing the claimed invention to practice. *ATI*, 920 F.3d at 1374.

VII. Conclusion

For these reasons, Patent Owner respectfully requests the Board reject the Petition and not institute an *inter partes* review of the Challenged Claims.

Respectfully submitted,

Dated: July 24, 2024 Mailing address for all correspondence: Saul Ewing LLP Centre Square West 1500 Market Street, 38th Floor Philadelphia, PA 19102-2186	*/s/ Brian R. Michalek* Brian R. Michalek (Reg. No. 65,816) Saul Ewing LLP 161 North Clark Street, Suite 4200 Chicago, IL 60601 Tel: (312) 876-7151 brian.michalek@saul.com Joseph M. Kuo (Reg. No. 38,943) Saul Ewing LLP 161 North Clark Street, Suite 4200 Chicago, IL 60601 Tel: (312) 876-7151 joseph.kuo@saul.com Brian Landry (Reg. No. 62,074) Saul Ewing LLP 131 Dartmouth Street, Suite 501 Boston, MA 02116 Tel: (617) 912-0969 Brian.Landry@saul.com Counsel for Patent Owner

Certification of Word Count Under 37 C.F.R. § 42.6(d)

The undersigned hereby certifies that the foregoing complies with the type-volume limitation in 37 C.F.R. § 42.24(b)(1). According to the word-processing system's word count, the document contains 13,959 words, excluding the parts of the brief exempted by 37 C.F.R § 42.24(b).

Date: July 25, 2024

/Brian R. Landry/
Reg. No. 62,074

Certification of Service Under 37 C.F.R. § 42.6(e)(4)

The undersigned hereby certifies that the foregoing was served in its entirety by filing through the Patent Trial and Appeal Board P-TACTS, as well as providing a courtesy copy via e-mail to the attorneys of record.

Date: July 25, 2024

/Brian R. Landry/
Reg. No. 62,074

EXHIBIT X

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC. and FORTINET, INC.,
Petitioners,

v.

INFOEXPRESS INC.,
Patent Owner.

IPR2024-00677
U.S. Patent No. 8,578,444

PATENT OWNER PRELIMINARY RESPONSE

TABLE OF CONTENTS

PAGE

I. Introduction....1

II. The '444 Patent....1
- A. Date of Invention....1
- B. Person of Ordinary Skill in the Art (POSITA)....1
- C. Overview of the '444 Patent....2

III. Claim Construction....6

IV. Petitioners' References....6
- A. Krantz....6
- B. Herrmann....9

V. Krantz In Combination with Herrmann Fails to Render Obvious the Challenged Claims....11
- A. Neither Krantz Nor Herrmann Disclose "Applying A Security Policy That Includes At Least One Requirements Pertaining To The Audit Data And At Least One Requirement Pertaining To Authentication" (All Challenged Claims)....12
  - 1. Krantz....12
  - 2. Herrmann....17
- B. There Is No Motivation To Combine Krantz With Herrmann To Meet The "Security Policy … Pertaining to Audit Data" Limitation (All Challenged Claims)....18
- C. Neither Krantz Nor Herrmann Disclose "Applying The Security Policy Includes Configuring The Access Point (Claims 2-7 and 22)....21
- D. Claims 5-7 Are Not Obvious In View of Krantz With Herrmann....28
- E. Claim 22 Is Not Obvious In View of Krantz In Combination With Herrmann....29

VI. All Grounds: Neither Reference Constitutes Prior Art....29
- A. Legal Standard....30
- B. The Inventors Conceived of the Claimed Inventions Prior to the Critical Dates of Both Krantz and Herrmann....31

C. The Inventors Exercised Reasonably Continuous Diligence Up and Through Constructive Reduction to Practice. 33
D. The inventors exercised achieved a constructive reduction to practice by the filing of U.S. Provisional Patent Application Serial No. 60/513,080 was filed on October 21, 2003. 42

VII. Conclusion 42

TABLE OF AUTHORITIES

FEDERAL CASES

ATI Techs. v. Iancu, 920 F.3d 1362 (Fed. Cir. 2019) 30, 34, 42

Bey v. Kollonitsch, 806 F.2d 1024 (Fed. Cir. 1986) 30

Monsanto Co. v. Mycogen Plant Sci., Inc., 261 F.3d 1356 (Fed. Cir. 2001) 30, 34

Perfect Surgical Techniques, Inc. v. Olympus Am., Inc., 841 F.3d 1004 (Fed. Cir. 2016) 30, 31

Polaris Indus., Inc. v. Arctic Cat, Inc., 882 F.3d 1056 (Fed. Cir. 2018) 19, 20, 27

SAS Institute Inc. v. Iancu, 138 S.Ct. 1348 (2018) 31

FEDERAL STATUTES

37 C.F.R. § 42.6(d) 44

37 C.F.R. § 42.6(e)(4) 45

37 C.F.R § 42.24(b) 44

37 C.F.R. § 42.24(b)(1) 44

35 U.S.C. § 102(e) 30, 31

35 U.S.C. §§ 119(e) & 112, ¶ 1 42

STATE STATUTES

ECL 18

OTHER AUTHORITIES

Globus Med., Inc. v. Depuy Synthes Prods., LLC, No. IPR2015-00107 (P.T.A.B. May 1, 2015) 31

, https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485048062.htm 27, 28

https://www.portnox.com/cybersecurity-101/mschapv2/ 28

LG Elecs., Inc. v. Wi-LAN Inc., No. IPR2018-00704, Paper No. 14 (P.T.A.B. Sept. 5, 2018) 29

Petitioners' "Tag Headers" 25

report on February 10, 2003. EX2075 36

Sequenom v. Leland Stanford Junior Univ., No. IPR2013-00390 (P.T.A.B. Nov. 25, 2014) 30

U.S. Patent 8,578,444 .....passim

EXHIBIT LIST

Exhibit Number	Description
2001	Declaration of Dr. Eric Cole
2002	Curriculum Vitae of Dr. Eric Cole
2003	Declaration of Stacey C. Lum
2004	Diligence Calendar
2005	U.S. Provisional App. No. 60/505,582
2006	U.S. Provisional App. No. 60/513,080
2007	Declaration of Hugh Smith, Ph.D.
2008	Curriculum Vitae of Hugh Smith, Ph.D.
2009	Conception of the '444 Patent
2010	Constructive Reduction to Practice of the '444 Patent
2011	LAN Based Policy Enforcement Engineering Specification
2012	Metadata for Exhibit 2011
2013	CyberGatekeeper Policy Manager
2014	Metadata for Exhibit 2013
2015	Internal InfoExpress Correspondence
2016	Internal InfoExpress Correspondence
2017	Internal InfoExpress Correspondence
2018	Internal InfoExpress Correspondence
2019	Internal InfoExpress Correspondence
2020	Internal InfoExpress Correspondence
2021	Internal InfoExpress Correspondence
2022	Correspondence with Globe Tech
2023	Email attachment to Exhibit 2022
2024	Internal InfoExpress Correspondence
2025	Correspondence with Meetinghouse
2026	Draft Meetinghouse Agreement
2027	Internal InfoExpress Correspondence
2028	Draft Meetinghouse Agreement
2029	Internal InfoExpress Correspondence
2030	Draft Meetinghouse Agreement
2031	Draft Meetinghouse Agreement
2032	Internal InfoExpress Correspondence
2033	Draft Meetinghouse Agreement
2034	Draft Meetinghouse Agreement
2035	Draft Meetinghouse Agreement

Exhibit Number	Description
2036	Internal InfoExpress Correspondence
2037	Draft Meetinghouse Agreement
2038	Draft Meetinghouse Agreement
2039	Internal InfoExpress Correspondence
2040	Draft Meetinghouse Agreement
2041	Draft Meetinghouse Agreement
2042	Draft Meetinghouse Agreement
2043	Draft Meetinghouse Agreement
2044	Internal InfoExpress Correspondence
2045	Draft Meetinghouse Agreement
2046	Draft Meetinghouse Agreement
2047	Internal InfoExpress Correspondence
2048	Correspondence with Globe Tech
2049	Correspondence with Globe Tech
2050	Internal InfoExpress Correspondence
2051	Correspondence with Globe Tech
2052	Correspondence with Globe Tech
2053	Correspondence with Globe Tech
2054	Correspondence with Globe Tech
2055	Correspondence with Globe Tech
2056	Draft Globe Tech Agreement
2057	Draft Globe Tech Agreement
2058	Draft Globe Tech Agreement
2059	Draft Globe Tech Agreement
2060	Draft Globe Tech Agreement
2061	Draft Globe Tech Agreement
2062	Draft Globe Tech Agreement
2063	Correspondence with Globe Tech
2064	Draft Globe Tech Agreement
2065	Correspondence with Globe Tech
2066	Network Device Configuration API Engineering Specification
2067	Correspondence with Globe Tech
2068	Correspondence with Globe Tech
2069	Network Device Configuration API Engineering Specification
2070	Network Device Configuration API Engineering Specification
2071	Correspondence with Globe Tech
2072	Network Device Configuration API Engineering Specification

Exhibit Number	Description
2073	Network Device Configuration API Engineering Specification
2074	Correspondence with Globe Tech
2075	Correspondence with Globe Tech
2076	Correspondence with Globe Tech
2077	Correspondence with Globe Tech
2078	Correspondence with Globe Tech
2079	Email attachment to Exhibit 2078
2080	Correspondence with Globe Tech
2081	Correspondence with Globe Tech
2082	Correspondence with Globe Tech
2083	Correspondence with Globe Tech
2084	Correspondence with Globe Tech
2085	Correspondence with Globe Tech
2086	Correspondence with Globe Tech
2087	Correspondence with Globe Tech
2088	Correspondence with Globe Tech
2089	Correspondence with Globe Tech
2090	Correspondence with Globe Tech
2091	Correspondence with Globe Tech
2092	Correspondence with Globe Tech
2093	Correspondence with Globe Tech
2094	Correspondence with Globe Tech
2095	Correspondence with Globe Tech
2096	Correspondence with Globe Tech
2097	Correspondence with Globe Tech
2098	Correspondence with Globe Tech
2099	Correspondence with Globe Tech
2100	Correspondence with Globe Tech
2101	Correspondence with Globe Tech
2102	Correspondence with Globe Tech
2103	Correspondence with Globe Tech
2104	Correspondence with Globe Tech
2105	Correspondence with Globe Tech
2106	Correspondence with Globe Tech
2107	Correspondence with Globe Tech
2108	Internal InfoExpress Correspondence
2109	Correspondence with Globe Tech

Exhibit Number	Description
2110	Correspondence with Globe Tech
2111	Correspondence with Globe Tech
2112	Correspondence with Globe Tech
2113	Internal InfoExpress Correspondence
2114	Correspondence with Globe Tech
2115	Email attachment to Exhibit 2114
2116	Correspondence with Globe Tech
2117	Internal InfoExpress Correspondence
2118	Correspondence with Globe Tech
2119	Correspondence with Globe Tech
2120	Correspondence with Globe Tech
2121	Correspondence with Globe Tech
2122	Correspondence with Globe Tech
2123	Correspondence with J. Ong
2124	Correspondence with Globe Tech
2125	Correspondence with Globe Tech
2126	Correspondence with Globe Tech
2127	Correspondence with Globe Tech
2128	Correspondence with Globe Tech
2129	Correspondence with Globe Tech
2130	Correspondence with Globe Tech
2131	Correspondence with Globe Tech
2132	Correspondence with Globe Tech
2133	Correspondence with Globe Tech
2134	Correspondence with Globe Tech
2135	Correspondence with Globe Tech
2136	Correspondence with Globe Tech
2137	Correspondence with Globe Tech
2138	Correspondence with Globe Tech
2139	Correspondence with Globe Tech
2140	Correspondence with Globe Tech
2141	Correspondence with Globe Tech
2142	Correspondence with Globe Tech
2143	Correspondence with Globe Tech
2144	Correspondence with Globe Tech
2145	Correspondence with Globe Tech
2146	Correspondence with Globe Tech

Exhibit Number	Description
2147	Correspondence with Globe Tech
2148	Correspondence with J. Ong
2149	Correspondence with Globe Tech
2150	Correspondence with J. Ong
2151	Correspondence with Globe Tech
2152	Correspondence with J. Ong
2153	Correspondence with Globe Tech
2154	Correspondence with Globe Tech
2155	Correspondence with Globe Tech
2156	Correspondence with Globe Tech
2157	Correspondence with Globe Tech
2158	Correspondence with Globe Tech
2159	Correspondence with Globe Tech
2160	Correspondence with Globe Tech
2161	Correspondence with J. Ong
2162	Correspondence with Globe Tech
2163	Correspondence with C. Tsai
2164	Correspondence with Globe Tech
2165	Correspondence with Globe Tech
2166	Correspondence with Globe Tech
2167	Correspondence with Globe Tech
2168	Correspondence with Globe Tech
2169	Correspondence with Globe Tech
2170	Correspondence with Globe Tech
2171	Correspondence with Globe Tech
2172	Correspondence with Globe Tech
2173	Correspondence with Globe Tech
2174	Correspondence with Globe Tech
2175	Correspondence with Globe Tech
2176	Correspondence with Globe Tech
2177	Correspondence with Globe Tech
2178	Correspondence with Globe Tech
2179	Correspondence with Globe Tech
2180	Correspondence with Globe Tech
2181	Correspondence with Globe Tech
2182	Correspondence with Globe Tech
2183	Correspondence with Globe Tech

Exhibit Number	Description
2184	Correspondence with Globe Tech
2185	Correspondence with Globe Tech
2186	Correspondence with Globe Tech
2187	Correspondence with Globe Tech
2188	Correspondence with Globe Tech
2189	Correspondence with C. Tsai
2190	Correspondence with Globe Tech
2191	Correspondence with Globe Tech
2192	Correspondence with Globe Tech
2193	Correspondence with Globe Tech
2194	Correspondence with Globe Tech
2195	Correspondence with Globe Tech
2196	Correspondence with Globe Tech
2197	Correspondence with Globe Tech
2198	Correspondence with J. Ong
2199	Correspondence with C. Tsai
2200	Correspondence with J. Ong
2201	Cisco Switch Feature Support Matrix
2202	Correspondence with M. Banin
2203	Correspondence with A. Lee
2204	Correspondence with M. Banin
2205	Correspondence with M. Banin
2206	Correspondence with M. Banin
2207	Correspondence with M. Banin
2208	Correspondence with M. Banin
2209	Correspondence with M. Banin
2210	Correspondence with M. Banin
2211	Correspondence with patent counsel
2212	Correspondence with patent counsel
2213	Correspondence with patent counsel
2214	Correspondence with patent counsel
2215	Correspondence with patent counsel
2216	Correspondence with patent counsel
2217	Correspondence with patent counsel
2218	Correspondence with patent counsel
2219	Correspondence with patent counsel
2220	Correspondence with patent counsel

Exhibit Number	Description
2221	Correspondence with patent counsel
2222	Correspondence with patent counsel
2223	Correspondence with patent counsel
2224	Correspondence with patent counsel
2225	Correspondence with patent counsel
2226	Correspondence with patent counsel
2227	Correspondence with patent counsel
2228	Correspondence with patent counsel
2229	Correspondence with patent counsel
2230	Correspondence with patent counsel
2231	Correspondence with patent counsel
2232	Correspondence with patent counsel
2233	Correspondence with patent counsel
2234	Correspondence with patent counsel
2235	Correspondence with patent counsel
2236	Correspondence with patent counsel
2237	Correspondence with patent counsel
2238	Correspondence with patent counsel
2239	Correspondence with patent counsel
2240	Correspondence with patent counsel
2241	Correspondence with patent counsel
2242	Correspondence with patent counsel
2243	Correspondence with patent counsel
2244	Correspondence with patent counsel
2245	Correspondence with patent counsel
2246	Correspondence with patent counsel
2247	Correspondence with patent counsel
2248	Correspondence with patent counsel
2249	Correspondence with patent counsel
2250	Correspondence with patent counsel
2251	Correspondence with patent counsel
2252	Correspondence with patent counsel
2253	Correspondence with patent counsel
2254	Correspondence with patent counsel
2255	Correspondence with patent counsel
2256	Correspondence with patent counsel
2257	Correspondence with patent counsel

Exhibit Number	Description
2258	Correspondence with patent counsel
2259	Correspondence with patent counsel
2260	Correspondence between S. Lum and A. Lee
2261	Correspondence between S. Lum and A. Lee
2262	Correspondence with patent counsel
2263	Correspondence with patent counsel
2264	Correspondence with patent counsel
2265	Correspondence with patent counsel
2266	Correspondence with patent counsel
2267	Correspondence with patent counsel
2268	Correspondence with patent counsel
2269	Correspondence with patent counsel
2270	Correspondence with patent counsel
2271	Correspondence with patent counsel
2272	Intentionally Left Blank
2273	Correspondence between S. Lum, J. Ong, C. Tsai and A. Lee
2274	Correspondence between S. Lum, C. Tsai and A. Lee
2275	Internal Notes
2276	Correspondence between C. Tsai, J. Ong and S. Lum
2277	Correspondence between C. Tsai, J. Ong and S. Lum
2278	Correspondence between C. Tsai, J. Ong and S. Lum
2279	Correspondence between C. Tsai, J. Ong and S. Lum
2280	Correspondence between C. Tsai and S. Lum
2281	Correspondence between T. Nakano and S. Lum
2282	Draft Meetinghouse Agreement
2283	Correspondence with Globe Tech
2284	Intentionally Left Blank
2285	Correspondence between S. Lum and corporate counsel
2286	Intentionally Left Blank
2287	Correspondence with Globe Tech
2288	Correspondence with Globe Tech
2289	Correspondence with Globe Tech
2290	Correspondence with Globe Tech
2291	Correspondence with Globe Tech
2292	Correspondence with Globe Tech
2293	Correspondence with Globe Tech
2294	Correspondence with Globe Tech

Exhibit Number	Description
2295	Correspondence with Globe Tech
2296	Correspondence with Globe Tech
2297	Correspondence with Globe Tech
2298	Correspondence between S. Lum and J. Ong
2299	Correspondence between S. Lum and J. Ong
2300	Correspondence with Globe Tech
2301	Correspondence with Globe Tech
2302	Correspondence between M. Banin and S. Lum
2303	Correspondence with Globe Tech
2304	Correspondence with Globe Tech
2305	Correspondence with Globe Tech
2306	Correspondence with Globe Tech
2307	Correspondence with Globe Tech
2308	Correspondence with Globe Tech
2309	Correspondence with Globe Tech
2310	Correspondence with Globe Tech
2311	Correspondence with Globe Tech
2312	Correspondence with Globe Tech
2313	Correspondence with Globe Tech
2314	Correspondence with Globe Tech
2315	Correspondence with Globe Tech
2316	Correspondence with Globe Tech
2317	Correspondence with Globe Tech
2318	Correspondence with Globe Tech
2319	Correspondence with Globe Tech
2320	Correspondence with Globe Tech
2321	Correspondence with Globe Tech
2322	Correspondence with Globe Tech
2323	Correspondence with Globe Tech
2324	Correspondence with Globe Tech
2325	Correspondence with Globe Tech
2326	Correspondence with Globe Tech
2327	Draft Patent Application
2328	Draft Patent Application
2329	CyberGatekeeper Enforcement Modes
2330	CyberGatekeeper Enforcement Modes
2331	Correspondence with Globe Tech

Exhibit Number	Description
2332	Correspondence with Globe Tech
2333	Correspondence with Globe Tech
2334	Correspondence with Globe Tech
2335	Correspondence with Globe Tech
2336	Correspondence with Globe Tech
2337	Correspondence with Globe Tech
2338	Correspondence with Globe Tech
2339	Correspondence with Globe Tech
2340	Internal InfoExpress Correspondence
2341	Intentionally left blank
2342	Internal InfoExpress Correspondence
2343	Correspondence with Globe Tech
2344	Correspondence with Globe Tech
2345	Correspondence with Globe Tech
2346	Correspondence with Globe Tech
2347	Correspondence with Globe Tech
2348	Correspondence with Globe Tech
2349	Correspondence with Globe Tech
2350	Correspondence with Globe Tech
2351	Correspondence with Globe Tech
2352	Correspondence with Globe Tech
2353	Correspondence with Globe Tech
2354	Correspondence with Globe Tech
2355	Correspondence with Globe Tech
2356	Correspondence with Globe Tech
2357	Correspondence with Globe Tech
2358	Correspondence with Globe Tech
2359	Correspondence with Globe Tech
2360	Correspondence with Globe Tech
2361	Correspondence with Globe Tech
2362	Correspondence with Globe Tech
2363	Correspondence with Globe Tech
2364	Correspondence with Globe Tech
2365	Correspondence with Globe Tech
2366	Correspondence with Globe Tech
2367	Correspondence with Globe Tech
2368	Correspondence with Globe Tech

Exhibit Number	Description
2369	Correspondence with Globe Tech
2370	Correspondence with Globe Tech
2371	Correspondence with Globe Tech
2372	Correspondence with Globe Tech
2373	Correspondence with Globe Tech
2374	Correspondence with Globe Tech
2375	Correspondence with Globe Tech
2376	Correspondence with Globe Tech
2377	Correspondence with Globe Tech
2378	Correspondence with Globe Tech
2379	Correspondence with Globe Tech
2380	Correspondence with Globe Tech
2381	Correspondence with Globe Tech
2382	Correspondence with Globe Tech
2383	Intentionally left blank
2384	Correspondence with Globe Tech
2385	Correspondence with Globe Tech
2386	Internal InfoExpress Correspondence
2387	Correspondence with Globe Tech
2388	Correspondence with Globe Tech
2389	Internal InfoExpress Correspondence
2390	Correspondence with Globe Tech
2391	Intentionally left blank
2392	Intentionally left blank
2393	Intentionally left blank
2394	Intentionally left blank
2395	Correspondence with Globe Tech
2396	Internal InfoExpress Correspondence
2397	Correspondence with Globe Tech
2398	Intentionally left blank
2399	Correspondence with Globe Tech
2400	Correspondence with Globe Tech
2401	Correspondence with Globe Tech
2402	Correspondence with Globe Tech
2403	Correspondence with Globe Tech
2404	Correspondence with Globe Tech
2405	Correspondence with Globe Tech

Exhibit Number	Description
2406	Correspondence with Globe Tech
2407	Correspondence with Globe Tech
2408	Correspondence with Globe Tech
2409	Correspondence with Globe Tech
2410	Correspondence with Globe Tech

I. Introduction

Patent Owner InfoExpress, Inc. submits this Patent Owner Preliminary Response related to claims 1-7, 10, 12, 17, and 22 (the "Challenged Claims") of U.S. Patent 8,578,444 (the '444 Patent"). The Board should reject the Petition and not institute an IPR because the Grounds and the art relied upon fail to render any of the Challenged Claims unpatentable. The art fails to render obvious all of the limitations of the Challenged Claims, and a POSITA would not have been motivated to combine the references as argued by Petitioners. Moreover, the art relied on does not qualify as prior art.

II. The '444 Patent

A. Date of Invention

For the reasons discussed in Section VII below, the date of invention for each of the Challenged Claims is no later than December 2, 2002.

B. Person of Ordinary Skill in the Art (POSITA)

A POSITA at the time of the invention would have had a working knowledge of computer network security art. A POSITA would have had a bachelor's degree in computer science, computer engineering, or electrical engineering and at least three years of experience in networking operating systems and cybersecurity, or a person with a master's degree in one of the foregoing and at least two years of experience in the aforementioned fields.

C. Overview of the '444 Patent

The '444 Patent is directed to a novel and seminal approach to a security solution for controlling access to a protected network. Before Patent Owner's inventions, network security required a "gatekeeper" placed directly between each client, i.e., user, and the network. EX1201, Fig. 1, 2:39-47; EX2001, ¶¶ 44-46. But as the '444 Patent further explains, access control further required evaluation of each accessing device's hardware and software, *e.g.*, virus protection and operating systems, before the gatekeeper granted such access—thus consuming substantial network resources and creating bottlenecks. EX1201, 2:34-45.

Exemplary prior art architecture is shown in annotated FIG. 1.

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 1097 of 1144
INFOEXPRESS, INC. - EX2572

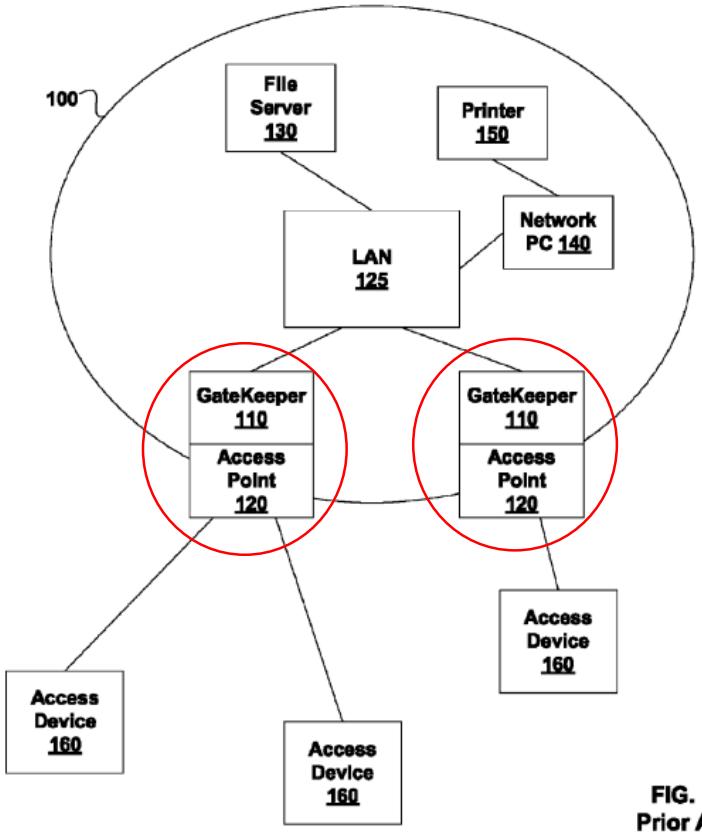


FIG. 1
Prior Art

The network 100 included two Gatekeepers 110, each associated with a different Access Point 120. With corporate networks including many access points, the "use of one instance of GateKeeper 110 to support numerous instances of Access Device 160 is limited by bandwidth and required sophistication (e.g., cost) of GateKeeper 110." EX1201, 2:39-42. The gatekeeper then becomes a limiting bottleneck on the system's bandwidth. *Id.*, 2:42-45.

The '444 Patent addressed this previously unidentified problem with a new approach, relieving computer resources through configuring an access point after clearing a device as authorized and satisfying security policies to access the

computer network. A disclosed example shows a protected network including a restricted subset with a gatekeeper and one or more less-restricted subsets.

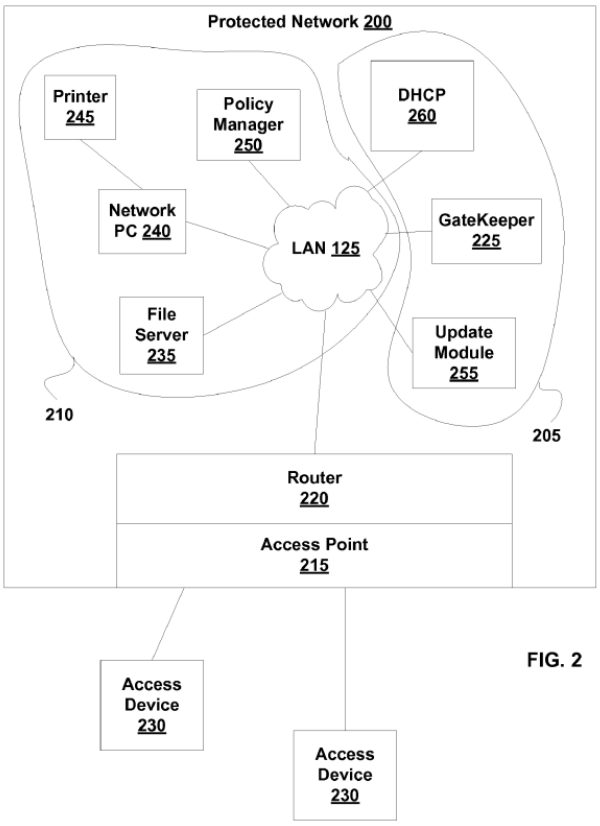


FIG. 2

EX1201, Fig. 2. Before a device can access a less-restricted subset 210, its request is first passed to the restricted subset (205). EX1201, 2:58-60, 5:38-40. A gatekeeper in the restricted subset checks whether the device is authentic (it is what it purports to be) and satisfies security policies. If so, the device is granted access to a less-restricted subset of the protected network. EX1201, 2:60-64. Regarding security policies, the patent teaches an agent on the device to receive requests for and to send audit data pertaining to the device so the gatekeeper can apply the security policy to

the device. See, EX1201, 11:60-61 ("Obtain Audit Data Step 450 is facilitated by an agent running on Access Device 230.")

Another feature of the patent is that rather than require all device access requests to pass through the gatekeeper (a previously unidentified shortcoming), the access point itself is configured based on user authentication and device compliance with security policies. The Detailed Description explains this.

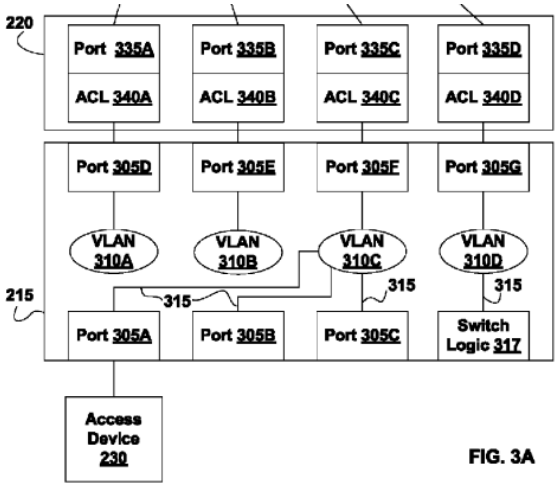


FIG. 3A

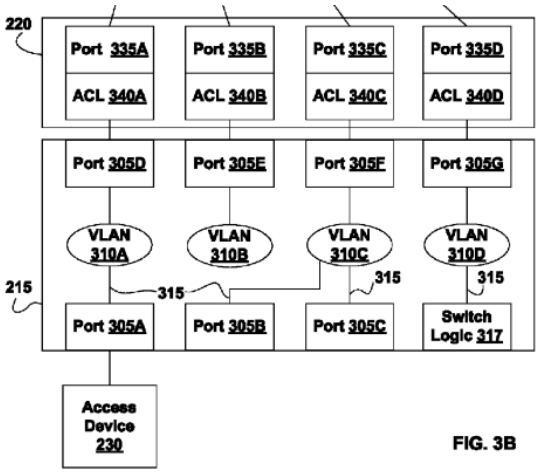


FIG. 3B

> Switch Logic 317 is configured for configuring and reconfiguring members of Ports 305A-305G responsive to received commands. For example, by receiving an appropriate command, Switch Logic 317 is configured to reconfigure Port 305A to be associated with VLAN 310A, as illustrated in FIG. 3B below. In this configuration, data received at Port 305A is directed to Port 305D via VLAN 310A, rather than to Port 305F.

EX1201, 8:25-32.

By configuring the access point after qualifying the access device for authentication and device security policy compliance, the device access the less-restricted subset

without going through the gatekeeper. Thus, substantial network traffic does not need to pass through the gatekeeper.

III. Claim Construction

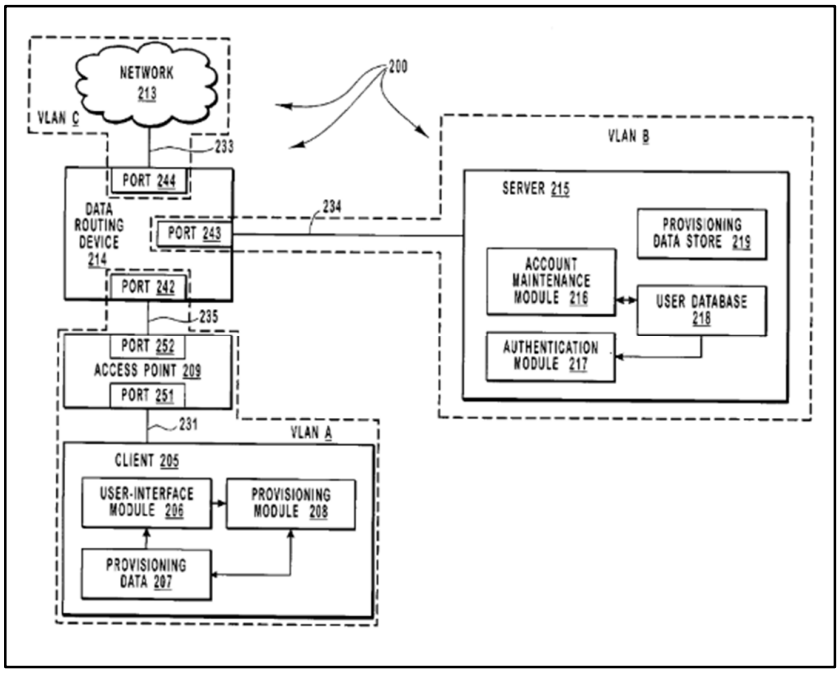
Petitioners assert claims should be given their ordinary and customary meaning as understood by a POSITA, and contends the Board need not expressly construe the claim terms. Pet. at 7. Patent Owner contends the claims should be given their plain meaning in the context of the intrinsic evidence, which is explained below in the context of the purported prior art.

IV. Petitioners' References

Petitioners' references, Krantz and Herrmann, are not prior art (discussed herein). Krantz and Herrmann are also different from the Challenged Claims, and merely illustrate network security approaches improved upon by the patent.

A. Krantz

Petitioners' primary reference is Krantz which details "[a] computer system attempts to authenticate with a server to gain authorization to access a first network." EX1205, Abstract.



A server includes the functionality to authorize clients to access a second network (e.g., the Internet). The server can be located on a first network that is separate from the second network or can be located on the second network. A client sends credentials to the server to attempt to authenticate with the server. Based on the credentials, the server may authorize the client for at least partial access to the second network and/or may deny access to the second network and authorize the client for at least partial to access to the first network. The server can be a Remote Authentication Dial-In User Service ("RADIUS") server that is located on the first network. Clients can be provided partial access to the first or second network at least for the purposes of authenticating with the server and downloading provisioning files used to gain full access to the second network. Thus, computer systems that are not currently able to access resources located on the second network may be able to electronically download provisioning files for gaining access to those resources.

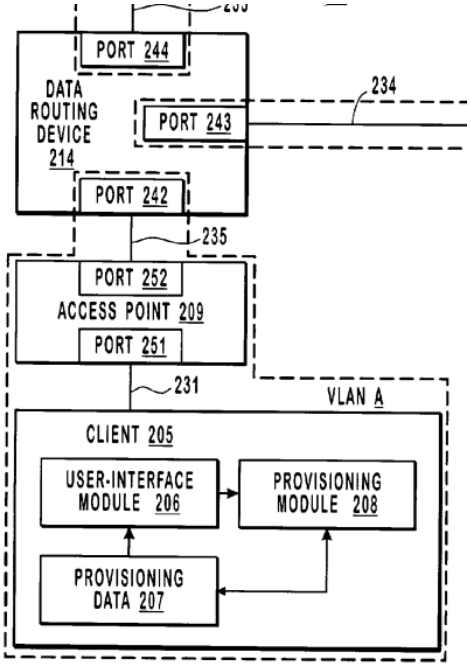
EX1205, [0016].

Regarding authentication of clients so as to access a network, Krantz teaches:

> In these embodiments, the server (based at least in part on received credentials) may authorize the client for at least partial access to the single network, such as, for example, by authorizing client access to selected computer systems or modules on the single network.
>
> Sending credentials can include sending an Extensible Authentication Protocol ("EAP") Response/Identity message from the client to the server. If the client is attempting to connect to a network via an access point, the EAP Response/Identity message may be encapsulated within some other type of message that can be transferred through the access point. In VLAN embodiments, the access point can insert a Tag Header into the encapsulating message to indicate to a data routing device that the encapsulating message is to be transferred to the first network. The access point may also be configured to block communications from the client that use protocols other than EAP and 802.1X.
>
> When credentials are sent to server 215, authentication module 217 can receive the credentials (e.g., user-identifier and password) and compare the credentials to entries in user database 218. If credential information matches an entry in user database 218, the identity of a user is authenticated (i.e., server 215 believes that the user represented by the user-identifier is the user who entered the credential information). If an authenticated user of client 205 is authorized to access resources located on VLAN C (e.g., the user is up to date on payments for their account), client 205 can then be authorized to access resources located on VLAN C.

EX1205, [0017]-[0018], [0076]. As Krantz explains, authentication merely checks whether the identification credentials match those in a database. Absent from Krantz is any discussion of auditing the device for compliance with security policy for the device. EX2001, ¶¶49, 58. Also absent is an agent on the device to receive requests for device information to be provided to a gatekeeper.

In the excerpted portion of Krantz Fig. 2 below, a client communicates through port 251 of access point 209, which then sends data to data routing device 214 via port 252. Data routing device directs data through ports 244 or 243.



EX1205, Fig. 2.

Krantz does not teach configuring any port of the access point 209 after applying a security policy to a device's audit data. EX2001, ¶¶57-58. Instead, all data pass ports 251 and 252 and then pass to the data routing device.

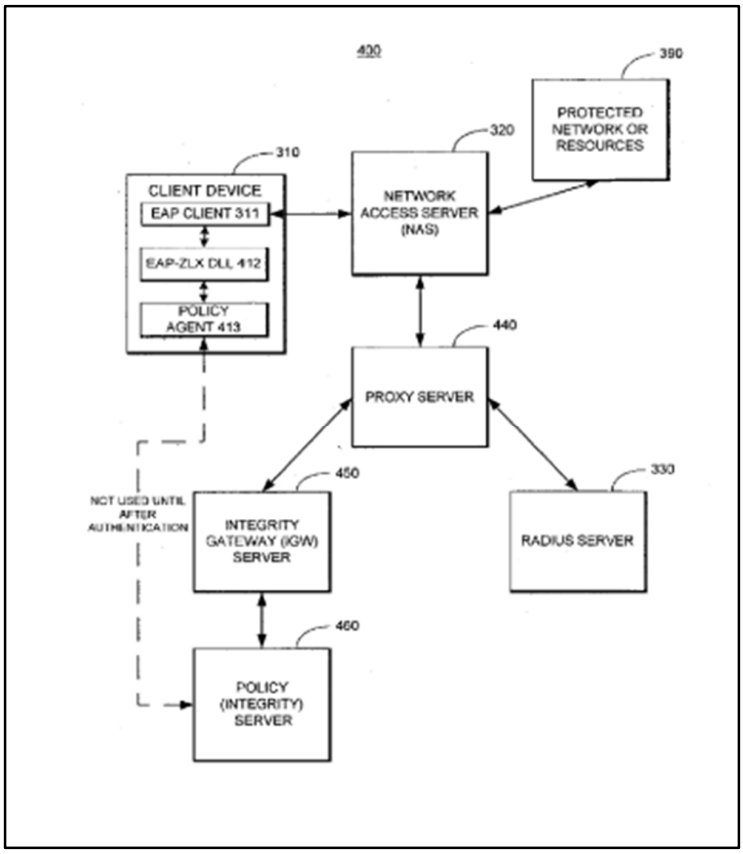
B. Herrmann

Petitioners cite to Herrmann in Ground 2 in combination with Krantz. Herrmann describes a system as follows:

> A system and methodology for policy enforcement during authentication of a client device for access to a network is described. A first authentication module establishes a session with a client device

> requesting network access for collecting information from the client device and determining whether to authenticate the client device for access to the network based, at least in part, upon the collected information. A second authentication module participates in the session with the client device for supplemental authentication of the client device for access to the network. The supplemental authentication of the client device is based, at least in part, upon the collected information and a policy required as a condition for network access.

EX1206, Abstract; EX2001, ¶¶51-53. Petitioners rely on Herrmann for an agent on a device to determine compliance of the device's software, e.g., virus software. Like the prior art discussed in the '444 Patent, Herrmann utilizes servers between the client and the protected network such that all attempts to access the network are first checked for device-based security policy compliance by at least a Network Access Server (NAS), and face bottleneck problems. EX2001, ¶¶53, 60.



EX1006, Fig. 1, *compare id. to* EX1201, Fig. 2.

V. Krantz In Combination with Herrmann Fails to Render Obvious the Challenged Claims

The Petition relies on Krantz alone as its base reference for several of the claimed limitations. With the limitations below related to an agent on the device for receiving a request for audit data and obtaining the audit data from the device, the Petition cherry picks portions of Herrmann.

[1.3] sending a request for audit data to an agent running on the device

[1.4] receiving the audit data at a gatekeeper configured to control access to a network, from the agent, the audit data pertaining to the device and having been obtained by the agent

> [1.5] applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication, the applying of the security policy taking place under control of the gatekeeper

The Petition fails to show how either reference—alone or in combination—meets several "security policy" limitations requiring both "audit data" and "authentication." Further, the arguments for the motivation to combine isolated teachings from Herrmann with Krantz do not pass muster. Accordingly, institution should be denied

A. Neither Krantz Nor Herrmann Disclose "Applying A Security Policy That Includes At Least One Requirements Pertaining To The Audit Data And At Least One Requirement Pertaining To Authentication" (All Challenged Claims)

The Challenged Claims recite "applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to authentication…." This limitation clearly distinguishes between "audit data" and "authentication." Yet, the Petition fails to show any single reference where a "security policy" includes both "audit data" and "authentication."

1. Krantz

Krantz teaches authentication, but not "audit data." Petitioners improperly conflate "audit data" and "authentication" to mean the same thing. Here, Petitioners assert Krantz's "user-identifier[s] and password[s]" are both "audit data" and "authentication."

message that can be transferred through the access point." Ex.1205, [0018]. Other "*audit data*" provided by Krantz's "*device*" may include, for example, "user-identifier[s] and password[s]." Ex.1205, [0076]. Krantz further explains that

Pet. at 21

Krantz discloses:

> When credentials are sent to server 215, authentication module 217 can receive the credentials **(e.g., user-identifier and password)** and compare the credentials ["*apply[ing] a security policy*"] to entries in **user database** 218. If credential information matches … **the identity of a user is authenticated** (server 215 believes that the user represented by the user-identifier is the user who entered the credential information) ["*that includes at least on requirement pertaining to authentication*"]. If an

Pet. at 59

But this would render the claim meaningless.[1]

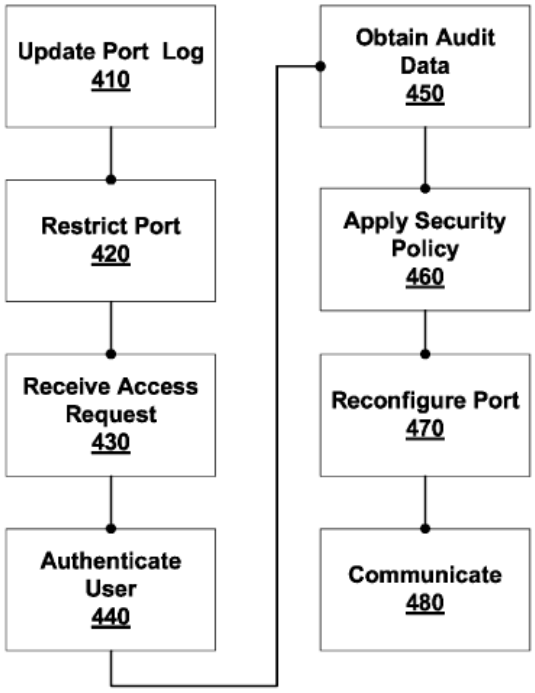
The patent explains that "audit data pertaining to a device" is data about the device's software and/or hardware necessary to comply with the security policy.

[1] Despite the distinction between authentication and audit data, Petitioners mix and match authentication and audit data throughout their Petition. In particular, for the limitation "sending a request for audit data to an agent running on the device," the Petition incorporates the discussion related to element [1.1] directed to "performing an authentication." Pet. at 31 ("As discussed for claim [1.1], Krantz discloses a method for 'auditing a device.'")

EX1201, 11:48-59. The '444 Patent further provides examples of types of "audit data pertaining to a device" include: "operating system status (version, updates, etc.), antivirus software status, information concerning devices connected to Access Device 230, Windows registry information, MAC address, IP addresses, cookies, status of applications executing on Access Device 230." *See id.*

Authentication is different. The patent describes "authentication" as identifying or authorization information, e.g., "requiring the user to enter a username and password…" *Id.*, 1:39-40. Authentication is different from the claimed "audit data pertaining to a device." Indeed, the claims recite authentication and auditing separately. *See e.g.* Claim 1 ("… performing an authentication using an EAP protocol" and "receiving the audit data… the audit data pertaining to the device…").

Fig. 4 further establishes authentication ("Authenticate User 440)" and audit data ("Obtain Audit Data 450") are distinct elements.



EX1201, Fig. 4

Yet, Krantz only discloses user authentication:

- "Krantz discloses that . . . '**authentication module 217** can receive the credentials (e.g. user-identifier and password) . . . and compare the credentials to entries in the user database 218.'" Pet. at 55 (citing EX1205, [0076]).
- "If an **authenticated user** of client 205 is authorized to access resources…" EX1205, [0076] (cited in Pet. at 55).
- "A presented user-interface can be used to receive user-entered information (e.g., user-identifier, password, name, address, credit card information, etc.) from a user at client 205." Pet. at 40-41 (citing EX1205, [0104]).
- "If credentials do not authorize full access to the second network (e.g., credentials cannot be **authenticated**, credentials are guest credentials, or an **authenticated user is not authorized**) . . ." EX1205, [0019].

Further, the Petition relies on purported disclosures from Krantz that pertain only to authentication. EX2001, ¶49; *see also* Pet. § VIII.A.1.ii. For example, Petitioners argue:

> [S]ending credentials can include sending an Extensible Authentication Protocol ("EAP") Response/Identity message from the client to the servers ['performing an authentication using an EAP protocol from the device'].

Pet. at 24-25 (quoting EX1205, [0018]) (quotation marks and emphasis omitted).

The Petition further references Krantz's disclosures of "EAP-messages," "EAP-Response/Identity message within an EAP-RADIUS message," "EAP-MSChap V2," and "EAP-TLS and EAP-MSCHAP V2." Pet. at 26-28. Again, these disclosures are only for authentication. *See* EX2001, ¶¶55-56.

Krantz's authentication disclosures do not pass muster. Indeed, the patent explains there are disadvantages to "reliance on mere user authentication" including the lack of any assurance that the device meets network security policies. *See* EX1201, 1:48-51.

Because Krantz does not disclose "audit data pertaining to a device," it also fails to disclose many of the other limitations of the Challenged Claims including: "A method of auditing a device" (all claims); "sending a request for audit data to an agent…." (all claims), "receiving the audit data…" (all claims).

2. Herrmann

The Petition relies on Herrmann only for an agent on a device. See Pet. at 50. Thus, it is not relevant to the "applying a security policy" limitation. Even if it was, Petitioners application of Herrmann continues to conflate authentication and auditing just like in Krantz. Petitioners argue:

- A POSITA would recognize that checking for anti-virus software would simply be an additional item for authentication module 217 (of server 215 to check in the authentication process…" Pet. at 14.

- A POSITA would have understood that checking for anti-virus software would merely be an additional item for server 215 ("*gatekeeper")* to check in the authentication process…" Pet. at 43.

- "Krantz's authentication module, which compares credentials of a user against a database (e.g., user-identifier and password), as modified by Herrmann, would also check for approved antivirus programs." Pet. at 15.

Thus, Petitioners claim Herrmann's supposed "audit data" would be evaluated through Krantz "authentication process"; not the audit process which is a separate claim element.

The claims, however, require "applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to authentication." Thus—even with Herrmann—Petitioners continue to conflate two different evaluations required in the Challenged Claims for two different features of the claimed system and fail to disclose this limitation.

B. There Is No Motivation To Combine Krantz With Herrmann To Meet The "Security Policy … Pertaining to Audit Data" Limitation (All Challenged Claims)

The claims require: "a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication… " But, Krantz only discloses authentication; not audit data. EX2001, ¶59. Further, the Petition only relies on Herrmann for a combination reference that runs an agent on a device. Pet. at 50.

Petitioners claim "[a] POSITA would have understood that checking for anti-virus software would merely be an additional item for server 215 ("*gatekeeper")* to check in the authentication process…" Pet. at 43. The intrinsic evidence says otherwise:

> The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol.

EX1201, 14:11-13.

This is aligned with the claims which recite "performing an authentication using an EAP protocol… to an access point configured to use an 802.1x protocol." The patent then explains how to do this complicated process. *See, e.g.*, EX1201, 14:53-65 ("The ECL calls the corresponding CF to perform authentication… If the SF receives a success response from the server EAPM… the SF changes to the audit state and calls GK to obtain audit requests to send back to the client. In this state, the SF returns

specifically formatted audit requests to the ESL…"). None of this is suggested by Krantz or Herrmann, and this is clearly not simply a matter of "merely be an additional item" to add to the authentication process.

Notwithstanding the patent's explanation that such a combination "is complicated and not an obvious variation," Petitioners argue a POSITA would have modified Krantz because it is "focused on network authentication and security." Pet. at 82 (citing to EX1205 (Abstract). Krantz's Abstract, like the rest of Krantz, is limited to authentication, and includes nothing about device auditing. EX2001, ¶¶49, 57-59. The lack of any recognition in Krantz of security policy compliance by a device further demonstrates the argument to merely be impermissible hindsight. *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1068 (Fed. Cir. 2018) (cautioning that hindsight "often overlooks that the genius of invention is often a combination of known elements which in hindsight seem preordained" and disparages looking to "what a skilled artisan would have been ***able*** to do, rather than what a skilled artisan would have been ***motivated*** to at the time of the invention.") (emphasis in original, internal quotations and citations omitted).

Further, the Petition argues motivation to combine on the claim that the "two stated goals of Krantz involve automation and security." Pet. at 35 (citing Krantz paragraphs [0014] and [0019]). Paragraph [0014] merely states it would be advantageous to increase "the level of automation when provisioning and

configuring a computer system to access a network." Automation has no bearing on whether a POSITA would incorporate an agent on a device for function related to audit data pertaining to the device. *See* EX2001, ¶49. The lack of any recognition in Krantz of security policy compliance by a device demonstrates the argument to merely be impermissible hindsight. See *Polaris*, 882 F.3d at 1068.

This lack of any recognition in Krantz to a "security policy" that includes "audit data" highlights the smoke and mirrors of the Petition's reliance on Krantz's paragraph [0019] and purported goal of "security." Krantz's goal of "security" only relates to user authentication and does not provide a reason to incorporate the agent for retrieving audit data pertaining to a device for security policy compliance evaluation of the device software and hardware. EX2001, ¶¶49, 57-59.

In addition, the Petition incorrectly asserts a "POSITA would have understood checking for anti-virus software would merely be an additional item for server 215 ('gatekeeper') to check in the authentication process disclosed by Krantz." Pet at 43. The Petition argues that a POSITA would have arrived at this supposed understanding because "Krantz is focused on network authentication/security." Pet. at 43. Again, Krantz is unrelated to device compliance with a security policies like virus protection. EX2001, ¶¶49, 57-59. Instead, Krantz's authentication relates only to determining whether the user or user's device has the necessary credentials, *i.e.*, whether the user is authorized to access the network such as through being a

subscriber. EX1205, [0016] ("A client sends credentials to the server to attempt to authenticate with the server. Based on the credentials, the server may authorize the client for at least partial access to the second network and/or may deny access to the second network and authorize the client for at least partial to access to the first network."); EX2001, ¶¶49, 57-59. Without any recognition of any evaluation of an access device other than authorization a POSITA would have not been motivated to combine Herrmann's checking for a virus-protection program with Krantz. EX2001, ¶¶49, 57-59.

With regard to the "applying step," Petitioners argue it would have been obvious to "implement 'applying of the security policy taking place under control of the gatekeeper' as described *supra* with respect to Herrmann, in the gatekeeper of Krantz" because the "server components in Herrmann are similar to the gatekeeper of Krantz." Pet. at 57. Even if this was true (it is not), Petitioners cite to no authority for the proposition that motivation to combine is present because two references have similar computer components. All computers have similar components, and mere commonality is not sufficient to establish motivation.

C. Neither Krantz Nor Herrmann Disclose "Applying The Security Policy Includes Configuring The Access Point (Claims 2-7 and 22)

Independent claim 22 and claims 2-7 of recite: "applying the security policy includes configuring the access point." As discussed with claim 1, these claims are

also not obvious in view of Krantz and Herrmann since neither teach "applying the security policy includes configuring the access point."

The patent explains: "[t]he reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less restricted VLAN." EX1201, 3:30-33. Thus, there are changing pathway assignments for the ports of *the access point*. The specification explains: "[t]he passing of access requests to the restricted subset and granting of access are accomplished by configuring and reconfiguring a communication port of an access point." EX1201, 2:64-67.

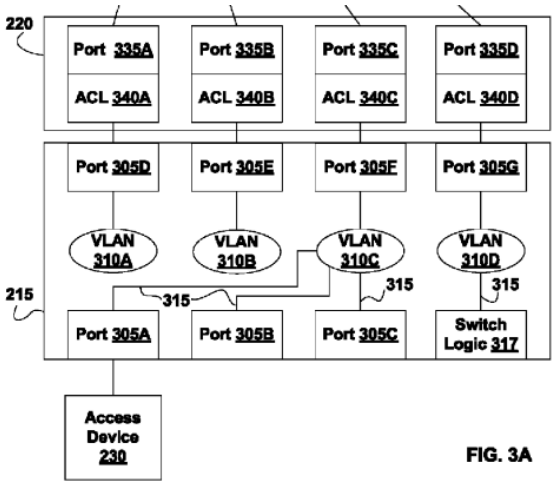


FIG. 3A

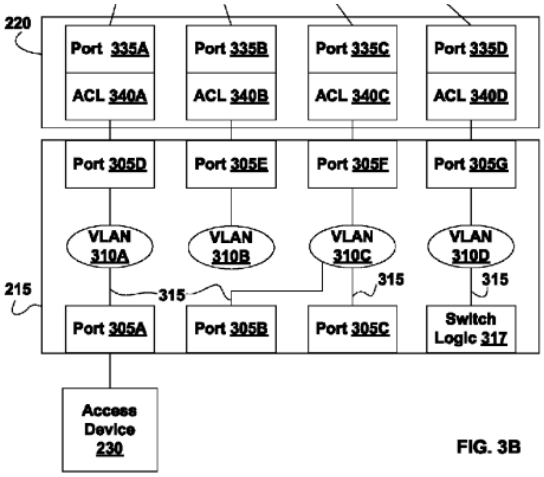


FIG. 3B

> Communication received at one member of Ports 305A-305G is directed internally to another member of Ports 305A-305G via a member of VLANs 310A-310D. VLANs 310A-310D are logical associations between members of Ports 305A-305G. Typically, any members of Ports 305A-305G that are configured to be associated with the same member of VLANs 310A-310D are in bi-directional communication with each other. These associations are illustrated in FIGS. 3A and 3B by Lines 315.

EX1201, 8:4-12.

> Switch Logic 317 is configured for configuring and reconfiguring members of Ports 305A-305G responsive to received commands. For example, by receiving an appropriate command, Switch Logic 317 is configured to reconfigure Port 305A to be associated with VLAN 310A, as illustrated in FIG. 3B below. In this configuration, data received at Port 305A is directed to Port 305D via VLAN 310A, rather than to Port 305F.

Id., 8:28-32.

As shown, an access point's port is configured to change connections. Petitioners make several arguments for how Krantz discloses "configuring the access point." None work.

Petitioners broadly suggest Krantz configures an access point because a user device originally directed to VLAN B is directed to VLAN C. Pet. at 62-63. But according to the annotated figure at page 62 of the Petition, the "access point 209" is never configured as part of applying a security policy. Instead, the access point 209 always transfers data from "client 205" via "port 251" to "data routing device 214" via "port 252," including before and after authentication.

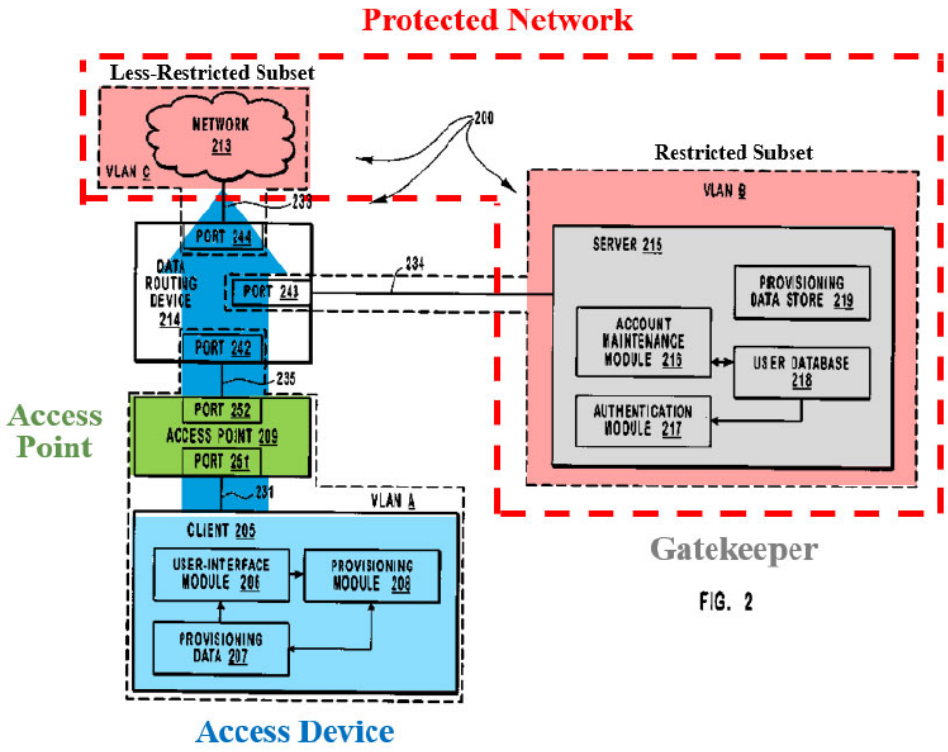


FIG. 2

Pet. at 62.

There is no configuration of access point 209 at all.

The patent is clear: "management of Access Point 215 is accomplished by configuring and reconfiguring one or more communication ports within Access Point 215…." EX1201, 7:6-7.

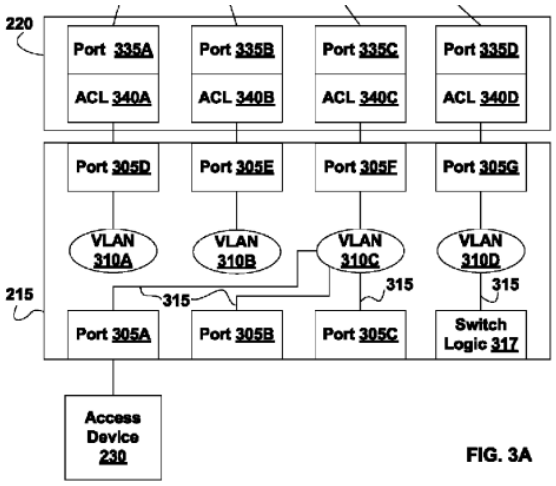


FIG. 3A

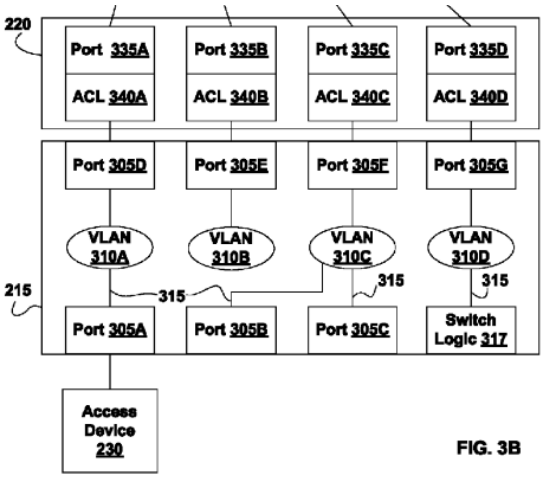


FIG. 3B

This means the access device's port is configured to send data to a particular network depending on the security policy application. As shown in FIG. 3A, port 305A of the access point 215 sends data to VLAN 310C (as shown by line 315).In FIG. 3B, however, that same port 305A has been "configured" to send data to VLAN 310A due to application of the security policy. By contrast, as shown above, Krantz discloses no configuring of access point 209 at all, let alone as part of applying a security policy.

Petitioners argue "Krantz explains that '[a]ccess point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 that are to be transferred to VLAN B and/or VLAN C." Pet. at 62 (citing EX1205, [0023], [0061] and [0064]). Petitioners' "Tag Headers" argument fails.

The claim requires configuring the access point, not the client data. Yet, the Petition contends Tag Headers are inserted "***into data frames received from client*** 205 that are to be transferred to VLAN B and/or VLAN C." *Id.* (emphasis supplied).

Data frames in client data are like the address an envelope. *See* EX1201, ¶61. Adding a header to an envelope, such as "Attn: John Doe," is simply different from configuring the access point. Krantz's "data routing device 214" directs the traffic to either the VLAN B or VLAN C based on consideration of the user's identification information.

> Data routing device 214 can process the inserted Tag Header and transfer the EAPOL packet onto VLAN B. Server 215 can receive the EAPOL packet, which is transferred to authentication module 217 for authentication. … When credentials are sent to server 215, authentication module 217 can receive the credentials (e.g., user-identifier and password) and compare the credentials to entries in user database 218. If credential information matches an entry in user database 218, the identity of a user is authenticated (i.e., server 215 believes that the user represented by the user-identifier is the user who entered the credential information). If an authenticated user of client 205 is authorized to access resources located on VLAN C (e.g., the user is up to date on payments for their account), client 205 can then be authorized to access resources located on VLAN C.

EX1205, [0073]-[0076]. There is no configuring of the access point 209. EX2001, ¶59.

Alternatively Petitioners argue if Krantz does not expressly disclose "wherein applying the security policy includes configuring the access point," it would have been obvious to implement the Data Routing Device disclosure of Krantz within the Access Point 209 itself." Pet. at 66. As discussed, configuring client data with tag headers is not configuring of the access point. Rather, it is only manipulating "data from client 205."

Even if "tag headers" could be considered to be configuring of access point, Krantz separately describes access point 209 and data routing device 214. Arbitrarily combining these distinct components finds no support in Krantz. To the contrary, Petitioners' own cited portions of Krantz expressly teaches access point 209 and a different component—data routing device 214. EX1205, [0073] ("[A]ccess point 209 and/or data routing device 214 may strip the 802.1X encapsulation and instead encapsulate the EAP-Response/Identity messages within an EAP-RADIUS message that is transferred onto VLAN B.")[2]

Lastly, Petitioners argue Krantz's data routing device and access point have the same functionality, and therefore, a POSITA would have combined them. Such speculation is without logic. Krantz's data routing device determines where data goes based on fields in the client data. EX1205, [0059]. An access point is, as the name suggests, a device through which data passes. As such, Krantz itself explains the components have different functions. Petitioners' reliance on its expert to make this leap amounts to nothing more than impermissible hindsight. *Polaris*, 882 F.3d at 1068.

[2] Notably, EAP-Response/Identity relates only to authentication. See, https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485048062.htm.

D. Claims 5-7 Are Not Obvious In View of Krantz With Herrmann

Claims 5-7 (depending from claim 1) include limitations related to updated audit data. For at least the reasons discussed, Krantz's failure to disclose anything about audit data pertaining to a device means the challenge to claims 5-7 must fail.

Just like Krantz failed to disclose device "audit data," it also fails to disclose "receiving, from the agent, updated audit data pertaining to the device" as required by claims 5-7. Petitioners' attempt to transform user authentication into "updated audit data pertaining to the device" (Pet. at 77-81) only demonstrate why such contortion does not work. Petitioners claims a subscription paid for by a user can expire, and Krantz provides for checking of the user's subscription. *Id*. But the validity of a user's subscription has nothing to do with the device or device compliance with a security policy.

Petitioners' references to an EAP-Response/Identity message or and EAP-MSChapV2 do not change this. Each of the EAP-Response/Identity message or and EAP-MSChapV2 message relates to user authentication.[3] But, the claim requires that the audit data relates to the device and a security policy – something different from Krantz. EX2001, ¶¶56-59.

[3] See https://www.portnox.com/cybersecurity-101/mschapv2/ (EAP-MSChapV2); https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485048062.htm (EAP-Response/Identity).

E. Claim 22 Is Not Obvious In View of Krantz In Combination With Herrmann

Claim 22 is an independent claim, but shares many of the limitations from claim 1. In addition, claim 22 includes the requirement of receiving, from the agent, updated audit data pertaining to the device while the device has access to a less-restricted subset of the network. This limitation is also found in claim 6. For the reasons discussed previously with respect to claims 1 and 6, Krantz in combination with Herrmann fails to render claim 22 unpatentable as obvious.

Claim 22 further requires re-auditing of the device based on the received updated audit data. Petitioners argue that this limitation is met by "submitting appropriate credentials to server 215." Pet. at 88. Again, user credentials are not audit data pertaining to a device. Therefore, Petitioners' unpatentability arguments for claim 22 must fails for failure to disclose this re-auditing limitation as well.

VI. All Grounds: Neither Reference Constitutes Prior Art

The Board has previously found antedating prior art references is sufficient grounds for denying *inter partes* review institution. *LG Elecs., Inc. v. Wi-LAN Inc.*, No. IPR2018-00704, Paper No. 14 at 20 (P.T.A.B. Sept. 5, 2018) ("[W]e determine that Patent Owner has provided sufficient evidence to antedate ZTE . . . [and therefore] Petitioner has not demonstrated a reasonable likelihood of prevailing[.]").

Neither Krantz nor Herrmann are prior art because the InfoExpress inventors conceived of the invention before the effective dates and exercised reasonably continuous diligence in reducing to the claimed inventions to practice.

A. Legal Standard

A reference is prior art only if filed before the date of "the invention by the [patent owner]." 35 U.S.C. § 102(e) (pre-AIA). *See, e.g.*, *Sequenom v. Leland Stanford Junior Univ.*, No. IPR2013-00390, at 5 (P.T.A.B. Nov. 25, 2014).

To antedate a reference, one must show conception prior to the critical date and "reasonably continuous diligence" throughout the critical period from just before the effective date of the prior art until reduction to practice. *E.g., ATI Techs. v. Iancu*, 920 F.3d 1362, 1369 (Fed. Cir. 2019).

For reasonable continuous diligence, an inventor need not work on reducing the invention to practice every day, and periods of inactivity do not automatically vanquish a claim of reasonable diligence. *ATI*, 920 F.3d at 1369; *Monsanto Co. v. Mycogen Plant Sci., Inc.*, 261 F.3d 1356, 1369 (Fed. Cir. 2001); *Perfect Surgical Techniques, Inc. v. Olympus Am., Inc.*, 841 F.3d 1004, 1009 (Fed. Cir. 2016).

Additionally, an attorney's work preparing a patent application can demonstrate diligence. *Perfect Surgical*, 841 F.3d at 1009-1012; *Bey v. Kollonitsch*, 806 F.2d 1024, 1030 (Fed. Cir. 1986).

Inventor declarations submitted to establish conception and diligence must be corroborated. *Perfect Surgical*, 841 F.3d at 1007. The "rule of reason" analysis governs whether corroboration is sufficient. *Id.* at 1009. "A variety of activities may corroborate an inventor's testimony of reasonable diligence, and such corroborating evidence is considered 'as a whole.'" *Id.* at 1007-08 (quotation omitted). The patent owner need not corroborate every contested factual issue, but instead merely needs to produce sufficient independent circumstantial evidence to support the testimony. *Perfect Surgical*, 841 F.3d at 1009.

The purpose of diligence is to show that the invention was not abandoned, set aside, or unreasonably delayed, not to "scour the patent owner's corroborating evidence in search of intervals of time where the patent owner has failed to substantiate some sort of activity." *Id.*

B. The Inventors Conceived of the Claimed Inventions Prior to the Critical Dates of Both Krantz and Herrmann.

Petitioner asserts Krantz has an effective date of December 6, 2002 (Pet. at 7) and Herrmann has an effective date of March 13, 2003.[4] *Id*. at 10. InfoExpress conceived of the claimed invention before that.

[4] Herrmann's provisional date is listed as December 2, 2002. Petitioners waived any right to establish this provisional date as the §102(e) date because they failed to submit, mention, or analyze its provisional filing in the Petition. *SAS Institute Inc. v. Iancu*, 138 S.Ct. 1348, 1355 (2018) (the petition must define the boundaries of the IPR); *Globus Med., Inc. v. Depuy Synthes Prods., LLC*, No. IPR2015-00107, at *3 (P.T.A.B. May 1, 2015). Notwithstanding, the Hermmann provisional date is still

On November 14, 2002, InfoExpress' inventors had the "CyberGatekeeper LAN Based Policy Enforcement Engineering Specification" (EX2011: "LAN Engineering Specification") prepared demonstrating that the claimed inventions were conceived of at least as of that date. EX2012; EX2003 (Lum Declaration), ¶ 12. This conception is demonstrated in the claim chart mapping by Dr. Smith showing the LAN Engineering Specification mapped to the challenged claims as set forth in EX2009. EX2007.

Indeed, leading up to the November 14, 2002 LAN Engineering Specification, InfoExpress were diligently working.

This was groundbreaking because preexisting security technologies did not include the implementation of auditing support functionality over authentication protocols such as 802.1x. The InfoExpress team diligently worked in October 2002 and November 2002 to produce the LAN Engineering Specification of November 14, 2002. EX2021; EX2056; EX2061; EX2273; EX2274; EX2275; EX2342.

later in time than the November 14, 2002 conception of the claimed inventions and thus would not be prior art regardless.

C. The Inventors Exercised Reasonably Continuous Diligence Up and Through Constructive Reduction to Practice.

Before and after the November 14, 2002 LAN Engineering Specification, InfoExpress exercised reasonably continuous diligence up and through at least the filing of U.S. Patent Application No. 60/513,080 on October 21, 2003. The filing of this application constitutes constructive reduction to practice of the claimed inventions. EX2007, EX2010.

The InfoExpress inventors and team members diligently pursued reducing the claimed invention to practice from conception until constructive reduction to practice on at least October 21, 2003. This diligence is shown by substantial InfoExpress evidence including:

i. emails (e.g., EX2015-EX2065; EX2067; EX2068; EX2071; EX2074-EX2200; EX2202-EX2271; EX2273; EX2274; EX2276-EX2283; EX2285; EX2287-EX2326; EX2331-EX2340; EX2342-EX2382; EX2384-EX2390; EX2395-EX2397; EX2399-EX2410);

ii. technical specifications and analyses (e.g., EX2011-EX2014; EX2066; EX2069; EX2070; EX2072; EX2073; EX2201; EX2275; EX2329; EX2330);

iii. source code (e.g., EX2113; EX2114; EX2121; EX2129; EX2138; EX2178; EX2191; EX2197; EX2206; EX2298; EX2303; EX2314; EX2339; EX2348; EX2352; EX2359; EX2364; EX2384; EX2399; EX2404; EX2405); and

iv. the inventor declaration of InfoExpress CEO Stacey Lum (EX2003). .

As further detailed in the diligence calendar submitted herewith (EX2004), InfoExpress worked consistently to reduce the claimed invention to practice. This evidence leaves no doubt that the InfoExpress inventors conceived of and diligently

pursued reduction to practice during the critical period. *See ATI*, 920 F.3d at 1373 (Court finding that Patent Owner's evidence did "not point to the remotest suggestion of abandonment or setting aside" where the Patent Owner provided a calendar demonstrating that designated activity on the majority of days in the diligence period, and a declaration summarizing various documents in support of diligence); *Monsanto*, 261 F.3d at 1369 (substantial diligence evidence where the Patent Owner identified record evidence showing activity multiple times per month during the critical period, and there was no reason to doubt that the activity was relevant in reducing the invention to practice).

December 2002:

- [redacted]
- See EX2003, ¶¶6-7, 30, 33, 37, 49 (Lum Declaration).

January 2003:

- [redacted]
- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- Mr. Lum spoke with eventual patent counsel to clear conflicts. EX2212.
- See EX2003, ¶¶6-7, 30, 33, 37, 49) (Lum Declaration).

February 2003:

- [redacted]

- *See* EX2003, ¶¶32-33, 38, 40-43, 50-51, 56-57 (Lum Declaration).

March 2003:

- See EX2003, ¶¶44, 52, 58 (Lum Declaration)

April 2003:

- [redacted]
- [redacted]

May 2003:

- [redacted]
- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- [redacted]

June 2003:

- [redacted]

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- [redacted]
- [redacted]

July 2003:

- [redacted]
  - [redacted]
  - [redacted]

- [redacted]

[redacted]

August 2003:

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]

[redacted]

September 2003:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

October 2003:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

D. The inventors exercised achieved a constructive reduction to practice by the filing of U.S. Provisional Patent Application Serial No. 60/513,080 was filed on October 21, 2003.

As set forth in EX2010 and discussed by Prof. Smith (EX2007), the '080 Provisional provides written description support for the Challenged Claims in accordance with pre-A.I.A. 35 U.S.C. §§ 119(e) & 112, ¶ 1.

The evidence discussed above demonstrates diligence on the part of the inventors towards reducing the claimed invention to practice. *ATI*, 920 F.3d at 1374.

VII. Conclusion

For these reasons, Patent Owner respectfully requests the Board reject the Petition and not institute an *inter partes* review of the Challenged Claims.

Respectfully submitted,

Dated: July 17, 2024 Mailing address for all correspondence: Saul Ewing LLP Centre Square West 1500 Market Street, 38th Floor Philadelphia, PA 19102-2186	*/s/ Brian R. Michalek* Brian R. Michalek (Reg. No. 65,816) Saul Ewing LLP 161 North Clark Street, Suite 4200 Chicago, IL 60601 Tel: (312) 876-7151 brian.michalek@saul.com Joseph M. Kuo (Reg. No. 38,943) Saul Ewing LLP 161 North Clark Street, Suite 4200 Chicago, IL 60601 Tel: (312) 876-7151 joseph.kuo@saul.com Brian Landry (Reg. No. 62,074) Saul Ewing LLP 131 Dartmouth Street, Suite 501 Boston, MA 02116 Tel: (617) 912-0969 Brian.Landry@saul.com Counsel for Patent Owner

Certification of Word Count Under 37 C.F.R. § 42.6(d)

The undersigned hereby certifies that the foregoing complies with the type-volume limitation in 37 C.F.R. § 42.24(b)(1). According to the word-processing system's word count, the document contains 12,340 words, excluding the parts of the brief exempted by 37 C.F.R § 42.24(b).

Date: July 17, 2024

/Brian R. Landry/
Reg. No. 62,074

Certification of Service Under 37 C.F.R. § 42.6(e)(4)

The undersigned hereby certifies that the foregoing was served in its entirety by filing through the Patent Trial and Appeal Board P-TACTS, as well as providing a courtesy copy via e-mail to the attorneys of record.

Date: July 17, 2024

/Brian R. Landry/
Reg. No. 62,074

CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00676]
Page 1140 of 1144
INFOEXPRESS, INC. - EX2572

CourtAlert® Case Management

From: ECF-CAND@cand.uscourts.gov
Sent: 8/24/2024 12:44:46 AM
To: efiling@cand.uscourts.gov
Subject: Activity in Case 4:23-cv-02698-YGR InfoExpress Inc. v. Cisco Systems, Inc. Brief

---

EXTERNAL EMAIL - This message originates from outside our Firm. Please consider carefully before responding or clicking links/attachments. This is an automatic e-mail message generated by the CM/ECF system. Please DO NOT RESPOND to this e-mail because the mail box is unattended. ***NOTE TO PUBLIC ACCESS USERS*** Judicial Conference of the United States policy permits attorneys of record and parties in a case (including pro se litigants) to receive one free electronic copy of all documents filed electronically, if receipt is required by law or directed by the filer. PACER access fees apply to all other users. To avoid later charges, download a copy of each document during this first viewing. However, if the referenced document is a transcript, the free copy and 30 page limit do not apply. U.S. District Court California Northern District Notice of Electronic Filing The following transaction was entered by Padmanabhan, Krishnan on 8/23/2024 5:43 PM and filed on 8/23/2024 Case Name: InfoExpress Inc. v. Cisco Systems, Inc. Case Number: 4:23-cv-02698-YGR https://ecf.cand.uscourts.gov/cgi-bin/DktRpt.pl?413477 Filer: Cisco Systems, Inc. Document Number: 111 Copy the URL address from the line below into the location bar of your Web browser to view the document: https://ecf.cand.uscourts.gov/doc1/035024784484?caseid=413477&de_seq_num=305&magic_num=47791060 Docket Text: Brief *Defendants Cisco Systems, Inc. and Fortinet, Inc.'s Responsive Claim Construction Brief [109]* filed byCisco Systems, Inc.. (Attachments: # (1) Declaration of William Logan, # (2) Exhibit A, # (3) Exhibit B, # (4) Exhibit C, # (5) Exhibit D, # (6) Exhibit E, # (7) Exhibit F, # (8) Exhibit G, # (9) Exhibit H, # (10) Exhibit I, # (11) Exhibit J, # (12) Exhibit K, # (13) Exhibit L, # (14) Exhibit M, # (15) Exhibit N, # (16) Exhibit O, # (17) Exhibit P, # (18) Exhibit Q, # (19) Exhibit R, # (20) Exhibit S, # (21) Exhibit T, # (22) Exhibit U, # (23) Exhibit V, # (24) Exhibit W, # (25) Exhibit X)(Padmanabhan, Krishnan) (Filed on 8/23/2024) 4:23-cv-02698-YGR Notice has been electronically mailed to: Andrew F. Schwerin , I andrew.schwerin@saul.com, judith.ferraro@saul.com Brenda Helen Entzminger bentzminger@bdiplaw.com Brian Raymond Michalek brian.michalek@saul.com, julie.dillner@saul.com, laura.disanto@saul.com, litigationdocketing@saul.com, rodney.johnson@saul.com Casey T. Grabenstein casey.grabenstein@saul.com David Lesht dlesht@sperling-law.com David P. Enzminger denzminger@winston.com, david-enzminger-5388@ecf.pacerpro.com, ecf_sf@winston.com, gmontoya@winston.com Eamon Padraic Kelly ekelly@sperling-law.com, cagnos@sperling-law.com Joseph M. Kuo joseph.kuo@saul.com, julie.dillner@saul.com, laura.disanto@saul.com, litigationdocketing@saul.com Krishnan Padmanabhan kpadmanabhan@winston.com, ecf_sf@winston.com, krishnan-padmanabhan-6052@ecf.pacerpro.com Michael E Flynn-O'Brien mflynnobrien@bdiplaw.com, 7121937420@filings.docketbird.com, bdipdocketing@bdiplaw.com Patrick D Clark pclark@winston.com, ECF_SF@winston.com, patrick-clark-0510@ecf.pacerpro.com William Mitchell Logan wlogan@winston.com, ECF_SF@winston.com, william-logan-1248@ecf.pacerpro.com 4:23-cv-02698-YGR Please see Local Rule 5-5; Notice has NOT been electronically mailed to: The following document(s) are associated with this transaction:

Document description: Main Document Original filename: C:\fakepath\2024.08.23 Defs' Responsive Claim Construction Brief.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-0] [68fcea09f1bb30b74b248df77e435c3eed1d5badbc201c9157c001d1496d19e0a0fb20da04ce83ce3d3a34426f9b767b8a3aae527817a04e05994456ab46d7ea]] Document description: Declaration of William Logan Original filename: C:\fakepath\2024.08.23 Logan Decl ISO Defs' Responsive Claim Construction Brief.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-1] [b328895edfecf14ddab52f3d2bb4f5128fb0cc3fe7f376597bab948a7dbf5900506488f7c630055bb69e6a4de3aa24b7d7bb0473e8207acc47371f09732f844a]] Document description: Exhibit A Original filename: C:\fakepath\Ex. A - Cisco's Identification of Preliminary Claim Constructions.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-2] [7523dfd6dc37eed1c4e5ba6b384af8111ad7ed6d0edbbfc8510e531a35c90aa354765100128235d0fcaa928c6128bc22cc3d610470066292d21b72002450228b]] Document description: Exhibit B Original filename: C:\fakepath\Ex. B - 2024-03-25 Cisco Identification of Prelim Claim Constructions and Evidence per PLR 4-2 (005).pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-3] [63144bfc292fb349315f939db4ebfe5f3899fdfa5c6bfe489449741c726e40fba3cc5f9797170ddf8782dcf4093e30823676c5fb79dedb06c755116e24ea8fcd]] Document description: Exhibit C Original filename: C:\fakepath\Ex. C - InfoExpress v. Cisco Meeting Invite.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-4] [4f12f5d0035779eaf69eda182a4447b9a0d8d0cfe36d242eec70da95d0488320235002f53bcd40a651b3f32178becceb768df62b72d8808ce83e0f58babf40ef]] Document description: Exhibit D Original filename: C:\fakepath\Ex. D - Re InfoExpress v. Cisco Case No. 423-cv-02698-YGR; InfoExpress v. Fortinet C.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-5] [b0bb2ba762054df8a8c6e72d31b8f950e2059b63d15e695aeceaf8229ee3c5815e7906030c568e7799760d1efa2adb591a2cb84aa29552ce5e71a4f4ea738bf0]] Document description: Exhibit E Original filename: C:\fakepath\Ex. E - Patent L.R. 4-3 Joint Claim.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-6] [9f8db8e67076ac44959f77ecdd70ff69015029f18036e078939cc3a9aa722858e4d8ead3a5a764dd578b805634583507bb7a2500756684d6c0d4c912d2375126]] Document description: Exhibit F Original filename: C:\fakepath\Ex. F - RE_ InfoExpress v. Cisco_Fortinet - Claim Construction Discovery DRAFT Stipulation.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-7] [af4b043f1647b5e0b7108c438fcb89836e870eba9b568299a6ad9af42f077f8dabed1fcaa9b2d3e414f9ad52f0de43152876c45c21affbfeb100ea1c2b80635d]] Document description: Exhibit G Original filename: C:\fakepath\Ex. G - RE_ InfoExpress v. Cisco [23-cv-02698] and Fortinet [23-cv-04389] _ Service of Sealed Filings.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-8] [814a556641793cd71467226af50d8db66ecac2450c9d2d6c67f86364537317c5340f875cc4e458c4de68885034722c2fbc97f4dbfda7e7bb50d337b3bed9571b]] Document description: Exhibit H Original filename: C:\fakepath\Ex. H - RE_ InfoExpress v. Cisco, Fortinet - Follow-up From Court's Video Conference.pdf Electronic document Stamp: [STAMP

CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-9] [79541a980c0ebf2dc7ff30a0700850bb4851e4ecff7efaa82632f1d1b2c5c0ebeac541d8cac04c3fae b01cac1d2bc2c5a6b4f8561c5e15ff650b8f2e11cd165b]] Document description: Exhibit I Original filename: C:\fakepath\Ex. I - Cisco Notice of Deposition of Dr. Striegel.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-10] [0c8d45a454ca6aadd21698187e84f63c91e8b8185891d41d7b70d5590eca08bbe32a5e16f17bbed 5d6ffbb5dbd536bddc129b7479bd51bf523eb6aa8fc1948db]] Document description: Exhibit J Original filename: C:\fakepath\Ex. J - 2024.07.09 Notice of Dep of Striegel (Infoexpress).pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-11] [69b481a841f74ef946335743fe1aa90d1558321a725e5fce7931ac7656ec41b5e2a2fe35b0c2f2462 b3ce963bdfc1c0b0f3755fa2cf7cdc1bcd2f7185d89978b]] Document description: Exhibit K Original filename: C:\fakepath\Ex. K - 2024-06-28 Reddy CC Expert Declaration.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-12] [0415a1e0e435dcd8f72b48e31d82fd60c274e13b369b8969c60ece3c3f0f8cd4c8ad0028e5baffeb8 b0a3260fb65267eec9e67dbb60c4d51f6493e09dc54935f]] Document description: Exhibit L Original filename: C:\fakepath\Ex. L - 2024.03.01 - InfoExpress - Cisco Invalidity Contention Cover Pleading (FINAL).pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-13] [3be2bad6a7df65a57e23784f63b19f552e07a5a3533cf749f4d65f52ddf9e26a7afb7005ceabbb9efa 8c2d1908e0ab49ba53f038d286d5f394b9187e0d859b3b]] Document description: Exhibit M Original filename: C:\fakepath\Ex. M - 2023-11-30 Cisco's Proposed Claims Terms for CC.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-14] [a3cbe32de41be38a85c56cf6fcc47b0decb7eaf0fb8b4683275cec2b852e4dfbf549ae559e457a5acc 531aa21a9dd8bd8a8284eaefa9152a0d5a2b1fee0759ec]] Document description: Exhibit N Original filename: C:\fakepath\Ex. N - 2023-11-30 InfoExpress's Proposed Patent Claim Terms for Construction.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-15] [1a41f972a0fb85081db77951069e722cb6bb02b27b55da81c947a47e3fecf5618670d091a561ebae c06b51b1fca6728ec1094f0fb9c49ffe0e597e6c87846dc5]] Document description: Exhibit O Original filename: C:\fakepath\Ex. O - 2024-03-04 InfoExpress's Proposed Patent Claim Terms for Construction per Patent L.R. 4-1.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-16] [3544c24575f3bb1d9065b6d9fe3f9a52c708393d6b660014b641e10a22e92b3dff17f3b480bd8f21 786977983ac9ec865ace4b1415282158eaa539cb7ca8ae84]] Document description: Exhibit P Original filename: C:\fakepath\Ex. P - 2024-03-15 InfoExpress's Amended Proposed Patent Claim Terms for Construction.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-17] [058fac5a381d27a30afc71a31743871f4d4f42f4c83f4f9463125e375b59a70f90af4c29cfa0e7f0a5 6c15fd8557aaf12ca4278f678fdadc2fbe9168aa0c57fc]] Document description: Exhibit Q Original filename: C:\fakepath\Ex. Q - 2024-03-22 InfoExpress's Second Amended Proposed Patent Claim Terms.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-18]

[87abf687431b3c41ab7f17f3633bb2673488566b62c5354be6f4cf391aa1a753996838d94c5b913c04c49be44c48e7d02097993d101cd2d7d8616b6934a1a508]] Document description: Exhibit R Original filename: C:\fakepath\Ex. R - 2024-03-25 InfoExpress's Claim Constructions and Evidence per Patent L.R. 4-2.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-19] [3d3802a38c72addc1810b84a3966a9a8f107b43d965a5b3b4a8bb6be465511f80d1336044bc5102a96d38584e44a871d5aaa68b9d5bd125b1be56be556fe71e1]] Document description: Exhibit S Original filename: C:\fakepath\Ex. S - Striegel, Ph.D, Aaron D. Transcript.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-20] [4323ce638d6d563d118d110b974a504883b4a28f50cca4f0f9aca7a822ed5aa2a9a110af76ffd5477eff2b17541dcd98d3e455b21821329ff32688608d4a2174]] Document description: Exhibit T Original filename: C:\fakepath\Ex. T - Prov. App. No. 60513080.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-21] [0d4f30445bce7934156612e4ef9011bc118522a4cf33ebe533940fa97c71abaa4b12823e5a6dee79d2f73bb903f20442bb9a757485eab41885749b7089c8e94f]] Document description: Exhibit U Original filename: C:\fakepath\Ex. U - BillJCo Reply CC Brief.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-22] [7f6d2c78acc848ce628a41beb6c668fd30d7f4c7a9f59aa8fe4a1d47427083138ebce515ce3fe954f7413d98589e43e65376278cffc851bae734fbc62894decf]] Document description: Exhibit V Original filename: C:\fakepath\Ex. V - InfoExpress's Disclosure of Asserted Claims and Infringement Contentions_w exhs.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-23] [7b3a360a6c0345dc038b9853bf818622e86bd1326d6887c768bb1fffe3012834bfa5f5f98bd66b417f54401080192840dc612e3306f6a22f2f575aadf9c07ffc]] Document description: Exhibit W Original filename: C:\fakepath\Ex. W - '484 POPR - PTAB-IPR2024-00675-9.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-24] [45b94ec7515feb09f910e21b72b852b6534dca6789be6eafffb1c9716109b2a77aa4a26b22d71d069a6e732b8b0d1122ec824651f72980bb2b683ac543d1c46a]] Document description: Exhibit X Original filename: C:\fakepath\Ex. X - '444 POPR - PTAB-IPR2024-00677-8.pdf Electronic document Stamp: [STAMP CANDStamp_ID=977336130 [Date=8/23/2024] [FileNumber=21615412-25] [0e4b4a0cd909d093b5800cfb30a7c99bddb98b8f501b321f56340ae604bab55d3e6a49bb7457c8eb8b933e9bddec722cae2a0b2bc32b67c88ad8ca2eae108f96]]