CISCO SYSTEMS

Cisco Trust Agent Administrator Guide

Version 1.0
June 2004

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number: OL-6191-02

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc. ; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChann el, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United Stat es and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word par tner does not imply a partnership relationship between Cisco and any other company. (0403R)

Cisco Trust Agent Administrator Guide
Copyright © 2004 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface vii

Audience vii

Organization viii

Conventions ix

Related Documentation x

Obtaining Documentation xi

Cisco.com xi

Ordering Documentation xi

Documentation Feedback xii

Obtaining Technical Assistance xii

Cisco Technical Support Website xii

Submitting a Service Request xiii

Definitions of Service Request Severity xiii

Obtaining Additional Publications and Information xiv

CHAPTER 1 **Cisco Trust Agent Overview** 1-1

Cisco NAC Overview 1-1

Cisco Trust Agent Deployment Considerations 1-3

CHAPTER 2 **Creating a Custom Installation Package** 2-1

Installation Package Components 2-1

The ctasetup.exe File 2-2

The Plugins Directory 2-2

The Certs Directory 2-2

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 3 of 81

The ctad.in Configuration File 2-3
The ctalogd.in Configuration File 2-3
The instmsiw.exe File 2-4
Creating the Installation Media 2-4

CHAPTER 3 Installing Cisco Trust Agent 3-1
Verify System Requirements 3-1
Installing Cisco Trust Agent on Windows 3-2
Verifying the Cisco Trust Agent Installation 3-5
Removing Cisco Trust Agent 3-5

CHAPTER 4 Configuring Communication Settings 4-1
Configurable Communication Settings 4-1
About Communication Settings Configuration 4-2

CHAPTER 5 Cisco Trust Agent Event Logging 5-1
How Logging Works 5-1
About Logging Configuration 5-2
About Logging Levels 5-3
About the Log Files 5-3
Log File Creation and Naming 5-4
Log File Format 5-5
Cisco Trust Agent Logging Command-line Interface 5-7
About the CTALOGUtility 5-7
Enabling and Disabling Logging from the Command Line 5-8
Clearing the Log File from the Command Line 5-9
Logging Considerations 5-9

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 4 of 81

CHAPTER 6 User Notifications 6-1
Notification Display 6-1
About User Notification Configuration 6-2
Logging Notifications 6-2

CHAPTER 7 Security Posture Plugins 7-1
Plugin Installation and Upgrade 7-1
The Cisco Trust Agent Posture Plugin 7-3

CHAPTER 8 Cisco Trust Agent Certificates 8-1
Installing and Updating the Server Root Certificate 8-2
About the ctaCert.exe Utility 8-3
Distinguished Name Matching 8-4

APPENDIX A Cisco Trust Agent Configuration File Reference A-1
Creating and Editing the Configuration Files A-1
The ctad.ini Configuration File A-2
ctad.ini Sample A-2
ctad.ini Settings A-3
DN Matching Rule Syntax A-5
The ctalogd.ini Configuration File A-6
ctalogd.ini Sample A-7
ctalogd.ini Settings A-7

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 5 of 81

APPENDIX B Cisco Trust Agent Posture Plugin Reference B-1

APPENDIX C System Change Reference C-1

APPENDIX D Open Source License Acknowledgement D-1

OpenSSL D-1

Info-ZIP D-4

INDEX

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 6 of 81

Preface

Cisco Trust Agent is a specialized application that runs on your network clients. It collects security posture information from the Network Admission Control (NAC)-compliant applications installed on those clients and reports the posture information to a posture validation server. Based on the reported security posture, the network client is then either permitted or denied access to the network.

Cisco Trust Agent also provides a security posture plugin that provides basic reporting of operating system type, version, and Cisco Trust Agent name and version.

Audience

The Cisco Trust Agent Administrator Guide provides installation, configuration, and monitoring information to administrators responsible for deploying Cisco Trust Agent to network clients.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 7 of 81

Organization

This guide contains the following chapters and appendixes:

- **Chapter 1, "Cisco Trust Agent Overview"**—Provides an overview of the Cisco NAC solution and the role that Cisco Trust Agent plays within that solution.
- **Chapter 2, "Creating a Custom Installation Package"**—Describes how the Cisco Trust Agent administrator can create a custom installation package to speed deployment of Cisco Trust Agent throughout the network.
- **Chapter 3, "Installing Cisco Trust Agent"**—Provides prerequisites and step-by-step instructions for installing and removing Cisco Trust Agent.
- **Chapter 4, "Configuring Communication Settings"**—Describes the Cisco Trust Agent communication settings and how to configure them.
- **Chapter 5, "Cisco Trust Agent Event Logging"**—Describes how to enable and configure event logging in Cisco Trust Agent.
- **Chapter 6, "User Notifications"**—Describes the behavior and configuration of user notifications.
- **Chapter 7, "Security Posture Plugins"**—Describes security posture plugins, where they are located, and how they are updated. This chapter also includes information about the default plugin installed with Cisco Trust Agent.
- **Chapter 8, "Cisco Trust Agent Certificates"**—Describes how to update the certificates used to establish a secure PEAP connection with the posture validation server.
- **Appendix A, "Cisco Trust Agent Configuration File Reference"**—Describes the configuration files used to configure Cisco Trust Agent and provides examples of the files, using the default settings.
- **Appendix B, "Cisco Trust Agent Posture Plugin Reference"**—Describes the attributes returned by the default Cisco Trust Agent posture plugin.
- **Appendix C, "System Change Reference"**—Describes the files, directories, and registry entries that are created when you install Cisco Trust Agent.
- **Appendix D, "Open Source License Acknowledgement"**—Provides license information for the third-party, open-source software used in Cisco Trust Agent.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 8 of 81

Conventions

This document uses the following conventions:

Item	Convention
Commands, keywords, special terminology, and options that should be selected during procedures	**boldface** font
Variables for which you supply values and new or important terminology	*italic* font
Displayed session and system information, paths and filenames	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font
Indicates menu items to select, in the order you select them	**Option > Network Preferences**

Tip Identifies information to help you get the most benefit from your product.

Note Means *reader take note*. Notes identify important information that you should reflect upon before continuing, contain helpful suggestions, or provide references to materials not contained in the document.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage, loss of data, or a potential breach in your network security.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 9 of 81

Warning **Identifies information that you must heed to prevent damaging yourself, the state of software, or equipment. Warnings identify definite security breaches that will result if the information presented is not followed carefully.**

Related Documentation

Note Although every effort has been made to validate the accuracy of the information in the printed and electronic documentation, you should also review Cisco Trust Agent documentation on Cisco.com for any updates.

The following documentation is available on Cisco.com:

- For Cisco Trust Agent, the following documents are available:
  - *Cisco Trust Agent Administrator Guide*
  - *Cisco Trust Agent Release Notes Version 1.0*
- For other components in the Cisco NAC solution, the following documents are available:
  - *User Guide for Cisco Secure ACS for Windows Server, Version 3.3*
  - *User Guide for Cisco Secure ACS Solution Engine, Version 3.3*
  - *Network Admission Control* feature documentation for Cisco IOS Release 12.(8)T.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 10 of 81

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 11 of 81

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 12 of 81

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 13 of 81

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 14 of 81

identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 15 of 81

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 16 of 81

Cisco Trust Agent Overview

Cisco Trust Agent is part of the Cisco Network Admission Control (NAC) solution. It collects security posture data for NAC-compliant applications running on your network clients and reports that data to a posture validation server.

This chapter contains the following sections:

- Cisco NAC Overview, page 1-1
- Cisco Trust Agent Deployment Considerations, page 1-3

Cisco NAC Overview

NAC enables network access devices to permit or deny network hosts access to the network based on the state of the software on the host. This process is called posture validation.

The four main components of the posture validation process are as follows:

- **Network Client running Cisco Trust Agent**—Cisco Trust Agent aggregates security posture information from the NAC-compliant applications running on the network client. NAC-compliant applications include:
  - Antivirus applications
  - Personal firewalls
  - Host-based intrusion protection applications, such as Cisco Security Agent
- **Network Access Device (NAD)**—The NAD permits or denies network access. Typically, the NAD is a Cisco IOS router.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 17 of 81

- **Authentication Server (Cisco Secure Access Control Server (ACS))**—The authentication server is responsible for obtaining and evaluating the security posture credentials from the network client, determining the overall system posture, and providing the appropriate network access policy to the NAD based on the system posture.
- **Posture Validation Servers (optional)**—Posture validation servers support Cisco Secure ACS in determining the overall system posture. They are typically third-party applications that support the validation of the security posture credentials for a specific NAC-compliant application.

The following provides an overview of how the posture validation components work together during the posture validation process.

1. The network client sends IP traffic on the network.
2. If this is the first packet the NAD has received from the client, or if it is the first packet received after a specified interval, and if the traffic is designated on the NAD as requiring posture validation, the NAD initiates posture validation. The NAD applies a default access policy to the client network traffic and initiates an EAP over UDP (EAPoUDP) session with the client.
3. The NAD sends an EAP identity request to the network client and then forwards the EAP identity response to Cisco Secure ACS.
4. Cisco Secure ACS establishes a secure PEAP session with the network client and requests the network client security posture credentials.
5. Cisco Trust Agent, running on the network client, receives the security posture credential request and in turn requests security posture credentials from the NAC-compliant applications on the client.The security posture credentials are requested and received through posture plugins provided by the NAC-compliant applications. Cisco Trust Agent aggregates all of the security posture information and returns the information to Cisco Secure ACS.
6. Cisco Secure ACS evaluates the security posture credentials for each application that resides on the network client. Cisco Secure ACS can perform the credential evaluation using rules in the local database or can relay application credentials to an application-specific posture validation server for evaluation. The result of the evaluation is an application posture token for each evaluated application and an optional user notification.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 18 of 81

7. Cisco Secure ACS consolidates the application posture tokens into an overall system posture token. The system posture token is typically the worst of the application posture tokens.

   The system posture token can have one of the following values:

   - Healthy
   - Checkup
   - Quarantine
   - Infected
   - Unknown

8. Cisco Secure ACS maps the system posture token to a network access policy and an optional user notification.
9. Cisco Secure ACS sends the result of the security posture validation and any user notification to Cisco Trust Agent on the network client. Depending upon how you have configured Cisco Trust Agent, the results of the posture validation are logged and any user notifications are displayed on-screen in a dialog box.
10. Cisco Secure ACS closes the PEAP session with the network client and downloads the appropriate enforcement policy to the NAD. The NAD enforces the policy and closes the EAP session with the network client.

Based on the access policy, the network client is permitted on the network, denied access to the network, or quarantined to a remediation network until the NAC-compliant applications have been updated to the required levels.

Cisco Trust Agent Deployment Considerations

Network clients are the hosts on your network. This includes PCs, laptops, workstations, and servers. You may have hundreds or thousands of network clients on which you are going to install Cisco Trust Agent. Installing and configuring Cisco Trust Agent on that many network clients can be a time-consuming process.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 19 of 81

To decrease the time spent installing and configuring Cisco Trust Agent throughout your network, you can create a custom installation package. The custom installation package lets you provision the Cisco Trust Agent settings at installation time. These settings include:

- Communication settings
- Logging and notification setting
- Certificate validation rules

Creating a custom installation package also allows you to pre-provision the posture validation server certificates, any additional posture plugins, and an update to the Microsoft Windows Installer (MSI), which may be needed in some installation cases.

See Chapter 2, "Creating a Custom Installation Package" for more information.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 20 of 81

Creating a Custom Installation Package

Before deploying Cisco Trust Agent on your network, you should create a custom installation package. Creating a custom installation package enables you to set Cisco Trust Agent configuration parameters and provision certificates, plugins, and the Microsoft Windows Installer Engine at install time. This saves you considerable configuration time during the deployment of Cisco Trust Agent across your network.

This chapter contains the following sections:

- Installation Package Components, page 2-1
- Creating the Installation Media, page 2-4

Installation Package Components

The Cisco Trust Agent install application is a single executable file. To create a custom installation package, you do *not* need to recompile the Cisco Trust Agent install application. Instead, you simply add the configuration files and installable components to the installation media, along with the Cisco Trust Agent install application. The following list shows the components and directory structure that make up a custom installation package:

- **ctasetup.exe**—The Cisco Trust Agent install application provided by Cisco System, Inc. You do not need to make any changes to this file. This is the only required component of the custom installation package.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 21 of 81

- **plugins**—A directory to contain any third-party plugins that you want to provision at install time.
- **certs**—A directory to contain the root certificates that sign the server certificates for your Cisco Secure Access Control Server (ACS) servers.
- **ctad.ini**—The file used to configure Cisco Trust Agent communication settings, user notifications, and certificate validation rules.
- **ctalogd.ini**—The file used to configure logging.
- **instmsiw.exe**—The Microsoft Windows Installer application.

The ctasetup.exe File

This is the Cisco Trust Agent installer. Do not make any changes to this file. During installation, ctasetup.exe detects and uses the other components that you have added to the installation package.

The Plugins Directory

Create this directory parallel to the ctasetup.exe application on the installation media. Place any posture plugins that you want to provision at installation time in this directory. During the installation process, the posture plugins located in this directory are copied to the appropriate location on the target system and registered with Cisco Trust Agent.

For more information about posture plugins, see Chapter 7, “Security Posture Plugins”.

The Certs Directory

Create this directory parallel to the ctasetup.exe application on the installation media. Place the root certificate for your Cisco Secure ACS server certificates in this directory. During installation, any certificates in this directory are added to the systems root certificate store, typically in the registry entry:

```
\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\
Root\Certificates
```


INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 22 of 81

If your Cisco Secure ACS server uses self-signed certificates, see the Cisco Secure ACS documentation for information about obtaining the certificate; if you use a CA server, refer to your CA server documentation.

For more information about certificates, see Chapter 8, "Cisco Trust Agent Certificates".

The ctad.ini Configuration File

Create the ctad.ini configuration file parallel to the ctasetup.exe application on the installation media. The ctad.ini configuration file controls the following aspects of Cisco Trust Agent operation:

- Communication settings, such as the listening port number, maximum number of allowed sessions, and session time-out value.
- User notification settings, such as if notifications are enabled, how notifications appear, and message timeouts.
- Certification filtering rules.

During the installation process, this file is copied to the appropriate location on the target system. If this file is not present during installation, Cisco Trust Agent uses the default settings for these settings.

For more information about creating the ctad.ini configuration file, see "The ctad.ini Configuration File" section on page A-2 of Appendix A, "Cisco Trust Agent Configuration File Reference". For more information about user notifications in general, see Chapter 6, "User Notifications". For more information about certificates, see Chapter 8, "Cisco Trust Agent Certificates".

The ctalogd.ini Configuration File

Create the ctalogd.ini configuration file parallel to the ctasetup.exe application on the installation media. The ctalogd.ini configuration file controls Cisco Trust Agent logging parameters. By default, logging is disabled in Cisco Trust Agent. You need to provide this file if you want to enable logging. During the installation process, this file is copied to the appropriate location on the target system.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 23 of 81

For more information about creating the ctalogd.ini configuration file, see "The ctalogd.ini Configuration File" section on page A-6 of Appendix A, "Cisco Trust Agent Configuration File Reference". For more information about Cisco Trust Agent logging in general, see Chapter 5, "Cisco Trust Agent Event Logging".

The instmsiw.exe File

Add this application parallel to the ctasetup.exe application on the installation media.

The Cisco Trust Agent installation requires version 2.0 of the Microsoft Windows Installer. The Windows installer does not come pre-installed on all Windows platforms. If you are installing Cisco Trust Agent on Microsoft Windows NT SP 6, you need to download the Windows installer engine from the Microsoft website (http://www.microsoft.com). Go to the downloads page, search for Windows Installer, and select **Windows Installer 2.0 Redistributable for Windows NT 4.0 and 2000**.

During the installation process, if the appropriate Windows installer is not located on the target system, the Cisco Trust Agent install application runs this file to update or install the Windows installer.

Creating the Installation Media

To create the custom installation media, follow these steps:

Step 1 Download the compressed Cisco Trust Agent installer package from Cisco.com.

Step 2 Unpack the installer application, ctasetup.exe.

Step 3 Add the custom configuration files and directories according to the information in this chapter.

Step 4 Create a distributable file set. You can burn the custom installation package to CD-ROM or create a distributable, compressed archive.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 24 of 81

Installing Cisco Trust Agent

This chapter contains the following sections:

- Verify System Requirements, page 3-1
- Installing Cisco Trust Agent on Windows, page 3-2
- Verifying the Cisco Trust Agent Installation, page 3-5
- Removing Cisco Trust Agent, page 3-5

Verify System Requirements

Before installing Cisco Trust Agent, verify that the target system meets the following requirements:

System Component	Requirement
System	ù Pentium-class processor ù Network connection
Operating System	English version of: ù Windows NT, Service Pack 6 ù Windows 2000 ù Windows XP Professional
Windows Installer	Version 2.0 or later.
Hard Disk Space	20 MB

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 25 of 81

System Component	Requirement
Memory	ù 128 MB for Windows NT and Windows 2000 ù 256 MB for Windows XP
Listening Port	By default, Cisco Trust Agent listens on UDP port 21862. You can change this port number. See Chapter 2, "Creating a Custom Installation Package"for configuring the port before installation, or Chapter 4, "Configuring Communication Settings" for changing the port after installation.

Cisco Trust Agent is compatible with the following Cisco NAC components:

- Cisco IOS routers running Cisco IOS Release 12.3(8)T or later.
- Cisco Secure Access Control Server (ACS) version 3.3 or later.

Installing Cisco Trust Agent on Windows

The Cisco Trust Agent installation uses the Microsoft Windows Installer (MSI). You must have Administrator privileges to install Cisco Trust Agent.

Note If the group policy for the target system allow for elevated privileges for the MSI, then users with Standard or Restricted privileges can install Cisco Trust Agent. However, to use the elevated privileges, MSI 2.0 must be installed before you begin the Cisco Trust Agent installation. You cannot use a custom installation package to install the MSI unless you have Administrator privileges.

To install Cisco Trust Agent, follow these steps:

Step 1 Exit all Windows programs and disable any antivirus programs.

Step 2 If you created a custom installation package, insert the installation media into the system. If you are using a downloaded version of Cisco Trust Agent, extract the Cisco Trust Agent installer, ctasetup.exe, to the target system.

Step 3 Browse to the `ctasetup.exe` file and double-click the file.

The Cisco Trust Agent Installation Wizard appears as shown in Figure 3-1.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 26 of 81

Figure 3-1 The Cisco Trust Agent Installation Wizard

Step 4 Click **Next**.

The License Agreement window appears.

Step 5 Read the license agreement. If you agree with the terms and conditions, choose the **I accept the license agreement** option and click **Next**.

If you do not agree with the terms and conditions, click **Cancel** to discontinue the installation.

If you accepted the license agreement, the Destination Folder window appears.

Step 6 If you want to change the installation directory, click **Browse**, navigate to the desired drive and folder, and then click **OK**.

The new install location appears in the Destination Folder field.

Step 7 Click **Next**.

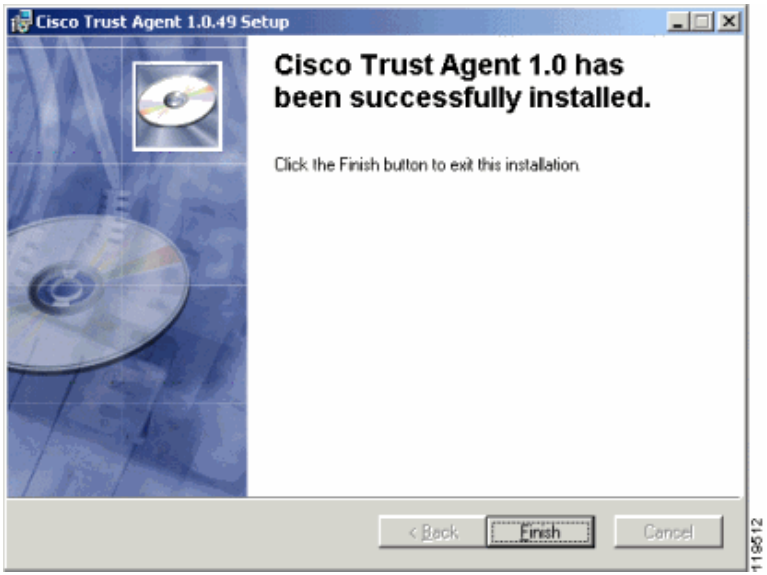
The Ready to Install the Application window appears.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 27 of 81

Step 8 Click **Next**.

The application installs to the selected directory. When the installation has been completed, the installer displays the dialog box shown in Figure 3-2.

Figure 3-2 Completing the Installation



Step 9 Click **Finish**.

The installation application closes. You do not need to restart your system.

Step 10 If you did not create a custom installation package that includes the root certificate for the Cisco Secure Access Control Server (ACS) certificate, you need to install the root certificate before using Cisco Trust Agent. See Chapter 8, "Cisco Trust Agent Certificates" for information about installing the Cisco Secure ACS certificate root certificate.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 28 of 81

Verifying the Cisco Trust Agent Installation

After installing Cisco Trust Agent, verify that the services are running.

To verify the Cisco Trust Agent installation, follow these steps:

Step 1 Open a command prompt on the target system.

Step 2 Type **net start** and press **Enter**.

Step 3 Verify that the following services are running

- Cisco Trust Agent
- Cisco Trust Agent Event Logging Service

If these services are not running, reboot the system. If the services still do not run, reinstall the application.

Removing Cisco Trust Agent

Cisco Trust Agent does not provide a standalone uninstall application; you must use Add/Remove Programs in the Windows Control Panel to remove Cisco Trust Agent.

To remove Cisco Trust Agent, follow these steps:

Step 1 Choose **Start > Settings > Control Panel > Add/Remove Programs**.

Step 2 Select Cisco Trust Agent from the list of installed applications.

Step 3 Click **Remove**.

A confirmation dialog box appears.

Step 4 Click **Yes** to continue the removal.

Cisco Trust Agent is removed from the system. You do not need to reboot the system.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 29 of 81

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 30 of 81

Configuring Communication Settings

Cisco Trust Agent does not initiate posture validation communication; it responds to posture validation requests from the Network Access Devices and Cisco Secure Access Control Server (ACS) servers.

This chapter contains the following sections:

- Configurable Communication Settings, page 4-1
- About Communication Settings Configuration, page 4-2

Configurable Communication Settings

You can configure the following communication settings for Cisco Trust Agent:

- **Listening Port**—By default, Cisco Trust Agent listens on UDP port 21862. If you change this setting, you need to configure your network access device to initiate the posture validation process on the new port number.
- **Maximum Number of Sessions**—Cisco Trust Agent only supports 1 established session per network access device, but can support sessions from multiple, different network access devices at the same time. By default, Cisco Trust Agent can support up to 8 session at one time.
- **Session Idle Timeout**—Specifies the number of seconds an EAPoUDP session can remain idle before timing out. The default value is 600.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 31 of 81

About Communication Settings Configuration

Cisco Trust Agent communication settings in the [EAPoUDP] section of the ctad.ini configuration file.

If the configuration file does not exist, the default values for these settings are used. To change the value for any of these items, you need to create the configuration file and save it to the appropriate location. For information about the default communication settings and how to create or edit the configuration file to change those settings, see "The ctad.ini Configuration File" section on page A-2 of Appendix A, "Cisco Trust Agent Configuration File Reference".

Any changes made to the [EAPoUDP] section of the ctad.ini configuration file are detected and implemented the next time the Cisco Trust Agent Event service restarts.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 32 of 81

Cisco Trust Agent Event Logging

Cisco Trust Agent can log events generated by Cisco Trust Agent components and the posture plugins for the NAC-compliant applications that reside on the system. By default, logging is not enabled.

This chapter contains the following sections:

- How Logging Works, page 5-1
- About Logging Configuration, page 5-2
- About Logging Levels, page 5-3
- About the Log Files, page 5-3
- Cisco Trust Agent Logging Command-line Interface, page 5-7
- Logging Considerations, page 5-9

How Logging Works

Event logging is implemented as a service on the network client. When the Cisco Trust Agent Event Logger service starts, it reads a configuration file to determine the logging settings. These settings include whether logging is enabled, the maximum size and location of the log file, and the level of logging for the various Cisco Trust Agent components. If the configuration file does not exist, the logging service uses the default values.

The Cisco Trust Agent Event Logging service receives event information from Cisco Trust Agent components and from the NAC-compliant applications that reside on the system. If logging is enabled, the events are evaluated against the

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 33 of 81

logging level set for the component that sent the event to determine if the event should be added to the log. Events that meet the logging level are formatted and written to the log file.

About Logging Configuration

Logging is configured with the ctalogd.ini configuration file. With this file, you can configure the following logging settings:

- The default logging state (enabled or disabled).
- The directory where the log file is stored.
- The maximum size of the log file. Once the log file reaches this size, it is closed and a new log file is created.
- The logging level for the Cisco Trust Agent components and posture plugins.

Note You can also change the logging state using the command line interface. See the "Cisco Trust Agent Logging Command-line Interface" section on page 5-7 for more information.

If the configuration file does not exist, the default values for these settings are used. To change the value for any of these items, you need to create the configuration file and save it to the appropriate location. For information about the default logging settings and how to create or edit the configuration file to change those settings, see the "The ctalogd.ini Configuration File" section on page A-6 of Appendix A, "Cisco Trust Agent Configuration File Reference".

Any changes made to the ctalogd.ini configuration file are detected and a implemented by the Cisco Trust Agent Event Logging service the next time it receives a log event.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 34 of 81

About Logging Levels

Setting the logging level determines which received events are added to the log file. You can choose the following logging levels for each component of Cisco Trust Agent:

- **1-LOW**—Low-level logging includes critical events.
- **2-MEDIUM**—Medium-level logging includes warnings and critical events.
- **3-HIGH**—High-level logging includes informational events, such as success messages, warnings, and critical events.
- **15-Debug**—Debug-level logging includes all events, including debug information from Cisco Trust Agent components. Debug-level logging is not available to posture plugins.

HIGH is the default level used when logging is enabled. You can change the logging level for each Cisco Trust Agent component in the [loglevel] section of the ctalogd.ini configuration file.

As a general guideline, when troubleshooting problems on systems running Cisco Trust Agent, you should set the logging level to High or Debug to receive the most information about the system operation. If you configure logging to be enabled by default, you should set the logging level to Medium or Low. Setting the logging level to medium or low prevents the log file from growing rapidly and consuming disk space, yet provides enough information to diagnose any problems with Cisco Trust Agent, posture plugins, or system posture.

About the Log Files

Cisco Trust Agent log files are text files created by the Cisco Trust Agent Event Logging service. They are simple ASCII text files that you can view using any text editor.

This section contains the following sections:

- Log File Creation and Naming, page 5-4
- Log File Format, page 5-5

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 35 of 81

Log File Creation and Naming

Log filenames are automatically generated by the event logger whenever a log file is created. A new log file is created whenever one of the following occurs:

- The Cisco Trust Agent Event Logging service is started or restarted while logging is enabled.
- The log file is cleared while logging is enabled.
- Logging is changed from disabled to enabled.
- The current log file reaches the maximum file size. The maximum file size 4 megabytes by default, but can be changed using the MaxFileSize parameter in the ctalogd.ini configuration file.

Note The actual creation of the log file does not occur until the first event is received while logging is enabled.

By default, log files are created in the `all_users_profile\Application Data\Cisco Systems\CiscoTrustAgent\Logs` directory (where *all_users_profile* is the path to the All Users profile directory). This location can be changed using the LogDir parameter in the ctalogd.ini configuration file.

Note To determine where the All Users profile is located on the target system, open a command prompt, enter **set**, and look for the ALLUSERSPROFILE= line in the output.

The file names use the date and time the event logger was started to create unique file names. The log file name have the following format: CTALOG-YYYY-MM-DDTHH-MM-SS_N.txt.

- **CTALOG**—A fixed prefix indicating that Cisco Trust Agent created the log.
- **YYYY**—A four-digit value for the year.
- **MM**—A two-digit value for the month.
- **DD**—A two-digit value for the day.
- **T**—A fixed separator between the date and time.
- **HH**—A two-digit value for the hours.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 36 of 81

- **MM**—A two-digit value for the minutes.
- **SS**—A two-digit value for the seconds.
- **N**—The nth log file created since the event logger was started. This occurs when the current log file reaches the maximum size or when logging is disabled and then enabled.

For example, if the event logger was started on 10/20/2003 at 17:12:58, the generated log file name would be `CTALOG-2003-10-20T17-12-58_1.txt`.

Log File Format

The log file contains the following fields:

- **Logging Instance**—An incremental number for the log entry.
- **Date/Time**—The date and time the entry was logged.
- **Severity**—The severity of the logged event. Valid severity values are:
  - Debug (not supported for plugins)
  - Critical
  - Informational
  - Warning
- **Log Level**—The logging level for the component that submitted the event. Valid values are:
  - 15 (Debug—not supported for plugins)
  - 1 (Low)
  - 2 (Medium)
  - 3 (High)
- **Component Name**—The name of the component that generated the event. The component names use one of the following conventions:
  - Vendor-ID:Application Name
  - Vendor Name: Application Name

  The Vendor-ID can be one of the following values:
  - **0**—Reserved

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 37 of 81

- **9**—Cisco Systems, Inc.
- **393**—Symantec Corporation
- **3401**—Network Associates, Inc.
- **6101**—Trend Micro, Inc.

For example, the component name for the Cisco Host Intrusion Protection System would appear as either 9:HIPS, where 9 is the vendor ID for Cisco and HIPS is the application name, or as Cisco:HIPS.

- **Error Code**—The error code associated with the event.
- **Message Body**—Text describing the event.

The following shows what a log file might look like:

```
Cisco Systems Trust Agent Version 1.0.14
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Trust Agent Type(s): Windows, WinNT Running on: 5.1.2600

1      15:29:57.748  09/13/03  Sev=Info/3  PADaemon/0x6300000C
Starting service:

2      15:29:58.779  09/13/03  Sev=Info/3  PADaemon/0x6300000E
Service initialization is complete

3      15:30:40.719  09/13/03  Sev=Info/3  NetTrans/0x63100016
NAD proposed AssociationID 56789

4      15:29:57.748  09/13/03  Sev=Info/3  9:HIP/0x00000001
Starting
```

Note Log entries are limited to 4 KB. Any event logs that exceed this size are truncated.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 38 of 81

Cisco Trust Agent Logging Command-line Interface

Cisco Trust Agent provides a command-line interface to event logging service. The command-line interface lets you programmatically control the logging service and enable or disable logging.

This section contains the following sections:

- About the CTALOGD Utility, page 5-7
- Enabling and Disabling Logging from the Command Line, page 5-8
- Clearing the Log File from the Command Line, page 5-9

About the CTALOGD Utility

The ctalogd utility lets you start, stop, and restart the logging service from the command line. It also lets you enable or disable logging and to clear the current log file from the command line.

Command Syntax

```
ctalogd {start| stop | restart | enable [-t] | disable | clear}
```

Command Options

Table 5-1 describes the command options for the ctalogd utility.

Table 5-1 ctalogd Utility Command Options

Option	Description
start	Starts the Cisco Trust Agent Event Logging service.
stop	Stops the Cisco Trust Agent Event Logging service.
restart	Restarts the Cisco Trust Agent Event Logging service.
enable	Enables logging. If the -t parameter is used with the enable option, logging is enable temporarily. Logging will be disabled when the logging service is restarted.
disable	Disables logging.
clear	Clears the current log file. A new log file is created if logging is enabled.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 39 of 81

Examples

The following examples assume that the commands are being executed from the directory where Cisco Trust Agent is installed.

- To clear the current log file, enter the following command:

  ctalogd clear

- To enable logging temporarily, enter the following command:

  ctalogd enable -t

- To restart the Cisco Trust Agent Event Logging service, enter the following command:

  ctalogd restart

Enabling and Disabling Logging from the Command Line

You can enable and disable logging from the command line. When you use the command line options, the ctalogd.ini configuration file is automatically updated to reflect the logging state.

To enable logging from the command line, follow these steps:

Step 1 Open a command prompt on the system.

Step 2 Change to the directory where Cisco Trust Agent is installed.

Step 3 To enable logging, enter **ctalogd enable**. This enables logging until you manually shut logging off.

To enable logging temporarily, enter **ctalogd enable -t**. This enables logging until the service is restarted.

Step 4 To disable logging, enter **ctalogd disable**.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 40 of 81

Clearing the Log File from the Command Line

You may need to clear the log file from the system if disk space is becoming low. You can also use the command line option to clear log files on a regular basis using a login script.

To clear the log file from the command prompt, follow these steps:

Step 1 Open a command prompt on the system.

Step 2 Change to the directory where Cisco Trust Agent is installed.

Step 3 Enter **ctalogd clear**.

The current log file is cleared from the system. If logging is enabled, a new log file is created when the next log event is received.

Logging Considerations

By default, log files are stored in the `all_users_profile\Application Data\Cisco Systems\CiscoTrustAgent\Logs` directory. This directory is available to all system users, including users with guest account privileges. If you want to limit access to the Cisco Trust Agent logs, you should change the location of the log file to a more secure area.

Log files are persistent. They remain on the disk until the user or administrator deletes them. If you enable a high-level of logging, you can potentially fill the disk over time. If you enable logging by default, you should make sure that a policy for regular log file removal or archival is in place. You can also use the command-line utility in a login script to clear the current log file on a regular basis.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 41 of 81

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 42 of 81

User Notifications

Notifications are the only part of Cisco Trust Agent that interact with the user. Users can copy and paste notification messages, which lets them to submit the exact message they receive if they request assistance.

This chapter contains the following sections:

- Notification Display, page 6-1
- About User Notification Configuration, page 6-2
- Logging Notifications, page 6-2

Notification Display

Based on the configuration, there are four possible states for notification display:

- **Disabled**—The user notification dialog box does not appear. The notification is still logged if logging is enabled and the message meets the minimum required log level.
- **Login Desktop Only**—The user notification dialog box only displays if the system is displaying the login desktop and nousers are logged in.
- **User Desktop Only**—The user notification dialog box only displays if a user is logged in. If no user is logged in when a notification is received, the notification will appear once a user logs in.
- **Login Screen and Desktop**—The user notification dialog box appears on the current desktop (login or user).

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 43 of 81

By default, the user notification dialog box is a system modal dialog box. This means that, while the dialog box displays, the user is unable to perform any action on the system except close the dialog box. You can change this setting so that the user can perform other actions on the system, such as logging in, without first having to close the dialog box.

Note If the user notification dialog box is set to system modal, and there is more than one notification message, only the newest message appears. Responding to the message closes all of the message dialog boxes.

About User Notification Configuration

User notifications are configured in the [UserNotifies] section of the ctad.ini configuration file. You can configure the following notification properties:

- When the notifications appear.
- How long the notification dialog box displays before automatically closing.
- Whether the notification is system modal.

If the configuration file does not exist, the default values for these settings are used. To change the value for any of these items, you need to create the configuration file and save it to the appropriate location. For information about the default notification settings and how to create or edit the configuration file to change those settings, see the "The ctad.ini Configuration File" section on page A-2 of Appendix A, "Cisco Trust Agent Configuration File Reference".

Any changes made to the [UserNotifies] of the ctad.ini configuration file are detected and implemented by Cisco Trust Agent the next time a notification is received.

Logging Notifications

If logging is enabled, the following events are logged:

- Notification failures, such as a failure to create the notification dialog box.
- User notification messages.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 44 of 81

The messages that are logged are filtered by the logging level assigned to the notification component of Cisco Trust Agent. This logging level is specified by the CTAMsg parameter in the [LogLevel] section of the ctalogd.ini configuration file. If this parameter does not appear in the configuration file, or if the configuration file does not exist, then a default level of 3 - High is used. This level allows all informational, warning, and critical messages to be written to the log file. The message severity is assigned by the component or plugin that sent the message.

For more information about logging, see Chapter 5, “Cisco Trust Agent Event Logging”.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 45 of 81

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 46 of 81

Security Posture Plugins

Security posture plugins are the means by which Cisco Trust Agent requests and receives security posture information from the NAC-compliant applications installed on the system. A posture plugin consists minimally of a .dll and a .inf file.

This chapter contains the following sections:

- Plugin Installation and Upgrade, page 7-1
- The Cisco Trust Agent Posture Plugin, page 7-3

Plugin Installation and Upgrade

Each NAC-compliant application is responsible for installing its own posture plugin in the `commonfiles\Cisco Systems\CiscoTrustAgent\Plugins\Install` directory, where *commonfiles* is the path to the Common Files directory. Typically, this directory is located here:

```
C:\Program Files\Common Files\Cisco Systems\CiscoTrustAgent\
Plugins\Install
```

Note To determine where the Common Files directory is located on the target system, open a command prompt, enter **set**, and look for the CommonProgramFiles= line in the output.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 47 of 81

Note Posture plugins can also be prepackaged with the Cisco Trust Agent installer. If there are prepackaged plugins in the Cisco Trust Agent installer, Cisco Trust Agent places them in the appropriate directory and registers them at install time.

When Cisco Trust Agent receives a posture request, it scans the Plugins/Install directory for new or updated posture plugins. If there are new or updated posture plugins in this directory, Cisco Trust Agent performs one of the following actions:

- If the plugin .dll does not exist in the Plugins directory Cisco Trust Agent registers the plugin and moves the plugin files to the Plugins directory.
- If the plugin .dll exists in the Plugins directory, then Cisco Trust Agent checks to see if the plugin in the Install directory is newer than the one in the plugins directory. If it is, Cisco Trust Agent registers the newer plugin and overwrites the older plugin. If the plugin in the Install directory is older than the one in the Plugins directory, Cisco Trust Agent deletes it and continues to use the original plugin.
- If the plugin creates an error during registration, Cisco Trust Agent moves the plugin to the `commonfiles\Cisco Systems\CiscoTrustAgent\Plugins\Quarantine` directory. If logging is enabled, the error information is logged.

Note Quarantined plugins do not participate in posture validation.

Cisco Trust Agent does not need to be installed for NAC-compliant applications to install their posture plugins. Because a common directory is used to store the plugins, Cisco Trust Agent can detect plugins that were installed prior to Cisco Trust Agent.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 48 of 81

The Cisco Trust Agent Posture Plugin

By default, Cisco Trust Agent installs and registers a basic posture plugin that provides the following security posture information:

- The posture agent name (Cisco Trust Agent).
- The posture agent version.
- The operating system name, such as “Windows XP Home Edition”.
- The operating system version.

This information can be used by Cisco Secure Access Control Server (ACS) to provide basic security posture assessment, even if there are no other NAC-compliant applications installed on the system. Refer to Appendix B, “Cisco Trust Agent Posture Plugin Reference” for more information about these security posture attributes and their associated values.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 49 of 81

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 50 of 81

Cisco Trust Agent Certificates

Cisco Trust Agent uses certificates to establish a PEAP session with the posture validation server (Cisco Secure Access Control Server (ACS)). You need to install the Cisco Secure ACS root certificate on the client system for this session to be established. This certificate is either a self-signed certificate generated by the Cisco Secure ACS server or a Certification Authority (CA) certificate used to authenticate the Cisco Secure ACS certificate.

Typically, this certificate is installed as part of a custom Cisco Trust Agent installation package. However, if it was not, Cisco Trust Agent provides a utility for installing and updating the posture validation server certificate on the client.

Note The Cisco Secure ACS certificate must have “server authentication” as the certificate purpose for the PEAP session to be created.

This chapter contains the following sections:

- Installing and Updating the Server Root Certificate, page 8-2
- About the ctaCert.exe Utility, page 8-3
- Distinguished Name Matching, page 8-4

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 51 of 81

Installing and Updating the Server Root Certifica

For Cisco Secure ACS to establish a secure PEAP session with Cisco Trust Agent, you must install the root certificate for the Cisco Secure ACS certificate on the network client. This certificate is either the CA certificate used to validate the server certificate, or a self-signed certificate generated by the Cisco Secure ACS server. Cisco Trust Agent supports PEM wrappered Base-64 or DER encoded binary X.509 certificates.

Before You Begin

You need to obtain the root certificate for the Cisco Secure ACS server certificate. If the Posture Validation Server (Cisco Secure ACS) uses self-signed certificates, obtain the certificate from the server. Refer to the Cisco Secure ACS documentation for information about obtaining the certificate. If you use a CA certificate, obtain the certificate from your certificate server.

To install the posture validation server certificate, follow these steps:

Step 1 Copy the certificate to the network client.

Step 2 Open a command prompt on the network client.

Step 3 Change directory to where Cisco Trust Agent is installed. By default, the location is `C:\Program Files\Cisco Systems\CiscoTrustAgent\`.

Step 4 Enter **`ctaCert.exe /add "cert_path" /store "Root"`**, where *cert_path* is the full path and file name to the certificate.

The certificate is added to the trusted certificate store on the network client.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 52 of 81

About the ctaCert.exe Utility

The ctaCert.exe utility enables you to import X.509 certificates. The ctaCert.exe utility can accept PEM wrappered Base-64 or DER encoded binary X.509 certificates. Use it to install or update the root certificate used by Cisco Trust Agent for PEAP sessions with Cisco Secure ACS.

Command Syntax

```
ctaCert.exe /ui {2 | 3| 4 | 5} /add "cert_path" /store "cert_store"
```

Command Parameters

Table 8-1 describes the command parameters for the ctaCert utility.

Table 8-1 ctaCert Utility Command Parameters

Parameter	Description
/ui	Specifies silent or verbose install. Accepts the following values: ù **2** or **3**—Silent installation. ù **4** or **5**—Full user interaction installation. Any other value entered is treated as full user interaction.
/add	Specifies the full path to the certificate being added. You can also specify *.cer to all certificates in the specified directory, for example: `c:\mycerts\*.cer`.
/store	Specifies the system certificate store. Typically this is “Root”.

Example

The following example assumes that the commands are being executed from the directory where Cisco Trust Agent is installed.

To add a certificate named csacs.cer, located in the c:\my certs\ directory, to the systems root certificate store, enter the following command:

```
ctaCert.exe /ui 2 /add "c:\my certs\csacs.cer" /store "Root"
```


INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 53 of 81

Distinguished Name Matching

When using CA certificates to validate your Cisco Secure ACS server certificate, you can implement additional security using distinguished name (DN) matching to validate the server certificate. This prevents other servers or processes that may be using the same root certificate from gaining a trust relationship with the network client.

DN matching occurs at the end of the TLS handshake, after the certificate chain is built.Invalid DN matching rules are ignored, but logged. Matched rules are logged. Failed rules are not logged.

DN matching rules are configured in the [ServerDNVerification] section of the ctad.ini configuration file. If the [ServerDNVerification] section does not exist, or if there are no rules configured, then the DN matching feature is disabled and the system accepts connections with any validated certificate chain. Otherwise, the server certificate must match one of the DN matching rules for the connection to continue.

If the configuration file does not exist, the default values for these settings are used. To change the value for any of these items, you need to create the configuration file and save it to the appropriate location. For information about the default notification settings and how to create or edit the configuration file to change those settings, see the "The ctad.ini Configuration File" section on page A-2 of Appendix A, "Cisco Trust Agent Configuration File Reference".

Any changes made to the [ServerDNVerification] section of the ctad.ini configuration file are detected and are implemented by Cisco Trust Agent the next time DN matching occurs.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 54 of 81

Cisco Trust Agent Configuration File Reference

Cisco Trust Agent uses two .ini files to configure its settings. If these configuration files are not present then Cisco Trust Agent uses the default settings for the missing values.

This chapter contains the following sections:

- Creating and Editing the Configuration Files, page A-1
- The ctad.ini Configuration File, page A-2
- The ctalogd.ini Configuration File, page A-6

Creating and Editing the Configuration Files

The easiest way to create the configuration files is to copy the examples provided in this section and paste them into a text editor. Then edit the values for the settings you want to change and delete the rest. Save the file to the location indicated in the description for each configuration file.

To edit an existing configuration, locate the file on the target system and open it in a text editor. Make the changes that you require and save the file. Changes to the configuration files take effect as follows:

- Changes to the ctalogd.ini file are implemented when the next log event occurs.
- Changes to the [EAPoUDP] section of the ctad.ini file are implemented when the Cisco Trust Agent service is restarted.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 55 of 81

- Changes to the [UserNotifies] section of the ctad.ini file are implemented when the next notification message is received.
- Changes to the [ServerCertDNVerification] section of the ctad.ini fileare implemented when the next DN matching occurs.

You can insert comments into the files. Use a semicolon (;) at the beginning of a line to indicate that the line is a comment and not part of the configuration.

The ctad.ini Configuration File

The ctad.ini configuration file contains the parameters for the Cisco Trust Agent communication settings, user notifications, and certificate filtering rules.

The ctad.ini configure file resides in the `install_path\Cisco Systems\CiscoTrustAgent\` directory, where *install_path* is the drive and directory where you installed Cisco Trust Agent.

This section contains the following sections:

- ctad.ini Sample, page A-2
- ctad.ini Settings, page A-3

ctad.ini Sample

The following example shows a ctad.ini file with the default values for each parameter.

Note There are no default settings for the [ServerCertDNVerification] section. Therefore, that section in this sample file contains example information. If you use this sample file as the basis for your own ctad.ini file, make sure you change or delete the [ServerCertDNVerification] section before saving it to the target system.

```
; ctad.ini sample
; use a semicolon at the beginning
; of a line to insert a comment
[EAPoUDP]
LocalPort=21862
MaxSession=8
```


INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 56 of 81

```
SessionIdleTimeout=600

[UserNotifies]
SysModal=1
EnableNotifies=1
MsgTimeout=300
EnableLogonNotifies=0
LogonMsgTimeout=0

[ServerCertDNVerification]
TotalRules=2
Rule1=CN*"server", ISSUER-CN*"Finance"
Rule2=CN="Finance posture Cert", OU*"Finance", ISSUER-CN*"ACME"
```

ctad.ini Settings

Table A-1 explains the sections and parameters used in the ctad.ini file.

Table A-1 The ctad.ini Parameter Settings

Keyword	Description
[EAPoUDP]	Section head for Cisco Trust Agent communication settings.
LocalPort	Specifies the Cisco Trust Agent listening port. Valid values range from 1 to 65550. The default value is 21862.
MaxSession	Specifies the maximum number of sessions supported by Cisco Trust Agent. Cisco Trust Agent only supports 1 established session per network access device, but can support sessions from multiple, different network access devices at the same time. Valid values range from 1 to 256. The default value is 8.
SessionIdleTimeout	Specifies the time, in seconds, after which an idle EAPoUDP session times out. Valid values range from 60 seconds to 2 days. The default value is 60 minutes.
[UserNotifies]	Section head for user notification parameters.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 57 of 81

Table A-1 The ctad.ini Parameter Settings (Continued)

Keyword	Description
SysModal	Specifies whether the user notification dialog boxes are modal or not. If they are modal, only the last notification received appears. The user must close the notification to be able to perform any other tasks on the desktop. This parameter only applies to logged-in users. It does not apply to notifications that may appear on the login desktop. ù 0 = Modal dialog boxes are disabled ù **1 = Modal dialog boxes are enabled (default)**
EnableNotifies	Enables/disables user notifications. This parameter applies to logged-in users. ù 0 = User notification are disabled ù **1 = User notifications are enabled (default)**
MsgTimeout	Specifies how long, in seconds, user notification dialog boxes are displayed. Valid values range from 30 to 4294967 seconds. Entering value of 0 disables the timeout. The default value for this setting is 30.
EnableLogonNotifies	Enables/disables user notifications. This parameter applies to notification at the login screen. ù **0 = User notification at the login screen are disabled (default)** ù 1 = User notifications at the login screen are enabled
LogonMsgTimeout	Specifies how long, in seconds, user notification dialog boxes at the login screen are displayed. Valid values range from 30 to 4294967 seconds. Entering value of 0 disables the timeout. The default value for this setting is 30.
[ServerCertDNVerification]	Section head for certificate distinguished name (DN) matching.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 58 of 81

Table A-1 The ctad.ini Parameter Settings (Continued)

Keyword	Description
TotalRules	The number of DN matching rules that follow. Valid values range from 0 to 64 rules. If TotalRules is 0, then DN matching is disabled. If the TotalRules is greater than 1, then the rules that follow are treated as if connected by an OR statement. Therefore, if one rule accepts the certificate, then the connection is accepted.
Rule*x*	A DN matching rule, where *x* is the index number for the rule. For example, the first rule is Rule1, the second rule is Rule2, and so on. See the "DN Matching Rule Syntax" section on page A-5 for information about writing DN matching rules.

DN Matching Rule Syntax

Each rule can contain multiple sub-rules, separated by a comma. If a single sub-rule within a rule fails, then the entire rule fails. The maximum length for a single rule is 255 characters.

The following shows the general format for a rule:

```
Rule1=subrule, subrule, subrule, ...
```

Each sub-rule consists of a certificate subject attribute followed by a value:

```
attribute[operator]"value"
```

The following operators are supported:

- **= (equals)**—The value must exactly match the value given in the subrule.
- *** (contains)**—The value must contain the value given in the subrule.

The following DN attributes are supported:

- **CN**—Common Name
- **SN**—Surname
- **GN**—Given Name
- **N**—Unstructured Name
- **I**—Initials

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 59 of 81

- **GENQ**—Generation Qualifier
- **C**—Country
- **L**—Locality
- **SP**—Province
- **ST**—State
- **O**—Organization
- **OU**—Organization Unit
- **T**—Title
- **EA**—E-mail Address

Note You can also create sub-rules that check certificate Issuer attributes by adding the ISSUER- prefix to the attributes listed above. For example, to validate the Common Name of certificate issuer, you would use the attribute ISSUER-CN.

See the "ctad.ini Sample" section on page A-2 for an example of DN matching rules.

The ctalogd.ini Configuration File

The ctalogd.ini file controls the aspects of Cisco Trust Agent logging. By default, logging is disabled. To enable logging, you need to create a ctalogd.ini file with a minimum of a [main] section and the EnableLog parameter set to 1.

The ctalogd.ini configure file resides in the `all_users_profile\Application Data\Cisco Systems\CiscoTrustAgent\` directory, where *all_users_profile* is the drive and directory where All Users user profile is located.

This section contains the following sections:

- ctalogd.ini Sample, page A-7
- ctalogd.ini Settings, page A-7

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 60 of 81

ctalogd.ini Sample

The following example shows a ctalogd.ini file with the default values for each parameter. Note that logging is disabled by default.

```
; ctalogd.ini sample
; use a semicolon at the beginning
; of a line to insert a comment
[main]
EnableLog=0
LogDir="c:\Documents and Settings\All Users\Application Data\
Cisco Systems\CiscoTrustAgent\logs"
MaxFileSize=4

[loglevel]
PADaemon=3
NetTrans=3
PAPlugin=3
CTAMsg=3
PEAP=3
EAPTLV=3
EAPSQ=3
PPMgr=3
Plugin=3
```

ctalogd.ini Settings

Table A-2 explains the sections and parameters used in the ctalogd.ini file.

Table A-2 The ctalogd.ini Parameter Settings

Keyword	Description
[main]	Required section head.
EnableLog	Enables/disables logging. ù **0 = Logging is disabled (default)** ù 1 = Logging is enabled (persistent) ù 2 = Logging is enabled temporarily

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 61 of 81

Table A-2 The ctalogd.ini Parameter Settings (Continued)

Keyword	Description
LogDir	Specifies the directory the event log files are created in. If this directory does not exist, you must create it before the log files can be created. Cisco Trust Agent does not create the directory for you.
MaxFileSize	Specifies the maximum log file size in megabytes. When a log file reaches this size, it is closed and a new log file is created. Valid values range from 0 to 4095. 0 specifies no limit to the log file size. 4 is the default value.
[loglevel]	Section head for the logging level parameters.
PADaemon	The Cisco Trust Agent service log level. ù 0 = Disable ù 1 = Low ù 2 = Medium ù **3 = High (default)** ù 15 = Everything
NetTrans	Network transport-specific log level. ù 0 = Disable ù 1 = Low ù 2 = Medium ù **3 = High (default)** ù 15 = Everything
PAPlugin	The Cisco Trust Agent Posture Plugin log level. ù 0 = Disable ù 1 = Low ù 2 = Medium ù **3 = High (default)** ù 15 = Everything

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 62 of 81

Table A-2 The ctalogd.ini Parameter Settings (Continued)

Keyword	Description
CTAMsg	Sets the logging level for the Cisco Trust Agent user notification module. ù 0 = Disable ù 1 = Low ù 2 = Medium ù **3 = High (default)** ù 15 = Everything
PEAP	Sets the logging level for the Cisco Trust Agent PEAP module. ù 0 = Disable ù 1 = Low ù 2 = Medium ù **3 = High (default)** ù 15 = Everything
EAPTLV	Sets the logging level for the Cisco Trust Agent TLV module. ù 0 = Disable ù 1 = Low ù 2 = Medium ù **3 = High (default)** ù 15 = Everything

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 63 of 81

Table A-2 The ctalogd.ini Parameter Settings (Continued)

Keyword	Description
EAPSQ	Sets the logging level for Cisco Trust Agent query log. ù 0 = Disable ù 1 = Low ù 2 = Medium ù **3 = High (default)** ù 15 = Everything
Plugin	Sets the logging level for all third-party plugins. ù 0 = Disable ù 1 = Low ù 2 = Medium ù **3 = High (default)**

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 64 of 81

Cisco Trust Agent Posture Plugin Reference

Use the information in Table B-1 when defining posture validation rules for the default Cisco Trust Agent plugin in Cisco Secure Access Control Server (ACS).

Table B-1 Cisco Trust Agent Posture Plugin Attributes and Values

Attribute	Value
Cisco:PA:OS-Version	The operating system version number in the format *major*.*minor*.*build-number*.0.
Cisco:PA:PA-Name	Cisco Trust Agent.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 65 of 81

Table B-1 Cisco Trust Agent Posture Plugin Attributes and Values (Continued)

Attribute	Value
Cisco:PA:PA-Version	The Cisco Trust Agent version number in the format *major*.*minor*.*build-number*.0.
Cisco:PA:OS-Type	The name of the host operating system: ù Windows Server 2003 Datacenter Edition ù Windows Server 2003 Enterprise Edition ù Windows Server 2003 Web Edition ù Windows Server 2003 Standard Edition ù Windows XP Home Edition ù Windows XP Professional ù Windows 2000 Datacenter Server ù Windows 2000 Advanced Server ù Windows 2000 Server ù Windows NT Workstation 4.0 ù Windows NT Server 4.0, Enterprise Edition ù Windows NT Server 4.0 ù Windows NT 4.0 ù Windows NT 3.51 ù Windows 95 ù Windows 95 OSR2 ù Windows 98 ù Windows 98 SE ù Windows Me

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 66 of 81

System Change Reference

This section describes the changes that are made to network clients when Cisco Trust Agent is installed. Table C-1 lists the directories that are created and the files that are installed.

Table C-1 Cisco Trust Agent Directories and Files

Directory	Description
all_users_profile\Application Data\Cisco Systems\CiscoTrustAgent\	The directory where the logging configuration file, ctalogd.ini, is stored. This file only appears if provisioned in the initial install package or added later by an administrator. By default, a file named ctalogd.tmp is installed in this directory. This is a sample logging configuration file that you can use by changing the name to ctalogd.ini. Edit the file to suit your needs. The default location for this directory is `c:\Documents and Settings\All Users\Application Data\Cisco Systems\CiscoTrustAgent\`.
all_users_profile\Application Data\Cisco Systems\CiscoTrustAgent\Logs\	The directory where Cisco Trust Agent creates the log files. Cisco Trust Agent does not create log files until logging is enabled and a logging event is received.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 67 of 81

Table C-1 Cisco Trust Agent Directories and Files (Continued)

Directory	Description
install_path\Cisco Systems\CiscoTrustAgent\	The directory where the Cisco Trust Agent application is installed. The default installation directory is `c:\Program Files\Cisco Systems\CiscoTrustAgent\` The following files are installed in this directory: ù **ctad.exe**—The Cisco Trust Agent service. ù **acsPEAP.dll**—The PEAP module. ù **EapSQ.dll**—The EAP Status Query module. ù **eapTLV.dll**—The EAP-TLV module. ù **ctaCert.exe**—The certificate registration utility. ù **ctamsg.exe**—The Cisco Trust Agent user notification module. ù **ctalogd.exe**—The Cisco Trust Agent logging service. ù **license.txt**—The Cisco Trust Agent end-user license agreement. ù **ctad.ini**—The Cisco Trust Agent configuration file. This configuration file controls the communication settings, user notification settings, and certificate DN matching rules. This file only appears if provisioned in the initial install package or added later by an administrator.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 68 of 81

Table C-1 Cisco Trust Agent Directories and Files (Continued)

Directory	Description
common_files\Cisco Systems\CiscoTrustAgent\Plugins\	The directory where the registered plugins are installed. This directory contains two subdirectories: ù **Install**—NAC-compliant applications install there plugins in this directory. When Cisco Trust Agent receives a posture request, it registers the plugins in this directory and moves them to the Plugins directory. ù **Quarantined**—Plugins that cause exception errors are moved to this directory. Quarantined plugins do not participate in posture validation.

Cisco Trust Agent creates the following entries in the Windows registry during installation:

- **Cisco Trust Agent Service**—\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ctad
- **Cisco Trust Agent Logging Service**—\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ctalogd
- **Cisco Trust Agent MSI Product Code**—This registry key provides a globally unique product ID code to Cisco Trust Agent.

  \HKEY_LOCAL_MACHINE\SOFTWARE\CiscoSystems\Cisco Trust Agent\ProductCode\
- **Cisco Trust Agent Install Paths**—This registry entry provide the keys that contain paths to the Cisco Trust Agent installation directory and the directories where the configuration files and the posture plugins are stored.

  \HKEY_LOCAL_MACHINE\SOFTWARE\CiscoSystems\Cisco Trust Agent\
- **MSI Uninstall Information**—\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*Product_Code*

  Product_Code indicates the code listed in the Cisco Trust Agent MSI Product Code key.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 69 of 81

- **MSI Install Information**—Like the MSI Uninstall Information registry location, the MSI Install Information uses Cisco Trust Agent MSI Product Code to store the registry keys. However, it scrambles the key. The easiest way to find the MSI installer registry entries for Cisco Trust Agent is to search the following registry area for the phrase "Cisco Trust Agent" (without the quotes):

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\

  The results of the search show you which code under the above registry area contains the Cisco Trust Agent MSI install information.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 70 of 81

Open Source License Acknowledgement

Cisco Trust Agent uses third-party, open-source software subject to the following licenses:

OpenSSL

```
  LICENSE ISSUES
  ==============

  The OpenSSL toolkit stays under a dual license, i.e. both the conditions of
  the OpenSSL License and the original SSLeay license apply to the toolkit.
  See below for the actual license texts. Actually both licenses are BSD-style
  Open Source licenses. In case of any license issues related to OpenSSL
  please contact openssl-core@openssl.org.

  OpenSSL License
  ---------------

/* ====================================================================
 * Copyright (c) 1998-2003 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
```


INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 71 of 81

```
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
```


INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 72 of 81

```
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to.  The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code.  The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)"
*    The word 'cryptographic' can be left out if the rouines from the library
*    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*    the apps directory (application code) you must include an acknowledgement:
*    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
```


INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 73 of 81

```
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

Info-ZIP

This is version 2004-May-22 of the Info-ZIP copyright and license. The definitive version of this document should be available at ftp://ftp.info-zip.org/pub/infozip/license.html indefinitely.

Copyright (c) 1990-2004 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Christian Spieler, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 74 of 81

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 75 of 81

Info-ZIP

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 76 of 81

Symbols

[EAPoUDP] section A-3
[loglevel] section A-8
[main] section A-7
[ServerCertDNVerification] section A-4
[UserNotifies] section A-3

A

authentication servers 1-2

C

certificates
  ctaCert.exe utility 8-3
  DN matching A-5
  in a custom installation package 2-2
  installing 8-2
  obtaining from Cisco Secure ACS 8-2
  updating 8-2
  use with Cisco Trust Agent 8-1
Cisco Trust Agent
  deployment considerations 1-3
communication settings
  about 4-1
  configurable 4-1
  configuring 4-2
  listening port 4-1
  sessions 4-1
  session timeout 4-1
configuration files
  creating A-1
  ctad.ini A-2
  ctad.ini sample A-2
  ctalogd.ini A-6
  editing A-1
  reference A-1
  when changes apply A-1
ctaCert.exe
  about 8-3
  example 8-3
  parameters 8-3
  syntax 8-3
ctad.ini
  about A-2
  in a custom installation package 2-3
  location A-2
  sample file A-2
  settings A-3

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 77 of 81

ctalogd
about 5-7
options 5-7
syntax 5-7
using from the command-line 5-8
ctalogd.ini
about A-6
in a custom installation package 2-3
location A-6
parameters A-7
sample file A-7
CTAMsg parameter A-9
ctasetup.exe
in a custom installation package 2-2
custom installation package
components 2-1
creating 2-4
overview 2-1

D

default posture plugin
about 7-3
attributes B-1
deploying cisco trust agent 1-4
directories
created during install C-1
distinguished name matching
See DN matching
DN matching
about 8-4,A-5
about rules 8-4
attributes supported A-5
Issuer attributes A-6
rule length A-5
rules A-5
sub-rule operators A-5
sub-rules A-5
when occurs 8-4
document
conventions ix
documentation
related x

E

EAPSQ parameter A-10
EAPTLV parameter A-9
EnableLogonNotifies parameter A-4
EnableLog parameter A-7
EnableNotifies parameter A-4

F

files
created during install C-1

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 78 of 81

I

Info-ZIP
license D-4
installation
certificates 3-4
creating a custom package 2-4
custom package components 2-1
custom package overview 2-1
directories created during C-1
files created during C-1
registry entries C-3
time savers 1-4
verifying 3-5
instmsiw.exe
in a custom installation package 2-4

L

licenses
for open-source software D-1
Info-ZIP D-4
OpenSSL D-1
SSLeay D-2
listening port 4-1
LocalPort parameter A-3
LogDir parameter A-8
log files
about 5-3
creating 5-4
format 5-5
location 5-9
naming 5-4
persistence 5-9
logging
about 5-1
command-line interface 5-7
configuration 5-2
considerations 5-9
disabling from the command line 5-8
enabling from the command-line 5-8
levels of 5-3
log files 5-3
notifications 6-2
overview 5-1
LogonMsgTimeout parameter A-4

M

MaxFileSize parameter A-8
MaxSession parameter A-3
MsgTimeout parameter A-4

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 79 of 81

N

NAC
compatibility 3-2
NAD
See network access devices
NetTrans parameter A-8
Network Access Control
Overview 1-1
network access devices 1-1
network clients 1-1
notifications
about 6-1
configuration 6-2
how displayed 6-1
logging 6-2

O

open source
software licenses D-1
OpenSSL
license D-1
OS-Type attribute B-2
OS-version attribute B-1

P

PADaemon parameter A-8
PA-Name attribute B-1
PAPlugin parameter A-8
PA-Version attribute B-2
PEAP parameter A-9
Plugin parameter A-10
port 4-1
posture plugins
about 7-1
Cisco Trust Agent default B-1
in a custom installation package 2-2
installing 7-1
process overview 7-2
upgrading 7-1
posture validation
authentication servers 1-2
components of 1-1
definition 1-1
network access devices 1-1
network clients 1-1
posture validation servers 1-2
process 1-2 to 1-3
posture validation servers 1-2

R

registry entries
created during install C-3
related documentation x

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 80 of 81

removing Cisco Trust Agent 3-5
Rule parameter A-5

S

SessionIdleTimeout parameter A-3
SSLeay
  license D-2
SysModal parameter A-4

W

Windows Installer
  in a custom installation package 2-4

INFOEXPRESS, INC. - EX2550
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00539]
Page 81 of 81