RAPID7

Nexpose

User's Guide

Product version: 5.16

Wiz - EXHIBIT 1122
Wiz, Inc. v. Orca Security Ltd.
IPR2024-00863

Table of contents

Table of contents 2

Revision history 16

About this guide 20

A note about documented features 20

Document conventions 20

For technical support 21

Getting Started 22

Running the application 23

Manually starting or stopping in Windows 23

Changing the configuration for starting automatically as a service 24

Manually starting or stopping in Linux 24

Working with the daemon 24

Using the Web interface 26

Activating and updating on private networks 26

Logging on 26

Navigating the Security Console Web interface 28

Using the search feature 34

Accessing operations faster with the Administration page 39

Using configuration panels 41

Extending Web interface sessions 41

Troubleshooting your activation 41

Discover 45

What is a site? 47

Different ways to add assets to a site 47

How are sites different from asset groups? 48

Site creation scenarios 49

Default settings 49

Find out what you have: Discovery scan 50

Get an outside view of your environment 52

Zero-day vulnerabilities 54

Assets in multiple locations 56

Large numbers of assets 56

Amazon Web Services 56

VMWare 56

Internal PCI compliance scans 57

Policy benchmarks 59

Creating and editing sites 60

Getting started: Info & Security 61

Giving users access to a site 63

Adding assets to sites 65

Specifying assets by Names/Addresses 65

Adding assets by connection 68

Best practices for adding assets to a site 70

Choosing a grouping strategy for creating a site with manually selected assets 70

Selecting a Scan Engine or engine pool for a site 75

Configuring distributed Scan Engines 78

Before you configure and pair a distributed Scan Engine 78

Configuring the Security Console to work with a new Scan Engine 78

Adding an engine 78

Pairing the Scan Engine with the Security Console 80

Assigning a site to the new Scan Engine 82

Working with Scan Engine pools 83

Selecting a scan template 87

Selecting a scan template 88

Targeted scanning: using multiple templates in a site 91

The benefits 91

How targeted scanning works 91

Configuring scan credentials 93

Maximizing security with credentials 96

Security best practices on Windows 96

Configuring site-specific scan credentials 97

Managing shared scan credentials 103

Using SSH public key authentication 108

Elevating permissions 112

Using LM/NTLM hash authentication 116

Using PowerShell with your scans 119

Authentication on Windows: best practices 122

Authentication on Unix and related targets: best practices 124

Configuring scan authentication on target Web applications 133

Creating a logon for Web site form authentication 134

Creating a logon for Web site session authentication with HTTP headers 138

Setting up scan alerts 143

Scheduling scans 145

Scan blackouts 150

- Creating a site-level blackout 150
- Managing site-level blackouts 152
- Creating a global blackout 153
- Managing global blackouts 154

Deleting sites 156

Managing dynamic discovery of assets 157

- What is Dynamic Discovery, and why use it? 157
- Verifying that your license enables relevant features 158
- Discovering mobile devices 159

Discovering Amazon Web Services instances 164
Discovering virtual machines managed by VMware vCenter or ESX/ESXi 167
Discovering assets through DHCP log queries 169
Creating and managing Dynamic Discovery connections 170
Initiating Dynamic Discovery 183
Using filters to refine Dynamic Discovery 186
Monitoring Dynamic Discovery 199
Configuring a dynamic site 200
Integrating NSX network virtualization with scans 203
Activities in an NSX-integrated site 203
Requirements for the vAsset Scan feature 204
Deployment steps for the vAsset Scan feature 204
Importing AppSpider scan data 219
Running a manual scan 222
Monitoring the progress and status of a scan 223
Understanding different Scan Engine statuses 227
Understanding different scan states 227
Pausing, resuming, and stopping a scan 229
Viewing scan results 230
Viewing the scan log 231
Tracking scan events in logs 233

Viewing history for all scans 238

Assess 239

Locating and working with assets 240

Viewing asset counts and statistics 240

Comparing scanned and discovered assets 242

Locating assets by sites 243

Locating assets by asset groups 246

Locating assets by operating systems 246

Locating assets by software 247

Locating assets by services 248

Viewing the details about an asset 248

Deleting assets 250

Applying RealContext with tags 254

Types of tags 255

Tagging assets, sites, and asset groups 255

Applying business context with dynamic asset filters 257

Removing and deleting tags 259

Changing the criticality of an asset 261

Creating tags without applying them 262

Avoiding "circular references" when tagging asset groups 263

Working with vulnerabilities 265

Viewing active vulnerabilities 265
Filtering your view of vulnerabilities 269
Viewing vulnerability details 274
Working with validated vulnerabilities 276
Working with vulnerability exceptions 279
Understanding cases for excluding vulnerabilities 279
Understanding vulnerability exception permissions 280
Understanding vulnerability exception status and work flow 281
Working with Policy Manager results 297
Getting an overview of Policy Manager results 298
Viewing results for a Policy Manager policy 300
Viewing information about policy rules 301
Overriding rule test results 303
Act 314
Working with asset groups 315
Comparing dynamic and static asset groups 317
Configuring a static asset group by manually selecting assets 318
Creating a dynamic or static asset group by copying an existing one 321
Performing filtered asset searches 324
Configuring asset search filters 324
Creating a dynamic or static asset group from asset searches 348

Changing asset membership in a dynamic asset group 350

Working with reports 351

Viewing, editing, and running reports 353

Creating a basic report 356

Starting a new report configuration 356

Entering CyberScope information 361

Configuring an XCCDF report 361

Configuring an Asset Reporting Format (ARF) export 363

Selecting assets to report on 363

Filtering report scope with vulnerabilities 365

Configuring report frequency 372

Best practices for using the Vulnerability Trends report template 374

Saving or running the newly configured report 375

Selecting a scan as a baseline 376

Working with risk trends in reports 378

Events that impact risk trends 378

Configuring reports to reflect risk trends 379

Selecting risk trends to be included in the report 380

Creating reports based on SQL queries 383

Prerequisites 383

Defining a query and running a report 383

Understanding the reporting data model: Overview and query design 387
Overview 387
Query design 388
Understanding the reporting data model: Facts 394
Understanding the reporting data model: Dimensions 462
Junk Scope Dimensions 462
Core Entity Dimensions 466
Enumerated and Constant Dimensions 504
Understanding the reporting data model: Functions 521
Distributing, sharing, and exporting reports 525
Working with report owners 525
Managing the sharing of reports 527
Granting users the report-sharing permission 529
Restricting report sections 534
Exporting scan data to external databases 537
Configuring data warehousing settings 538
For ASVs: Consolidating three report templates into one custom template 539
Configuring custom report templates 543
Creating a custom report template based on an existing template 546
Adding a custom logo to your report 547
Working with externally created report templates 549

Working with report formats 551
Working with human-readable formats 551
Working with XML formats 551
Working with CSV export 554
How vulnerability exceptions appear in XML and CSV formats 558
Working with the database export format 563
Understanding report content 564
Scan settings can affect report data 565
Understanding how vulnerabilities are characterized according to certainty 566
Looking beyond vulnerabilities 567
Using report data to prioritize remediation 567
Using tickets 569
Viewing tickets 569
Creating and updating tickets 569
Tune 571
Working with scan templates and tuning scan performance 572
Defining your goals for tuning 573
The primary tuning tool: the scan template 578
Configuring custom scan templates 582
Starting a new custom scan template 584
Selecting the type of scanning you want to do 584

Tuning performance with simultaneous scan tasks 585

Configuring asset discovery 588

Determining if target assets are live 588

Fine-tuning scans with verification of live assets 590

Ports used for asset discovery 590

Configuration steps for verifying live assets 590

Collecting information about discovered assets 591

Finding other assets on the network 591

Fingerprinting TCP/IP stacks 591

Reporting unauthorized MAC addresses 592

Enabling authenticated scans of SNMP services 593

Creating a list of authorized MAC addresses 594

Configuring service discovery 596

Performance considerations for port scanning 596

Changing discovery performance settings 598

Selecting vulnerability checks 602

Configuration steps for vulnerability check settings 603

Using a plug-in to manage custom checks 607

Selecting Policy Manager checks 608

Configuring verification of standard policies 611

Configuring Web spidering 615

Configuration steps and options for Web spidering 616
Fine-tuning Web spidering 619
Configuring scans of various types of servers 620
Configuring spam relaying settings 620
Configuring scans of database servers 621
Configuring scans of mail servers 622
Configuring scans of CVS servers 622
Configuring scans of DHCP servers 622
Configuring scans of Telnet servers 623
Configuring file searches on target systems 624
Using other tuning options 625
Change Scan Engine deployment 625
Edit site configuration 625
Make your environment “scan-friendly” 626
Open firewalls on Windows scan targets 626
Managing certificates for scanning 627
Importing custom certificates 627
Removing certificates 629
Creating a custom policy 631
Uploading custom SCAP policies 642
File specifications 642

Version and file name conventions 644
Uploading SCAP policies 644
Uploading specific benchmarks or datastreams 646
Troubleshooting upload errors 646
Working with risk strategies to analyze threats 652
Comparing risk strategies 653
Changing your risk strategy and recalculating past scan data 658
Using custom risk strategies 660
Setting the appearance order for a risk strategy 661
Changing the appearance order of risk strategies 662
Understanding how risk scoring works with scans 664
Adjusting risk with criticality 665
Interaction with risk strategy 666
Viewing risk scores 667
Sending custom fingerprints to paired Scan Engines 668
Ensuring correct formatting for the fingerprints 668
Resources 670
Finding out what features your license supports 671
Linking assets across sites 672
Option 1 672
Option 2 672

What exactly is an "asset"? 673
Do I want to link assets across sites? 673
Enabling or disabling asset linking across sites 676
Using regular expressions 678
General notes about creating a regex 678
How the file name search works with regex 679
How to use regular expressions when logging on to a Web site 680
Using Exploit Exposure 681
Why exploit your own vulnerabilities? 681
Performing configuration assessment 682
Scan templates 684
Report templates and sections 689
Built-in report templates and included sections 689
Document report sections 704
Export template attributes 712
Glossary 718

Revision history

Copyright © 2015 Rapid7, LLC. Boston, Massachusetts, USA. All rights reserved. Rapid7 and Nexpose are trademarks of Rapid7, Inc. Other names appearing in this content may be trademarks of their respective owners.

For internal use only.

Revision date	Description
June 15, 2010	Created document.
August 30, 2010	Added information about new PCI-mandated report templates to be used by ASVs as of September 1, 2010; clarified how CVSS scores relate to severity rankings.
October 25, 2010	Added more detailed instructions about specifying a directory for stored reports.
December 13, 2010	Added instructions for SSH public key authentication.
December 20, 2010	Added instructions for using Asset Filter search and creating dynamic asset groups. Also added instructions for using new asset search features when creating static asset groups and reports.
January 31, 2011	Added information about new PCI report sections and the PCI Host Details report template.
March 14, 2011	Added information about including organization information in site configuration and managing assets according to host type.
July 11, 2011	Added information about expanded vulnerability exception workflows.
July 25, 2011	Updated information about supported browsers.
September 19, 2011	Updated information about using custom report logos.
November 15, 2011	Added information about viewing and overriding policy results.
December 5, 2011	Added information about downloading scan logs.

Revision date	Description
January 23, 2012	Nexpose 5.1: Added information about viewing Advanced Policy Engine compliance across your enterprise, using LM/NTLM hash authentication for scans, and exporting malware and exploit information to CSV files.
March 21, 2012	Nexpose 5.2: Added information about drilling down to view Advanced Policy Engine policy compliance results using the Policies dashboard. Corrected the severity ranking values in the Severity column. Updated information about supported browsers.
June 6, 2012	Nexpose 5.3: Added information on scan template configuration, including new discovery performance settings for scan templates; CyberScope XML Export report format; vAsset discovery; appendix on using regular expressions.
August 8, 2012	Nexpose 5.4: Added information vulnerability category filtering in reports and customization of advanced policies.
December 10, 2012	Nexpose 5.5: Added information about working with custom report templates, uploading custom SCAP templates, and working with configuration assessment. Updated workflows for creating, editing and distributing reports. Updated the glossary with new entries for top 10 report templates and shared scan credentials.
April 24, 2013	Nexpose 5.6: Added information about elevating permissions.
May 29, 2013	Updated Web spider scan template settings.
July 17, 2013	Nexpose 5.7: Added information about creating multiple vulnerability exceptions and deleting multiple assets. Added information about Vulnerability Trends Survey report template. Added information about new scan log entries for asset and service discovery phases
July 31, 2013	Deleted references to a deprecated feature.
September 18, 2013	Added information about vulnerability display filters.

Revision date	Description
November 13, 2013	Added information about validating vulnerabilities.
December 4, 2013	Nexpose 5.8: Added information about new Administration page, language selection options, SCAP 1.2 support, open port asset search filter, and last logon date in user configuration table.
January 8, 2014	Added information about using the Reporting Data Model to create CSV export reports based on SQL queries.
March 26, 2014	Nexpose 5.9: Added information about RealContext.
April 9, 2014	Added information about tag-related elements to Reporting Data Model.
August 6, 2014	Nexpose 5.10: Added information about policy rule results in Reporting Data Model and about new, interactive charts. Updated document look and feel.
August 13, 2014	Added information on specific permissions required for scanning Unix and related targets.
August 20, 2014	Added information about non-exploitable slice for asset pie chart.
September 10, 2014	Added information about VMware NSX integration.
September 17, 2014	Added a link to a white paper on security strategies for managing authenticated scans on Windows targets.
October 10, 2014	Made minor formatting changes.
October 22, 2014	Nexpose 5.11: Added information about Scan Engine pooling, update scheduling, and cumulative scan results.
November 5, 2014	Added PCI executive summary content to the Reporting Data model.
December 10, 2014	Published PDF for localization.
December 23, 2014	Updated information about upcoming targeted scanning feature and support for VMware NSX versions for integration with Nexpose.

Revision date	Description
January 28, 2015	Nexpose 5.12: Added information about new *Site Configuration* panel and import option for custom Root certificates. Reorganized section on configuring sites and added section on scenarios for creating sites for specific use cases.
April 8, 2015	Nexpose 5.13: Added information about Dynamic Discovery of via ActiveSync for mobile devices and via DHCP log queries for other assets; asset group scanning; linking matching assets across sites; scan scheduling enhancements.
May 27, 2015	Nexpose5.14: Added information about scan schedule blackouts.
June 24, 2015	Nexpose 5.15: Added content on "listening" for syslog data as a collection method and using Infoblox Trinzic DDI as a data source for dynamic discovery via DHCP log queries. See *Discovering assets through DHCP log queries* on page 169. Added content on *Importing AppSpider scan data* on page 219. Added protocol_id column to to dim_asset_service_credential. See *Understanding the reporting data model: Dimensions* on page 462.
July 29, 2015	Nexpose 5.16: Added instructions for *Sending custom fingerprints to paired Scan Engines* on page 668. Added information about Reporting data model version 2.0.1, which enables SQL queries on mobile device data. See *dim_mobile_asset_attribute* on page 475.

About this guide

This guide helps you to gather and distribute information about your network assets, vulnerabilities, and configuration compliance using Nexpose. It covers the following activities:

- logging onto the Security Console and navigating the Web interface
- setting up a site
- running scans
- managing Dynamic Discovery
- viewing asset and vulnerability data
- applying Real Context with tags
- creating remediation tickets
- creating reports
- reading and interpreting report data

A note about documented features

All features documented in this guide are available in the Nexpose Enterprise edition. Certain features are not available in other editions. For a comparison of features available in different editions see http://www.rapid7.com/products/nexpose/compare-editions.jsp.

Document conventions

Words in bold are names of hypertext links and controls.

Words in italics are document titles, chapter titles, and names of Web interface pages.

Steps of procedures are indented and are numbered.

Items in `Courier font` are commands, command examples, and directory paths.

Items in **`bold Courier font`** are commands you enter.

Variables in command examples are enclosed in box brackets.
Example: `[installer_file_name]`

Options in commands are separated by pipes. Example:

```
$ /etc/init.d/[daemon_name] start|stop|restart
```

Keyboard commands are bold and are enclosed in arrow brackets.Example:
Press and hold **<Ctrl + Delete>**

Note: NOTES contain information that enhances a description or a procedure and provides additional details that only apply in certain cases.

Tip: TIPS provide hints, best practices, or techniques for completing a task.

Warning: WARNINGS provide information about how to avoid potential data loss or damage or a loss of system integrity.

Throughout this document, Nexpose is referred to as *the application*.

For technical support

- Send an e-mail to support@rapid7.com (Enterprise and Express Editions only).
- Click the **Support** link on the Security Console Web interface.
- Go to community.rapid7.com.

Getting Started

If you haven't used the application before, this section helps you to become familiar with the Web interface, which you will need for running scans, creating reports, and performing other important operations.

- *Running the application* on page 23: By default, the application is configured to run automatically in the background. If you need to stop and start it automatically, or manage the application service or daemon, this section shows you how.
- *Using the Web interface* on page 26: This section guides you through logging on, navigating the Web interface, using configuration panels, and running searches.

Running the application

This section includes the following topics to help you get started with the application:

- *Manually starting or stopping in Windows* on page 23
- *Changing the configuration for starting automatically as a service* on page 24
- *Manually starting or stopping in Linux* on page 24
- *Working with the daemon* on page 24

Manually starting or stopping in Windows

Nexpose is configured to start automatically when the host system starts. If you disabled the initialize/start option as part of the installation, or if you have configured your system to not start automatically as a service when the host system starts, you will need to start it manually.

Starting the Security Console for the first time will take 10 to 30 minutes because the database of vulnerabilities has to be initialized. You may log on to the Security Console Web interface immediately after the startup process has completed.

If you have disabled automatic startup, use the following procedure to start the application manually:

1. Click the **Windows Start** button
2. Go to the application folder.
3. Select **Start Services**.

Use the following procedure to stop the application manually:

1. Click the **Windows Start** button.
2. Open the application folder.
3. Click the **Stop Services** icon.

Changing the configuration for starting automatically as a service

By default the application starts automatically as a service when Windows starts. You can disable this feature and control when the application starts and stops.

1. Click the **Windows Start** button, and select **Run...**
2. Type services.msc in the *Run* dialog box.
3. Click **OK**.
4. Double-click the icon for the Security Console service in the *Services* pane.
5. Select *Manual* from the drop-down list for **Startup type:**
6. Click **OK**.
7. Close *Services*.

Manually starting or stopping in Linux

If you disabled the initialize/start option as part of the installation, you need to start the application manually.

Starting the Security Console for the first time will take 10 to 30 minutes because the database of vulnerabilities is initializing. You can log on to the Security Console Web interface immediately after startup has completed.

To start the application from graphical user interface, double-click the Nexposein the *Internet* folder of the *Applications* menu.

To start the application from the command line, take the following steps:

1. Go to the directory that contains the script that starts the application:

   ```
   $ cd [installation_directory]/nsc
   ```
2. Run the script: `./nsc.sh`

Working with the daemon

The installation creates a daemon named *nexposeconsole.rc* in the /etc/init.d/ directory.

WARNING: Do not use <**CTRL+C**>, it will stop the application.

To detach from a screen session, press <CTRL +A + D>.

Manually starting, stopping, or restarting the daemon

To manually start, stop, or restart the application as a daemon:

1. Go to the /nsc directory in the installation directory:

   cd [installation_directory]/nsc

2. Run the script to start, stop, or restart the daemon. For the Security Console, the script file name is *nscsvc*. For a scan engine, the service name is *nsesvc*:

   ```
   ./[service_name] start|stop
   ```

Preventing the daemon from automatically starting with the host system

To prevent the application daemon from automatically starting when the host system starts, run the following command:

```
$ update-rc.d [daemon_name] remove
```

Using the Web interface

This section includes the following topics to help you access and navigate the Security Console Web interface:

- *Logging on* on page 26
- *Navigating the Security Console Web interface* on page 28
- *Using the search feature* on page 34
- *Using configuration panels* on page 41
- *Extending Web interface sessions* on page 41

Activating and updating on private networks

If your Security Console is not connected to the Internet, you can find directions on updating and activating on private networks. See the topic *Managing versions, updates, and licenses* in the administrator's guide.

Logging on

The Security Console Web interface supports the following browsers:

- Internet Explorer, versions 9.0.x, 10.x, and 11.x
- Mozilla Firefox, version 24.x
- Google Chrome, most current, stable version

If you received a product key, via e-mail use the following steps to log on. You will enter the product key during this procedure. You can copy the key from the e-mail and paste it into the text box; or you can enter it with or without hyphens. Whether you choose to include or omit hyphens, do so consistently for all four sets of numerals.

If you do not have a product key, click the link to request one. Doing so will open a page on the Rapid7 Web site, where you can register to receive a key by e-mail. After you receive the product key, log on to the Security Console interface again and follow this procedure.

If you are a first-time user and have not yet activated your license, you will need the product key that was sent to you to activate your license after you log on.

To log on to the Security Console take the following steps:

1. Start a Web browser.

   If you are running the browser on the same computer as the console, go to the following URL: `https://localhost:3780`

   Indicate HTTPS protocol and to specify port 3780.

   If you are running the browser on a separate computer, substitute `localhost` with the correct host name or IP address.

   Your browser displays the *Logon* window.

Tip: If there is a usage conflict for port 3780, you can specify another available port in the *httpd.xml* file, located in [installation_directory]\nsc\conf. You also can switch the port after you log on. See the topic *Changing the Security Console Web server default settings* in the administrator's guide.

Note: If the logon window indicates that the Security Console is in maintenance mode, then either an error has occurred in the startup process, or a maintenance task is running. See *Running in maintenance mode* in the administrator's guide.

2. Enter your user name and password that you specified during installation.

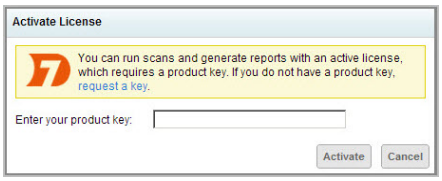
   User names and passwords are case-sensitive and non-recoverable.



Logon window

3. Click the **Logon** button.

   If you are a first-time user and have not yet activated your license, the Security Console displays an activation dialog box. Follow the instructions to enter your product key.



Activate License window

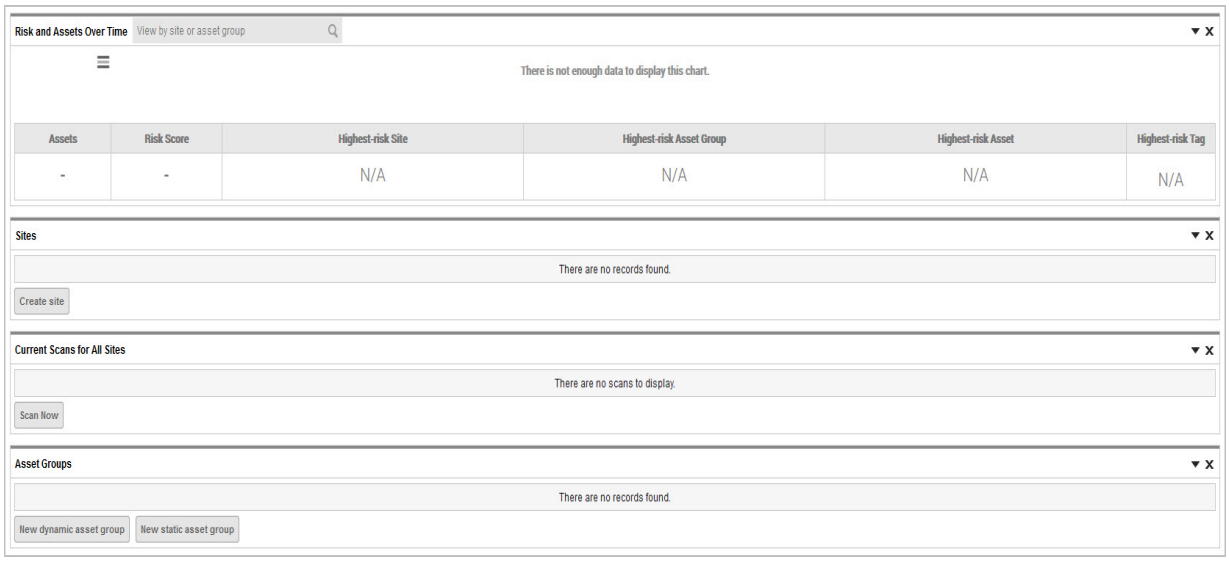
4. Click **Activate** to complete this step.
5. Click the **Home** link to view the Security Console *Home* page.
6. Click the **Help** link on any page of the Web interface for information on how to use the application.

The first time you log on, you will see the *News* page, which lists all updates and improvements in the installed system, including new vulnerability checks. If you do not wish to see this page every time you log on after an update, clear the check box for automatically displaying this page after every login. You can view the *News* page by clicking the **News** link that appears near the top right corner of every page of the console interface.

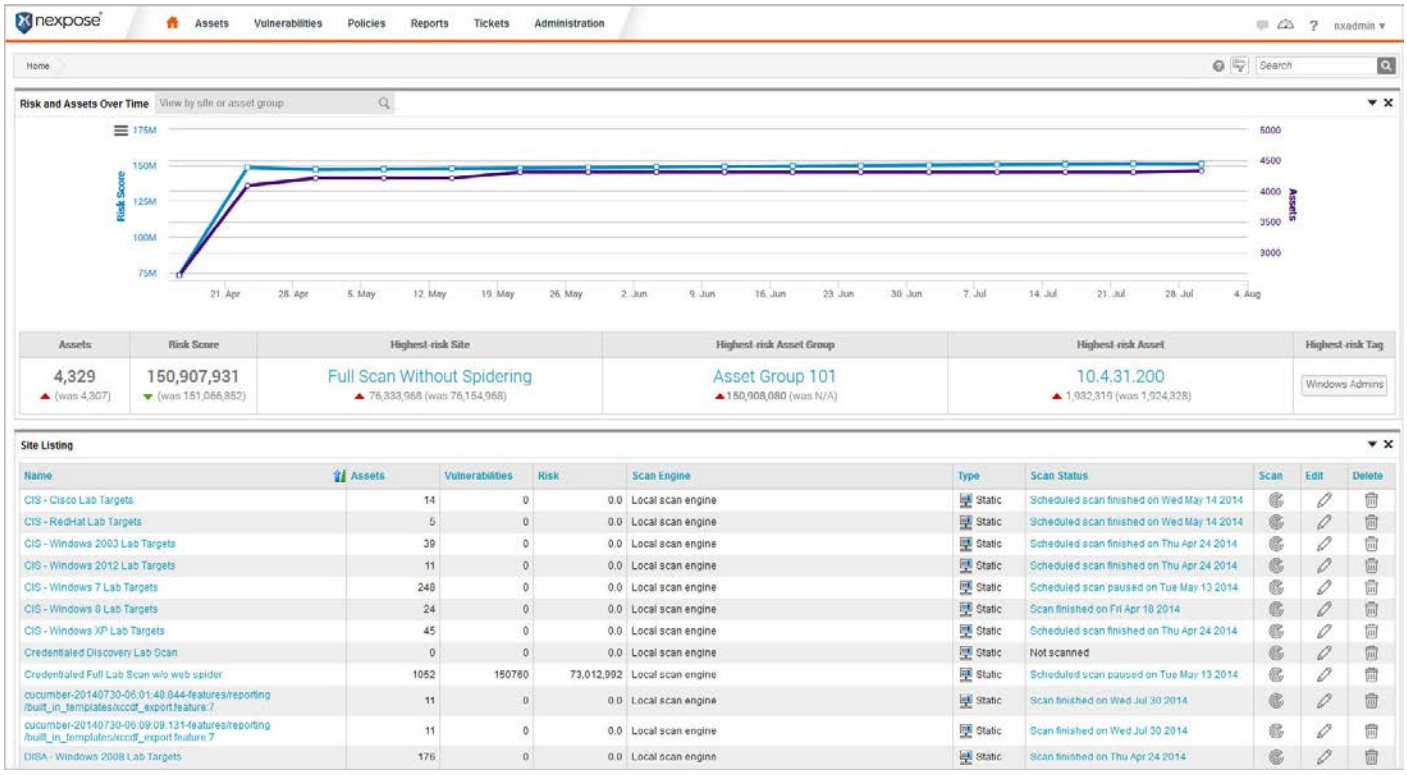
Navigating the Security Console Web interface

The Security Console includes a Web-based user interface for configuring and operating the application. Familiarizing yourself with the interface will help you to find and use its features quickly.

When you log on to the to the *Home* page for the first time, you see place holders for information, but no information in them. After installation, the only information in the database is the account of the default Global Administrator and the product license.



The Home page as it appears in a new installation



The Home page as it appears with scan data

The *Home* page shows sites, asset groups, tickets, and statistics about your network that are based on scan data. If you are a Global Administrator, you can view and edit site and asset group information, and run scans for your entire network on this page.

The *Home* page also displays a chart that shows trends of risk score over time. As you add assets to your environment your level of risk can increase because the more assets you have, the more potential there is for vulnerabilities.

Each point of data on the chart represents a week. The blue line and measurements on the left show how much your risk score has increased or decreased over time. The purple line displays the number of assets.

Note: This interactive chart shows a default of a year's worth of data when available; if you have been using the application for a shorter historical period the chart will adjust to show only the months applicable.

The following are some additional ways to interact with charts:

- In the search filter at the top left of the chart, you can enter a name of a site or asset group to narrow the results that appear in the chart pane to only show data for that specific site or group.
- Click and drag to select a smaller, specific timeframe and view specific details. Select the **Reset/Zoom** button to reset the view to the previous settings.
- Hover your mouse over a point of data to show the date, the risk score, and the number of assets for the data point.
- Select the sidebar menu icon on the top left of the chart window to export and print a chart image.



Print or export the chart from the sidebar menu

On the *Site Listing* pane, you can click controls to view and edit site information, run scans, and start to create a new site, depending on your role and permissions.

Information for any currently running scan appears in the pane labeled *Current Scan Listings for All Sites*.

On the *Ticket Listing* pane, you can click controls to view information about tickets and assets for which those tickets are assigned.

On the *Asset Group Listing* pane, you can click controls to view and edit information about asset groups, and start to create a new asset group.

A row of tabs appears at the top of the *Home* page, as well as every page of the Security Console. Use these tabs to navigate to the main pages for each area.



Home tab bar

The *Assets* page links to pages for viewing assets organized by different groupings, such as the sites they belong to or the operating systems running on them.

The *Vulnerabilities* page lists all discovered vulnerabilities.

The *Policies* page lists policy compliance results for all assets that have been tested for compliance.

The *Reports* page lists all generated reports and provides controls for editing and creating report templates.

The *Tickets* page lists remediation tickets and their status.

The *Administration* page is the starting point for all management activities, such as creating and editing user accounts, asset groups, and scan and report templates. Only Global Administrators see this tab.

Selecting your language

Some features of the application are supported in multiple languages. You have the option to set your user preferences to view Help in the language of your choosing. You can also run Reports in multiple languages, giving you the ability to share your security data across multi-lingual teams.

To select your language, click your user name in the upper-right corner and select **User Preferences**. This will take you to the *User Configuration* panel. Here you can select your language for Help and Reports from the corresponding drop down lists.

When selecting a language for Help, be sure to clear your cache and refresh your browser after setting the language to view Help in your selection.

Setting your report language from the *User Configuration* panel will determine the default language of any new reports generated through the *Create Report Configuration* panel. Report configurations that you have created prior to changing the language in the user preferences will remain in their original language. When creating a new report, you can also change the selected language by going to the **Advanced Settings** section of the *Create a report* page. See the topic *Creating a basic report* on page 356.

Throughout the Web interface, you can use various controls for navigation and administration.

Control	Description	Control	Description
	Minimize any pane so that only its title bar appears.		Click to add items to your dashboard.
	Expand a minimized pane.		Copy a built-in report template to create a customized version.
x	Close a pane.		Edit properties for a site, report, or a user account.
	Click to display a list of closed panes and open any of the listed panes.		View a preview of a report template.
	Reverse the sort order of listed items in a given column. You can also click column headings to produce the same result.		Delete a site, report, or user account.
	Export asset data to a comma-separated value (CSV) file.		Exclude a vulnerability from a report.
	Start a manual scan.		View Help. View the Support page to search FAQ pages and contact Technical Support. View the *News* page which lists all updates.
	Pause a scan.		Click Home to return to the main dashboard.

Control	Description	Control	Description
	Resume a scan.	**User: <user name>** link	This link is the logged-on user name. Click it to open the User Configuration panel where you can edit account information such as the password and view site and asset group access. Only Global Administrators can change roles and permissions.
	Stop a scan.	**Log Out** link	Log out of the Security Console interface. The *Logon* box appears. For security reasons, the Security Console automatically logs out a user who has been inactive for 10 minutes.
	Initiate a filtered search for assets to create a dynamic asset group.		

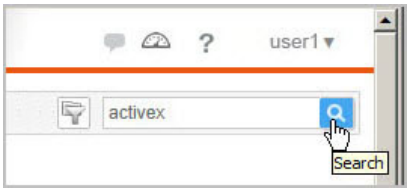
Using the search feature

With the powerful full-text search feature, you can search the database using a variety of criteria, such as the following:

- full or partial IP addresses
- asset names
- site names
- asset group names
- vulnerability titles
- vulnerability CVE IDs
- internal vulnerability IDs
- user-added tags
- criticality tags
- Common Configuration Enumerator (CCE) IDs
- operating system names

Enter your search criteria in the **Search** box on any a page of the Security Console interface, and click the magnifying glass icon. For example, if you want to search for discovered instances of the vulnerabilities that affect assets running ActiveX, enter *ActiveX* or *activex* in the **Search** text box. The search is not case-sensitive.

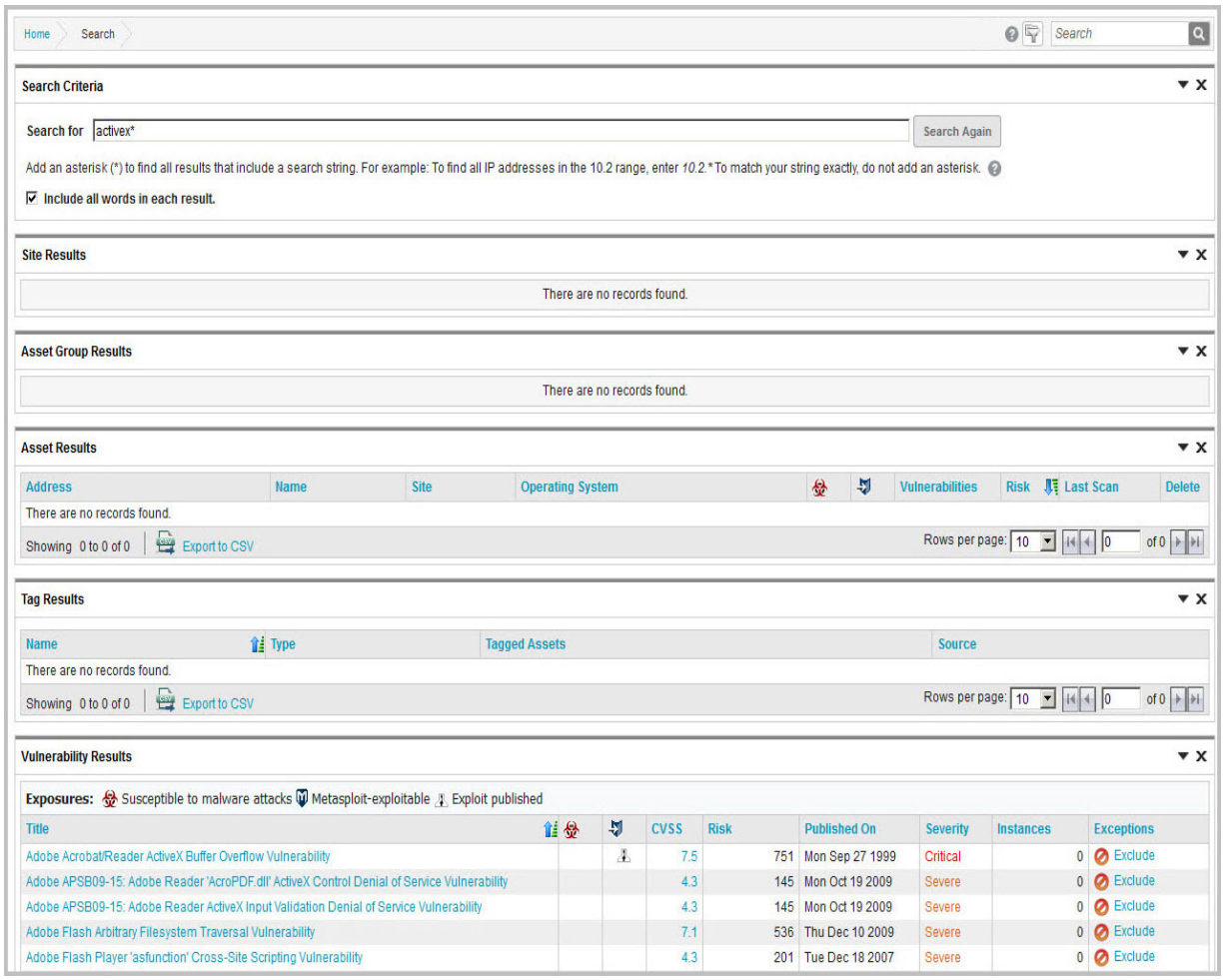
For example, if you want to search for discovered instances of the vulnerabilities that affect assets running ActiveX, enter ActiveX or activex in the **Search** text box. The search is not case-sensitive.



Starting a search

The application displays search results on the *Search* page, which includes panes for different groupings of results. With the current example,

ActiveX, results appear in the *Vulnerability Results* table. At the bottom of each category pane, you can view the total number of results and change settings for how results are displayed.



Search results

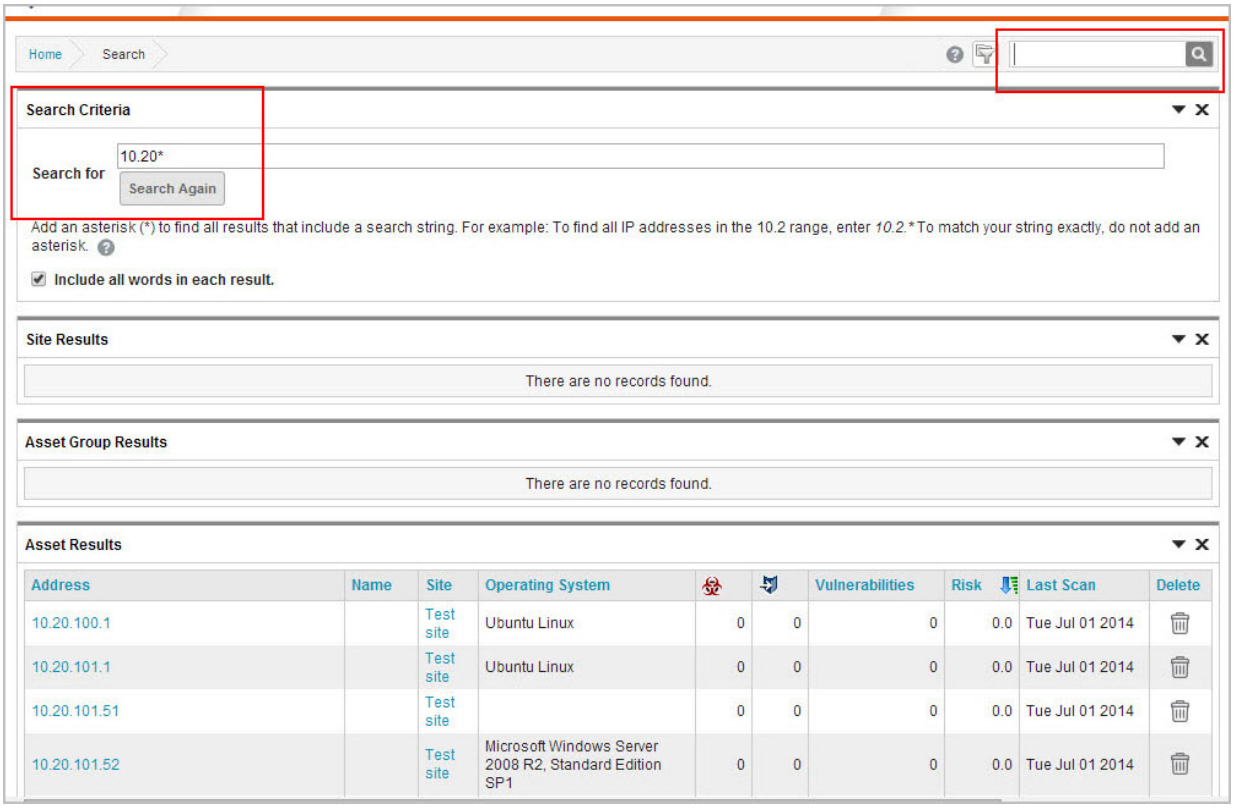
In the *Search Criteria* pane, you can refine and repeat the search. You can change the search phrase and choose whether to allow partial word matches and to specify that all words in the phrase appear in each result. After refining the criteria, click the **Search Again** button.

Using asterisks and avoiding *stop words*

When you run initial searches with partial strings in the *Search* box that appears in the upper-right corner of most pages in the Web interface, results include all terms that even partially match those strings. It is not necessary to use an asterisk (*) on the initial search. For example, you can enter *Win* to return results that include the word Windows, such as any Windows operating system. Or if you want to find all IP addresses in the 10.20 range, you can enter 10.20 in the Search text box.



If you want to modify the search after viewing the results, an asterisk is appended to the string in the *Search Criteria* pane that appears with the results. If you leave the asterisk in, the modified search will still return partial matches. You can remove the asterisk if you want the next set of results to match the string exactly.



If you precede a string with an asterisk, the search ignores the asterisk and returns results that match the string itself.

Certain words and individual characters, collectively known as *stop words* return no results, even if you enter them with asterisks. For better performance, search mechanisms do not recognize stop words. Some stop words are single letters, such as *a*, *i, s*, and *t*. If you want to include one of these letters in a search string, add one or more letters to the string. Following is a list of stop words:

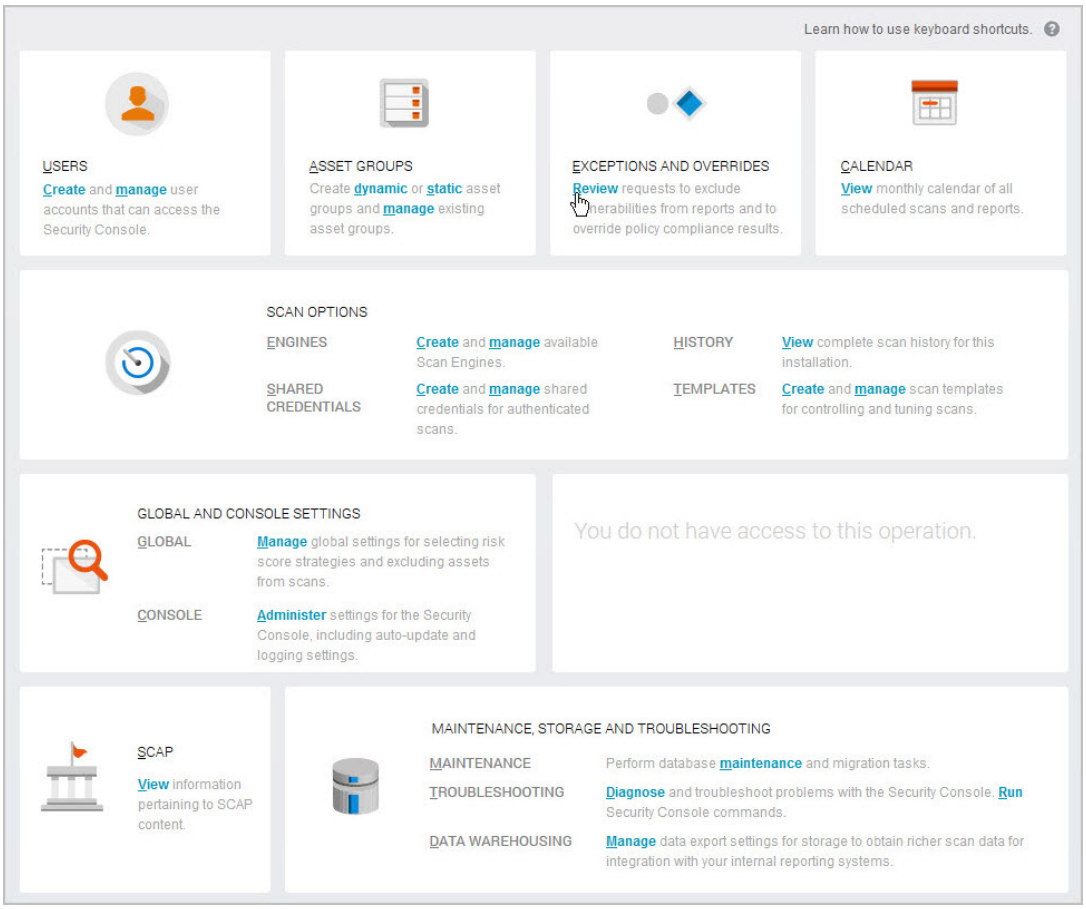
a	about	above	after	again	against	all	am	an	and
any	are	as	at	be	because	been	being	below	before
between	both	but	by	can	did	do	doing	don	does
down	during	each	few	for	from	further	had	has	have
having	he	her	here	hers	herself	him	himself	his	how
i	if	in	into	it	is	its	itself	just	me
more	most	my	myself	no	nor	not	now	of	off
on	once	only	or	other	our	ours	ourselves	out	over
own	s	same	she	should	so	some	such	t	than
that	the	their	theirs	them	themselves	then	there	these	they
this	those	through	to	too	under	until	up	very	was
we	were	what	when	where	which	while	who	whom	why
will	with	you	your	yours	yourself	yourselves			

Accessing operations faster with the Administration page

You can access a number of key Security Console operations quickly from the *Administration* page. To go there, click the **Administration** tab. The page displays a panel of tiles that contain links to pages where you can perform any of the following operations to which you have access:

- managing user accounts
- managing asset groups
- reviewing requests for vulnerability exceptions and policy result overrides
- creating and managing Scan Engines
- managing shared scan credentials, which can be applied in multiple sites
- viewing the scan history for your installation
- managing scan templates
- managing different models, or strategies, for calculating risk scores
- managing various activities and settings controlled by the Security Console, such as license, updates, and communication with Scan Engines
- managing settings and events related to discovery of virtual assets, which allows you to create dynamic sites
- viewing information related to Security Content Automation Protocol (SCAP) content
- maintaining and migrating the database
- troubleshooting the application
- using the command console to type commands
- managing data export settings for integration with third-party reporting systems

Tiles that contain operations that you do not have access to because of your role or license display a label that indicates this restriction.



Administration page

Tip: Click the keyboard shortcut **Help** icon at the top of the page to see a list of all available key combinations.

After viewing the options, select an operation by clicking the link for that operation.

OR

Type the underlined two-letter combination for the desired operation. First type the letter of the section, then type the letter for the action. For example, to create a user, type *u* to select all options under *Users*, then *c* for the *create* option.

Using configuration panels

The Security Console provides panels for configuration and administration tasks:

- creating and editing sites
- creating and editing user accounts
- creating and editing asset groups
- creating and editing scan templates
- creating and editing reports and report templates
- configuring Security Console settings
- troubleshooting and maintenance

Note: Parameters labeled in red denote required parameters on all panel pages.

Extending Web interface sessions

Note: You can change the length of the Web interface session. See *Changing Security Console Web server default settings* in the administrator's guide.

By default, an idle Web interface session times out after 10 minutes. When an idle session expires, the Security Console displays a logon window. To continue the session, simply log on again. You will not lose any unsaved work, such as configuration changes. However, if you choose to log out, you will lose unsaved work.

If a communication issue between your browser and the Security Console Web server prevents the session from refreshing, you will see an error message. If you have unsaved work, do not leave the page, refresh the page, or close the browser. Contact your Global Administrator.

Troubleshooting your activation

Your product key is your access to all the features you need to start using the application. Before you can being using the application you must activate your license using the product key you received. Your license must be active so that you can perform operations like running scans and creating reports. If you received an error message when you tried to activate your license you can try the troubleshooting techniques identified below before contacting Technical Support.

Product keys are good for one use; if you are performing the installation for a second time or if you receive errors during product activation and these techniques have not worked for you, contact Technical Support.

Try the following techniques to troubleshoot your activation:

Did I enter the product key correctly?

- Verify that you entered the product key correctly.

Is there an issue with my browser?

- Confirm the browser you are using is supported. See *Logging on* on page 26 for a list of supported browsers.
- Clear the browser cache.

Are my proxy settings correct?

- If you are using a proxy server, verify that your proxy settings are correct because inaccurate settings can cause your license activation to fail.
    - Go to the *Administration* page and click **Manage** *settings for the Security Console* to open the Security Console Configuration panel. Select Update Proxy to display the Proxy Settings section ensure that the address, port, domain, User ID, and password are entered correctly.
    - If you are not using a proxy, ensure the **Name or address field** is specified as *updates.rapid7.com*. Changing this setting to another server address may cause your activation to fail. Contact Technical Support if you require a different server address and you receive errors during activation.

Are there issues with my network or operating system?

- By running diagnostics, you can find operating system and network issues that could be preventing license activation.
    - Go to the *Administration* page and click **Diagnose** *and troubleshoot problems with the Security Console*.
    - Select the OS Diagnostics and Network Diagnostics checkboxes.
    - Click **Perform diagnostics** to see the current status of your installation. The results column will provide valuable information such as, if DNS name resolution is successful, if firewalls are enabled, and if the Gateway ping returns a 'DEAD' response.

- Confirm that all traffic is allowed out over port 80 to updates.rapid7.com.
    - If you are using Linux, open a terminal and enter `telnet updates.rapid7.com 80`. You will see `Connected` if traffic is allowed.
    - If you are using Windows, open a browser and enter http://updates.rapid7.com. You should see a blank page.
    - White-list the IP address of the application server on your firewall so that it can send traffic outbound to http://updates.rapid7.com.
    - Make the same rule changes on your proxy server.
    - If you see an error message after adding the IP address to a white-list you will need to determine what is blocking the application.

Are there issues with firewalls in my network?

- Confirm that host-based firewall and antivirus detection are disabled on the system you are installing the application on. See *Using anti-virus software on the server* in the *administrator's guide* for more information.
- Ensure the IP address of the application server is white-listed through firewalls and content filters. This will allow you to reach the update server and pull down any necessary .jar files for activation and updates.

Have I tried everything?

- Restart the application, in some cases a browser anomaly can cause an error message that your activation failed. Restarting may be successful in those rare cases.

Discover

To know what your security priorities are, you need to discover what devices are running in your environment and how these assets are vulnerable to attack. You discover this information by running scans.

First, if you don't know what a site is, go to *What is a site?* on page 47. And learn about different *Site creation scenarios* on page 49 for use cases such as discovering all the assets in your environment, running PCI scans, and dealing with Zero-day vulnerabilities.

The *Discover* section provides guidance on operations that enable you to prepare and run scans.

Creating and editing sites on page 60: Before you can run a scan, you need to create a site. A site is a collection of assets targeted for scanning. A basic site includes assets, a scan template, a Scan Engine, and users who have access to site data and operations. This section provides steps and best practices for creating a basic static site.

Adding assets to sites on page 65: This section explains different ways to specify which assets should be scanned, and it provides best practices for planning sites.

Selecting a Scan Engine or engine pool for a site on page 75: A Scan Engine is a requirement for a site. It is the component that will do the actual scanning of your target assets. By default, a site configuration includes the local Scan Engine that is installed with the Security Console. If you want to use a distributed or hosted Scan Engine, or a for a site, this section guides you through the steps of selecting it.

Configuring distributed Scan Engines on page 78: Before you can select a distributed Scan Engine for your site, you need to configure it and pair with the Security Console, so that the two components can communicate. This section shows you how.

Working with Scan Engine pools on page 83: You can improve the speed of your scans for large numbers of assets in a single site by pooling your Scan Engines. This section shows you how to use them.

Configuring scan credentials on page 93: To increase the information that scans can collect, you can authenticate them on target assets. Authenticated scans inspect assets for a wider range of vulnerabilities, as well as policy violations and adware or spyware exposures. They also can collect information on files and applications installed on the target systems. This section provides guidance for adding credentials to your site configuration. It also links to sections on elevating permissions, working with PowerShell, and best practices.

Configuring scan authentication on target Web applications on page 133: Scanning Web applications at a granular level of detail is especially important, since publicly accessible Internet

hosts are attractive targets for attack. Authenticated scans of Web assets can flag critical vulnerabilities such as SQL injection and cross-site scripting. This section provides guidance on authenticating Web scans.

Managing dynamic discovery of assets on page 157: If your environment includes virtual machines, you may find it a challenge to keep track of these assets and their activity. A feature called vAsset discovery allows you find all the virtual assets in your environment and collect up-to-date information about their dynamically changing states. This section guides you through the steps of initiating and maintaining vAsset discovery.

Configuring a dynamic site on page 200: After you initiate vAsset discovery, you can create a dynamic site and scan these virtual assets for vulnerabilities. A dynamic site's asset membership changes depending on continuous vAsset discovery results. This section provides guidance for creating and updating dynamic sites.

Integrating NSX network virtualization with scans on page 203: Integrating Nexpose with the VMware NSX network virtualization platform gives a Scan Engine direct access to an NSX network of virtual assets. This section provides guidance on setting up the integration.

Running a manual scan on page 222: After you create a site, you're ready to run a scan. This section guides you through starting, pausing, resuming, and stopping a scan, as well as viewing the scan log and monitoring scan status.

What is a site?

A site is a collection of assets that are targeted for a scan. You must create a site in order to run a scan of your environment and find vulnerabilities.

A site consists of:

- target assets
- a scan template
- one or more Scan Engines
- other scan-related settings such as schedules or alerts

Different ways to add assets to a site

Your first choice is how you want to add assets to your site. You can do this by manually inputting individual assets and/or asset groups, or by dynamically discovering assets through a connection. The main factor to consider is the fluidity of your scan target environment.

Note: You select how assets are added to your site on the **Assets** tab of the *Site Configuration*.

Specifying individual assets or ranges is a good choice for situations where the addresses of your assets are likely to remain stable.

Specifying asset groups allows you to scan based on logical groupings that you have previously created. In the case of scanning dynamic asset groups, you can scan based on whether assets meet certain criteria. For example, you can scan all assets whose operating system is Ubuntu. To learn more about asset groups, see *Working with asset groups* on page 315.

Adding assets through connection is ideal for a highly fluid target environment, such as a deployment of virtualized assets. It is not unusual for virtual machines to undergo continual changes, such as having different operating systems installed, being supported by different resource pools, or being turned on and off. Because asset membership in such a site is based on continual discovery of virtual assets, the asset list changes as the target environment changes, as reflected in the results of each scan.

You can change asset membership in a site that populates assets through a connection by changing the discovery connection or the criteria filters that determine which assets are discovered. See *Managing dynamic discovery of assets* on page 157.

How are sites different from asset groups?

Asset groups provide different ways for members of your organization to grant access to, view, scan, and report on asset information. You can create asset groups that contain assets across multiple sites. See *Working with asset groups* on page 315.

Site creation scenarios

This section discusses "recipes" for sites to suit common needs. By selecting an appropriate template, assets, and configuration options, you can customize your site to suit specific goals.

- *Default settings* on page 49
- *Find out what you have: Discovery scan* on page 50
- *Get an outside view of your environment* on page 52
- *Zero-day vulnerabilities* on page 54
- *Assets in multiple locations* on page 56
- *Large numbers of assets* on page 56
- *Amazon Web Services* on page 56
- *VMWare* on page 56
- *Internal PCI compliance scans* on page 57
- *Policy benchmarks* on page 59

Default settings

The default scan template is Full Audit without Web Spider.

This scan template gives you thorough vulnerability checks on the majority of non-Web assets. It runs faster than the scan template with the Web spider.

To check thoroughly for vulnerabilities, you should specify credentials. See *Configuring scan credentials* on page 93 for more information.

As you establish your vulnerability scanning practice, you can create additional sites with various scan templates and change your Scan Engine from the default as needed for your network configuration.

Find out what you have: Discovery scan

Summary: The first step in checking for vulnerabilities is to make sure you are checking all the assets in your organization. You can find basic information about the assets in your organization by conducting a discovery scan. The application includes a built-in scan template for a discovery scan.

If there is an asset you do not know about that can be exploited, attackers can use that to bypass the Virtual Private Network (VPN) and corporate firewall, and launch attacks from within the local network. If you are new to your role, you might not already be aware of every asset you are responsible for securing. In any case, new assets are frequently added. You can conduct discovery scans to find and learn more about those assets, in preparation for developing an ongoing scanning program.

Your discovery scan may vary depending on your organization's network configuration.We recommend conducting a discovery scan on as wide a range of IP addresses as possible, in case your organization has items outside the typical range. Therefore, for the initial discovery scan, we recommend initially checking the entire private IPv4 address space (10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0) as well as all of the public IP addresses owned or controlled by the organization. Doing so will help you find the largest possible number of hosts. We recommend this certainly for organizations who actually make use of all the private address space, but also for organizations with smaller networks, in order to make sure they find everything they can.

Note: Scanning so many assets could take some time. To estimate how long the scans will take, see the *Planning for capacity requirements* section of the administrator's guide. In addition, a discovery scan can set off alerts through your system administration or antivirus programs; you may want to advise users before scanning.

To conduct the initial discovery scan in Nexpose:

1. Create a new static site [see Configuring a basic static site], including the following settings:
    - When specifying the included assets, specify a range in Classless Inter-Domain Routing (CIDR) notation. See http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing. This notation allows you to specify a large group of machines in a concise syntax. As mentioned above, a best practice at this point is to scan all IP addresses controlled by the organization, as well as each of the private IP address ranges.
    - Select the **Discovery Scan** scan template.
    - Do not specify credentials. They are not needed for determining the presence of the machine on the network.

2. Run a scan on this site.

- Examine the results of the scan in comparison to what you know about your network. Look for and address any anomalies. For example:
  - **Ports incorrectly showing as active:** If the discovery scan shows every single port as active, it is likely that this result is not showing the actual network configuration, but is being affected by something else such as a piece of security equipment (for example, intrusion detection software, intrusion protection software, or a load balancer). Determine what is causing the unexpected result and make changes so that you can get accurate scan information. For example, if a firewall is causing the inaccurate results, whitelist Nexpose on the firewall.
  - **Ports incorrectly showing as inactive:** You may find areas of the network where you were not able to scan. For instance, there may be an address you know about that was not found on the discovery scan. Check whether the omission was due to a firewall or logical routing issue. If so, configure an additional Scan Engine on the other side of the barrier and scan those assets.

Get an outside view of your environment

Summary: In addition to conducting thorough scans of your network, we recommend to use a Scan Engine outside your network to check what can be found. Once you have a Scan Engine ready, you can add it in the *Site Configuration*.

If you have external IP addresses, you can check on what someone could access from outside. You can set up a Scan Engine outside your network perimeter and see what it can find. If you would like to get an "external" view of your firewall, perform a scan from an engine that is external to the organization and treated the same as other external machines. You may want to consider using a Rapid7 hosted engine.

We recommend the following configurations:

- Do not use credentials for these external scans.
- Do not whitelist the source IP address.
- You may need to exempt the engine from certain active/adaptive intrusion prevention technologies (e.g., Web Application Firewall, Unknown Unicast and Muticast Flood Control, intrusion prevention systems, Dynamic Firewall Blacklisting).
- Use the Full Audit with Web Spider scan template or a similar custom template.
- Scan the entirety of your organization's assigned public address space, not just the systems you believe to be alive or accessible.
- Scan at least monthly, or as frequently as feasible given change control and duration of scans.
- Always combine external scanning with internal authenticated scanning as described above, because firewall rules screen access to certain vulnerabilities, services, and hosts.

We recommend the following prioritization for remediation:

- One of the most dangerous types of vulnerabilities is one that could let an unauthenticated external user log on, such as an exposed Telnet port. Make it an urgent priority to remediate such vulnerabilities.
- Otherwise, begin addressing the results by reducing the attack surface:
    - Take down or block access to hosts that do not need to be public.
    - Use firewall rules to restrict access to as many services and hosts as possible.
    - Address the remaining external-facing vulnerabilities based on CVSSv2 score and prevalence.

Zero-day vulnerabilities

In the case of newly announced, high risk vulnerabilities, you may want to scan for just that specific vulnerability, in order to find out as quickly as possible which of your assets are affected.

You can create a custom scan template that checks just for specific vulnerabilities, and scan your sites with this special template. You can use the Common Vulnerabilities and Exposures Identifier (CVE-ID) to focus only on checks for that vulnerability.

Note: Check the Rapid7 Community for additional guidance related to recently-announced major vulnerabilities.

To scan for specific vulnerabilities:

1. Typically, the best practice is to create a new scan template by copying an existing one. The best one to copy will vary depending on the nature of the vulnerability, but *Full Audit with Web Spider* or *Full Audit without Web Spider* are usually good starting points. For more information on scan templates, see *Scan templates* on page 684.
2. Ensure the **Vulnerabilities** option is selected, and that the **Web Spidering** option is selected if relevant. Clear the **Policies** option to focus the template on the checks specific to this vulnerability.
3. Edit the scan template name and description so you will be able to recognize later that the template is customized for this purpose.
4. Go to the *Vulnerability Checks* page. First, you will disable all checks, check categories, and check types so that you can focus on scanning exclusively for items related to this issue.
5. Expand the *By Category* section and click **Remove categories**.
6. Select the check box for the top row (*Vulnerability Category*), which will auto-select the check boxes for all categories. Then click Save. Note that 0 categories are now enabled.
7. Expand the *By Individual Check* section and click **Add checks**.
8. Enter or paste the relevant CVE-ID in the *Search Criteria* box and click **Search**. Select the check box for the top row (Vulnerability Check), which will auto-select the check boxes for all types. Then click Save.
9. Repeat step 7 for any additional CVE-IDs associated with the issue.
10. Save the scan template.
11. Create or edit a site to include:
    - the new custom scan template
    - credentials for the authenticated vulnerability checks

12. Start scanning.

Assets in multiple locations

If you have assets in multiple locations, there are several factors to take into consideration:

- You can apply tags to indicate the locations of the assets. See *Applying RealContext with tags* on page 254. You can then create reports based in these tags so you can assess the risk of your assets by location. See *Selecting assets to report on* on page 363.
- It is a good practice to create sites and associate them with scan engines in a way that makes the most of your network configuration. For example, if you have assets in Houston and Singapore, you probably will be better off placing Scan Engines in both locations and creating a site for each, rather than trying to scan all the assets with a scan engine in just one of the locations.

Large numbers of assets

To scan large numbers of assets, you may want to take advantage of Scan Engine pooling. A Scan Engine pool can help with load balancing and serve as backup if one Scan Engine fails. To learn more about configuring Scan Engine pools, see *Working with Scan Engine pools* on page 83.

Amazon Web Services

To scan Amazon Web Services (AWS) virtual assets, you need to perform some preparation in your AWS environment and create a discovery connection specific to this type of assets. To learn more, see *Preparing for Dynamic Discovery in an AWS environment* on page 165.

VMWare

To scan VMWare virtual assets, you will need to perform some preparation steps in the target VMWare environment, and then create a discovery connection specific to this type

of assets. To learn more, see *Preparing the target VMware environment for Dynamic Discovery* on page 167.

Internal PCI compliance scans

If your systems process, store, or transmit credit card holder data, you may be using Nexpose to comply with the Payment Card Industry (PCI) Security Standards Council Data Security Standards (DSS). The *PCI internal audit* scan template is designed to help you conduct your internal assessments as required in the DSS.

To learn more about PCI DSS 3.0, visit our resource page.

The following is an outline of a suggested process to use with Nexpose to help with your internal PCI scans. (For more information on how to use any of the features in the application, see the Help or User's Guide.)

1. As described in PCI DSS 3.0 section 6.1, you need to create a process to identify security vulnerabilities. To do so create one or more sites in Nexpose using the following configurations:
    a. Enter your organization information as required for PCI-specific reports in the *Organization* section of the *Info & Security* tab of the *Site Configuration*.
    b. Include the assets you need to scan for PCI compliance. (Generally these hosts will comprise your Cardholder Data environment or "CDE").
    c. Use the *PCI internal audit* scan template.
    d. Specify credentials for the scan. (These credentials should have privileges to read the registry, file, and package management aspects of target systems).

2. As indicated in the PCI Data Security Standard requirements 11.2.1 and 11.2.3, you need to create and examine reports to verify that you have scanned for and remediated vulnerabilities. You should also keep copies of these reports to prove your compliance with the PCI DSS.
    a. Create a new report as indicated in *Creating a basic report* on page 356. You will most likely want to use the *PCI Executive Summary* and *PCI Vulnerability Details* reports. Follow this process for each of those templates. Specify the following settings:
        i. For the **Scope** of the report, specify the assets you are scanning for PCI.
        ii. In the advanced settings, under **Distribution**, specify the e-mail sender address and the recipients of the report.

3. Mitigate the vulnerabilities. The description of a vulnerability contains remediation steps.

4. Re-scan to verify that your mitigations have successfully resolved the findings
    a. If compensating controls are used, it may be necessary to use exception handling to eliminate the associated findings. (It may not be possible for automated tools to detect your compensating control even if it is effective in mitigating associated risk.)

5. Continue to scan and mitigate. You will need to scan internally quarterly until you have remediated all high-risk vulnerabilities, as defined in sections 6.1 and 11.2.1 of the PCI DSS. You will also need to scan after major changes, as defined in section 11.2.3. The acceptable timeframes for applying remediations are outlined in section 6.2.

Policy benchmarks

The application includes built-in scan templates that can be used for policy benchmarking. These include CIS, DISA, and USGCB. Each of these templates contains a bundle of policies to be used for different platforms; only the ones that apply are evaluated. Of the three, CIS contains support for the widest variety of platforms. For more information on these templates, see *Scan templates* on page 684.

All policy scan templates require a username and password pair used to gain access to assets such as desktop and server machines. Typically this account will have the privileges of an administrator or root user. For more on credentials, see *Configuring scan credentials* on page 93.

The CIS scan template includes policy checks specific to databases, and requires a username and password for database access.

Creating and editing sites

In this section you will learn how to create and configure sites. If you are a new user, you will learn how to create your first basic site. Experienced users can find information on more advanced practices and configurations.

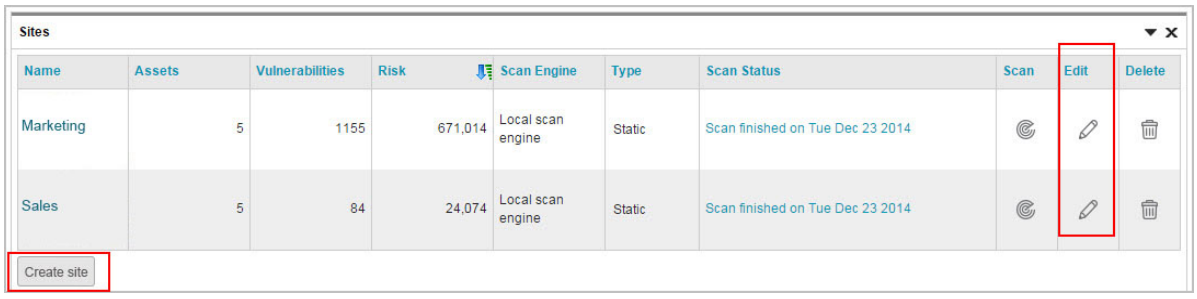
Topics include:

- *Getting started: Info & Security* on page 61
- *Adding assets to sites* on page 65
- *Configuring scan credentials* on page 93
- *Configuring scan authentication on target Web applications* on page 133
- *Selecting a scan template* on page 87
- *Selecting a Scan Engine or engine pool for a site* on page 75
- *Setting up scan alerts* on page 143
- *Scheduling scans* on page 145
- *Site creation scenarios* on page 49
- *Managing dynamic discovery of assets* on page 157

Note: Not all of the procedures described are required for every kind of site. The basic requirements to save a site are a name and at least one asset.

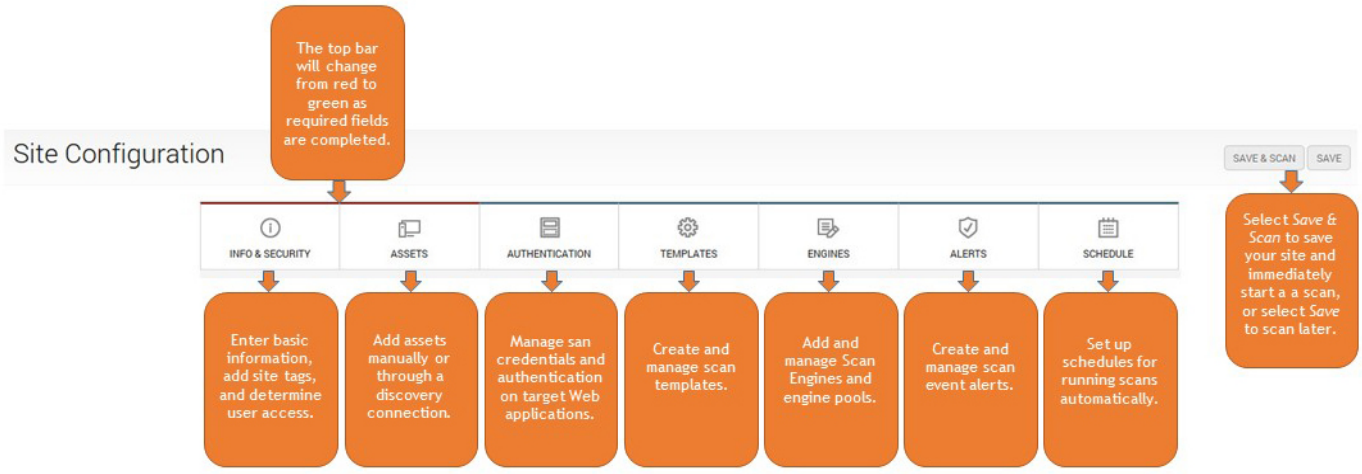
If you want to edit an existing site, click that site's **Edit** icon in the *Sites* table on the *Home* page.

If you want to create a new site, click the **Create site** button on the *Home* page.

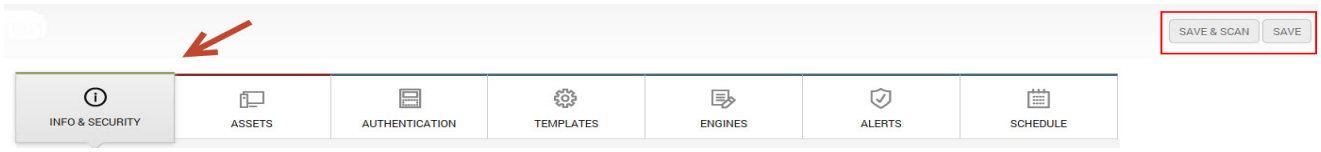


Starting to create or edit a site

Click the tabs in the *Site Configuration* to configure various aspects of your site and scans:



Getting started: Info & Security



Save & Scan

The **Save & Scan** and **Save** buttons are enabled after you enter the minimum required site information, which includes the site name and at least one asset.

The top of each required tab-*Info & Security* and *Assets*-changes from to red to green after you enter as the minimum required information, which includes the name of the site and at least one asset to scan.

1. On the *Site Configuration - Info & Security* tab, type a name for your site.

   Tip: You may want to name your site based on how the assets within that site are grouped. For example, you could name them based on their locations, operating systems, or the types of assets, such as those that need to be audited for compliance.

2. Type a brief description of the site.

3. Select a level of importance from the drop-down list:

- The *Very Low* setting reduces the risk index to 1/3 of its initial value.
- The *Low* setting reduces the risk index to 2/3 of its initial value.
- *High* and *Very High* settings increase the risk index to twice and 3 times its initial value respectively.
- A *Normal* setting does not change the risk index.

The importance level corresponds to a risk factor used to calculate a risk index for each site. See *Adjusting risk with criticality* on page 665.

5. Add business context tags to the site. Any tag you add to a site will apply to all of the member assets. For more information and instructions, see *Applying RealContext with tags*.
6. Click **Organization** to enter your company information. These fields are used in PCI reports.

For more information on managing user access, see *Giving users access to a site* on page 63.

Giving users access to a site

When editing a site, you can control which users have access to it. Allowing users to configure and run scans on only those assets for which they are responsible is a security best practice, and it ensures that different teams in your organization are able to manage targeted segments of your network.

For example, your organization has an administrative office in Chicago, a sales office in Hong Kong, and a research center in Berlin. Each of these locations has its own site with a dedicated IT or security team in charge of administering its assets. By giving one team access to the Berlin site and not to the other two sites, you allow that team to monitor and patch the research center assets without being able to see sensitive information in the administrative or sales offices.

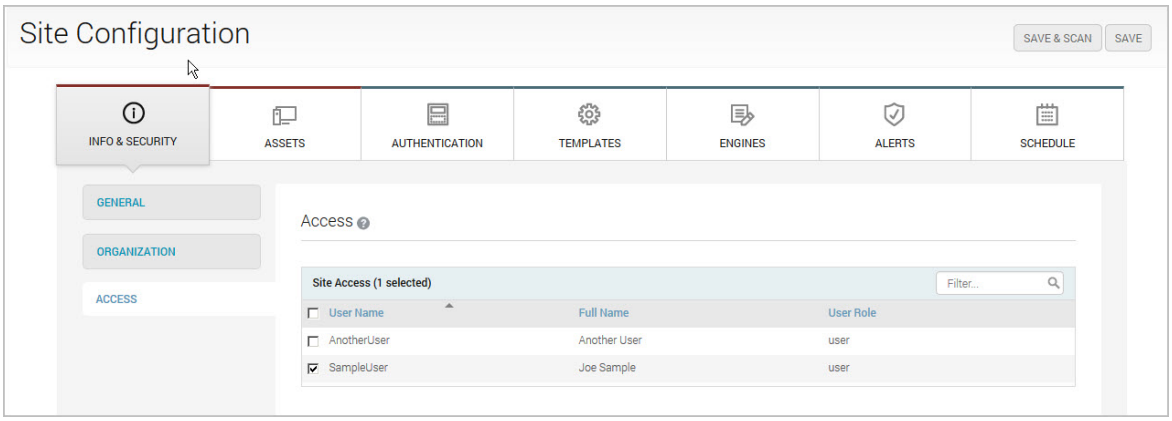
When Global Administrator creates a user account, he or she can grant the user access to all sites, or restrict access by adding the user to access lists for specific sites. See the topic *Configure general user account attributes* in the administrator's guide

After users are added to a site's access list, you can control whether they actually can view the site as you are editing that site:

1. On the *Home* page, click the **Edit** icon for the site that you want to add users to.
2. Click the **Info & Security** tab.
3. Click **Access**.
4. The *Site Access* table displays every user in the site's access list. Select the check box for every user whom you want to give access to the site.
   To give access to all displayed users, select the check box in the top row.

Note: Global Administrators and users with access to all sites do not appear in the table. They automatically have access to any site.

5. Configure other site settings as desired.
6. When you have finished configuring the site, click **Save**.



Adding users to a site

Adding assets to sites

An asset is a single device on a network that the application discovers during a scan. In order to create a site you must assign assets to it.

- If you want to add or remove assets to an existing site, click that site's **Edit** icon in the *Sites* table on the *Home* page.
- If you want to add assets while creating a new site, click the **Create site** button on the *Home* page.

Note: If you created the site through the integration with VMware NSX, you cannot edit assets, which are dynamically added as part of the integration process. See *Integrating NSX network virtualization with scans* on page 203.

Click the **Assets** tab in the *Site Configuration*.

You can either manually input your assets or asset groups, or specify a connection that discovers assets.

Note: Switching between **Name/Address** and **Connections** methods will delete any unsaved assets that have been included for scanning. Also, refreshing your browser will remove unsaved assets.

Note: After you save a site, you cannot change the method for specifying assets. For example, if you specify assets with a discovery connection and then save the site, you can not manually add IP addresses or host names afterward.

Specifying assets by Names/Addresses

Use this method to create a site that scans a manually specified collection of assets or asset groups. Such sites work best for scanning environments that have non-virtual assets and do not often change. You can specify individual assets, ranges, asset groups, or a mixture.

Adding individual assets or ranges

Use this method to specify individual assets or ranges of assets. You can use only this method, or also add asset groups to the same site.

To add assets:

1. Click the **Names/Addresses** button.
2. Enter host names, IP addresses, or ranges in the *Assets* text box in the *Include* section. To expand the text box, hover over the right corner and select the pencil icon. This allows you to edit or remove multiple assets at a time.

   Use any of the following notations Each target can be separated by either typing a comma or **Enter** after each asset or range:

- 10.0.0.1
- 10.0.0.1 - 10.0.0.255
- 10.0.0.0/24
- 2001:db8::1
- 2001:db8::0 - 2001:db8::ffff
- 2001:db8::/112
- 2001:db8:85a3:0:0:8a2e:370:7330/124
- www.example.com

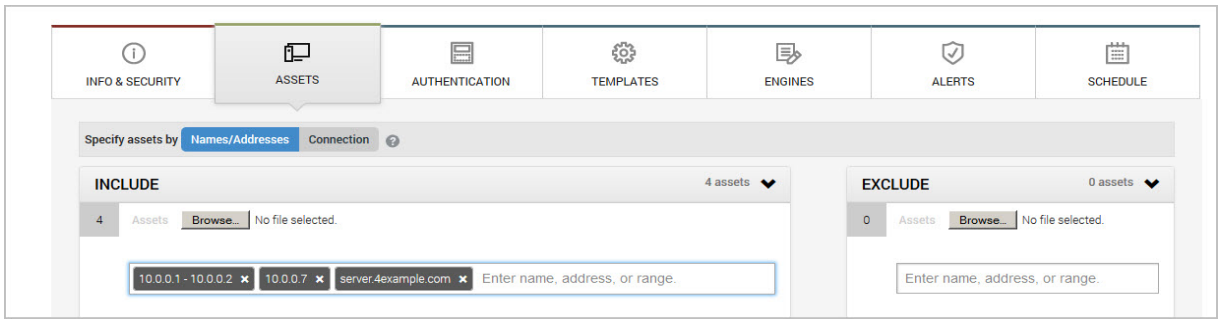
  IPv6 addresses can be fully compressed, partially uncompressed, or uncompressed. The following are equivalent:

- 2001:db8::1
- 2001:db8:0:0:0:0:0:1
- 2001:0db8:0000:0000:0000:0000:0000:0001

  If you use CIDR notation for IPv4 addresses (x.x.x.x/24) the Network Identifier (.0) and Network Broadcast Address (.255) will be ignored, and the entire network is scanned.

- 10.0.0.0/24 will become 10.0.0.1 - 10.0.0.254
- 10.0.0.0/16 will become 10.0.0.1 - 10.0.255.254

You also can import a comma- or new-line-delimited ASCII-text file that lists IP address and host names of assets you want to scan by clicking **Choose File** or **Browse**, depending or your browser.



Specifying assets by names or IP addresses

If you don't want to scan certain assets, enter their names or addresses in the *Exclude* pane. You may, for example, want to avoid scanning a specific asset within an IP address range either because it is unnecessary to scan, as with a printer, or it may require a different template or scan window than other assets in the range. The same format notations apply.

3. Configure any other site settings as desired.
4. Click **Save** or **Save & Scan** in the *Site Configuration*, depending on your preference.

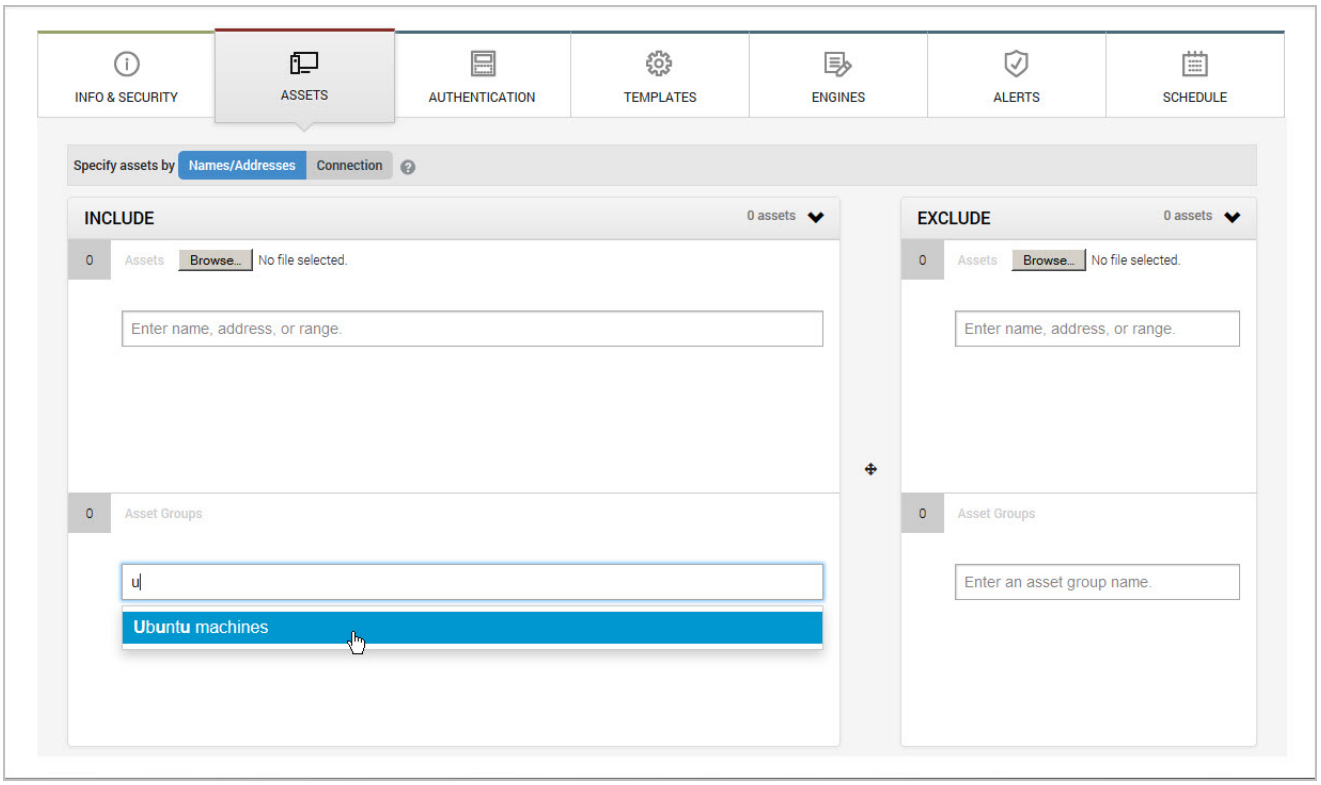
Tip: For a list of your assets that you can copy to your clipboard, click next to the **Browse** button.

Adding asset groups

Use this method to scan one or more asset groups that you have previously created based on logical groupings. You can also combine the asset groups with individually specified assets or a range, as described above. You can either scan all the assets with the same Scan Engine or pool, or scan them each with the Scan Engine that was most recently used to scan the asset. To learn more, see *Determining how to scan each asset when scanning asset groups* on page 76.

To add asset groups:

1. Click the **Names/Addresses** button.
2. In the *Asset Groups* text box in the *Include* section, begin typing the name of the asset group. As you type, matching suggestions will populate automatically. Select the asset group.



Adding an asset group to a site

If you don't want to scan certain assets, enter their names or addresses in the *Exclude* pane. You may, for example, want to avoid scanning a specific asset within an IP address range either because it is unnecessary to scan, as with a printer, or it may require a different template or scan window than other assets in the range. The same format notations apply.

3. Configure any other site settings as desired.

4. Click **Save** or **Save & Scan** in the *Site Configuration*, depending on your preference.

Adding assets by connection

Use this method to create a site in which the Security Console discovers assets via a connection with a server that manages those assets. Asset membership in a site created this way is subject to change under any of the following conditions:

- the discovery connection changes
- filter criteria for asset discovery change
- assets are added to or removed from the environment managed by the connection server

Such sites are ideal for scanning Amazon Web Services (AWS) and virtual assets managed by VMware vCenter or ESX/ESXi. Asset membership in a site is subject to change if the discovery connection changes or if filter criteria for asset discovery change.

For information on different types of discovery connections and best practices see *Managing dynamic discovery of assets* on page 157.

Best practices for adding assets to a site

Consider several things when selecting assets for a site. Asset selection can have an impact on the quality of scans and reports.

Choosing a grouping strategy for creating a site with manually selected assets

There are many ways to divide network assets into sites. The most obvious grouping principle is physical location. A company with assets in Philadelphia, Honolulu, Osaka, and Madrid could have four sites, one for each of these cities. Grouping assets in this manner makes sense, especially if each physical location has its own dedicated Scan Engine. Remember, each site is assigned to a specific Scan Engine.

With that in mind, you may find it practical simply to base site creation on Scan Engine placement. Scan engines are most effective when they are deployed in areas of separation and connection within your network. So, for example, you could create sites based on subnetworks.

Other useful grouping principles include common asset configurations or functions. You may want have separate sites for all of your workstations and your database servers. Or you may wish to group all your Windows 2008 Servers in one site and all your Debian machines in another. Similar assets are likely to have similar vulnerabilities, or they are likely to present identical logon challenges.

If you are performing scans to test assets for compliance with a particular standard or policy, such as Payment Card Industry (PCI) or Federal Desktop Core Configuration (FDCC), you may find it helpful to create a site of assets to be audited for compliance. This method focuses scanning resources on compliance efforts. It also makes it easier to track scan results for these assets and include them in reports and asset groups.

Being flexible with site membership

When selecting assets for sites, flexibility can be advantageous. You can include an asset in more than one site. For example, you may wish to run a monthly scan of all your Windows Vista workstations with the Microsoft hotfix scan template to verify that these assets have the proper Microsoft patches installed. But if your organization is a medical office, some of the assets in your “Windows Vista” site might also be part of your “Patient support” site, which you may have to scan annually with the HIPAA compliance template.

You can also define an asset group within a site, in order to scan based on a specific logical grouping.

Grouping options for Example, Inc.

Your grouping scheme can be fairly broad or more granular.

The following table shows a serviceable high-level site grouping for Example, Inc. The scheme provides a very basic guide for scanning and makes use of the entire network infrastructure.

Site name	Address space	Number of assets	Component
New York	10.1.0.0/22 10.1.10.0/23 10.1.20.0/24	360	Security Console
New York DMZ	172.16.0.0/22	30	Scan Engine #1
Madrid	10.2.0.0/22 10.2.10.0/23 10.2.20.0/24	233	Scan Engine #1
Madrid DMZ	172.16.10.0/24	15	Scan Engine #1

A potential problem with this grouping is that managing scan data in large chunks is time consuming and difficult. A better configuration groups the elements into smaller scan sites for more refined reporting and asset ownership.

In the following configuration, Example, Inc., introduces asset function as a grouping principle. The New York site from the preceding configuration is subdivided into Sales, IT, Administration, Printers, and DMZ. Madrid is subdivided by these criteria as well. Adding more sites reduces scan time and promotes more focused reporting.

Site name	Address space	Number of assets	Component
New York Sales	10.1.0.0/22	254	Security Console
New York IT	10.1.10.0/24	25	Security Console
New York Administration	10.1.10.1/24	25	Security Console
New York Printers	10.1.20.0/24	56	Security Console
New York DMZ	172.16.0.0/22	30	Scan Engine 1
Madrid Sales	10.2.0.0/22	65	Scan Engine 2
Madrid Development	10.2.10.0/23	130	Scan Engine 2
Madrid Printers	10.2.20.0/24	35	Scan Engine2
Madrid DMZ	172.16.10.0/24	15	Scan Engine 3

An optimal configuration, seen in the following table, incorporates the principal of physical separation. Scan times will be even shorter, and reporting will be even more focused.

Site name	Address space	Number of assets	Component
New York Sales 1st floor	10.1.1.0/24	84	Security Console
New York Sales 2nd floor	10.1.2.0/24	85	Security Console
New York Sales 3rd floor	10.1.3.0/24	85	Security Console
New York IT	10.1.10.0/25	25	Security Console
New York Administration	10.1.10.128/25	25	Security Console
New York Printers Building 1	10.1.20.0/25	28	Security Console
New York Printers Building 2	10.1.20.128/25	28	Security Console
New York DMZ	172.16.0.0/22	30	Scan Engine 1
Madrid Sales Office 1	10.2.1.0/24	31	Scan Engine 2
Madrid Sales Office 2	10.2.2.0/24	31	Scan Engine 2
Madrid Sales Office 3	10.2.3.0/24	33	Scan Engine 2
Madrid Development Floor 2	10.2.10.0/24	65	Scan Engine 2

Madrid Development Floor 3	10.2.11.0/24	65	Scan Engine 2
Madrid Printers Building 3	10.2.20.0/24	35	Scan Engine 2
Madrid DMZ	172.16.10.0/24	15	Scan Engine 3

Selecting a Scan Engine or engine pool for a site

A Scan Engine is one of the components that a site must have. It discovers assets during scans and checks them for vulnerabilities or policy compliance. Scan Engines are controlled by the Security Console, which integrates their data into the database for display and reporting.

If you have deployed distributed Scan Engines or engine pools, or you are using Nexpose hosted Scan Engines, you will have a choice of engines or pools for this site. Otherwise, your only option is the local Scan Engine that was installed with the Security Console. It is also the default selection.

For more information about Scan Engine options:

- *Configuring distributed Scan Engines* on page 78
- *Working with Scan Engine pools* on page 83

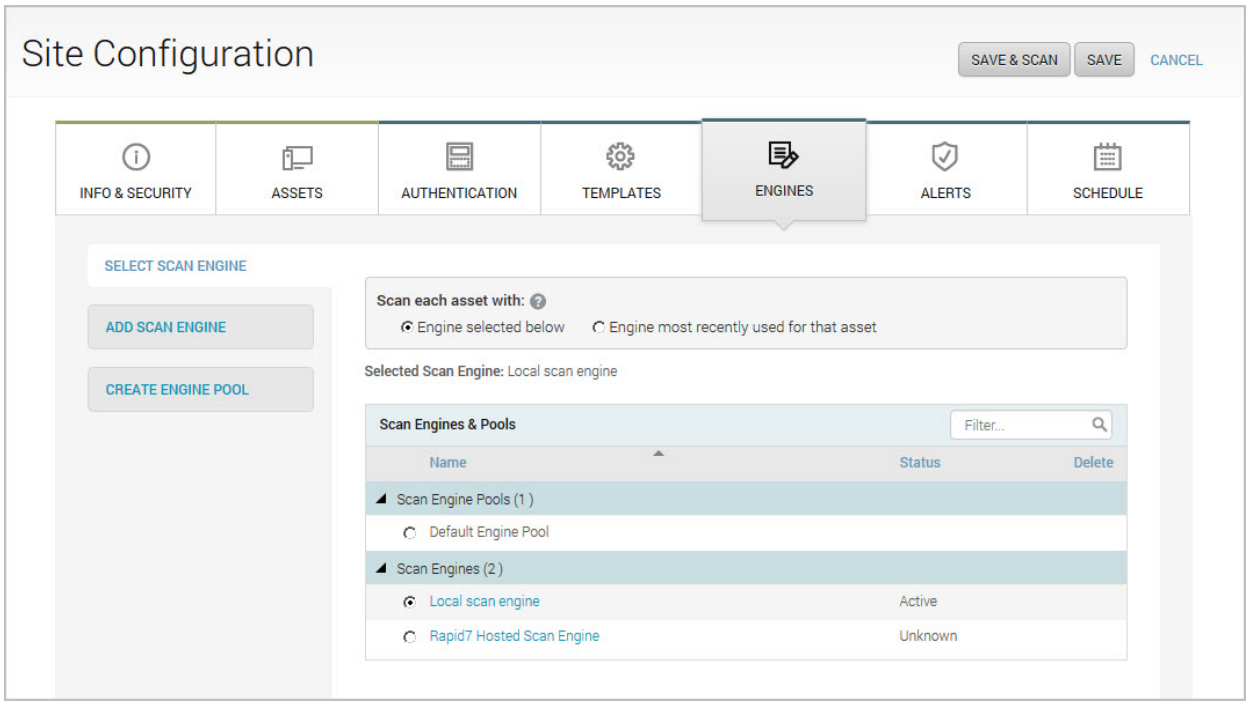
Note: If you created the site through the integration with VMware NSX, you cannot change the Scan Engine, which is automatically configured as part of the integration process. See *Integrating NSX network virtualization with scans* on page 203.

To change the Scan Engine selection:

- If you are adding an engine while configuring a new site, click the **Create site** button on the *Home* page.
- If you are adding a new engine option to an existing site, click that site's **Edit** icon in the *Sites* table on the *Home* page.

1. Click the **Engines** tab of the *Site Configuration*.
2. If you are scanning an asset group, select the desired option for scanning assets. See *Determining how to scan each asset when scanning asset groups* on page 76*Determining how to scan each asset when scanning asset groups*.

   Note: Although this option appears in any site configuration, it only applies when scanning asset groups.



Selecting a Scan Engine or pool

Tip: If you have many engines or pools you can make it easier to find the one you want by entering part of its name in the **Filter** text box.

3. Configure other site settings as desired.
4. Click **Save** or **Save & Scan**, depending on your preference.

Determining how to scan each asset when scanning asset groups

When scanning asset groups, you have the option to use the same Scan Engine or Scan Engine Pool to scan all the assets in a site, or to scan each asset with the Scan Engine that was previously used. The best choice depends on your network configuration: for example, if your assets are geographically dispersed, you may want to use the most recent Scan Engine for each asset so they will be more likely to be scanned by a Scan Engine in the same location.

To determine which Scan Engine to use for each asset:

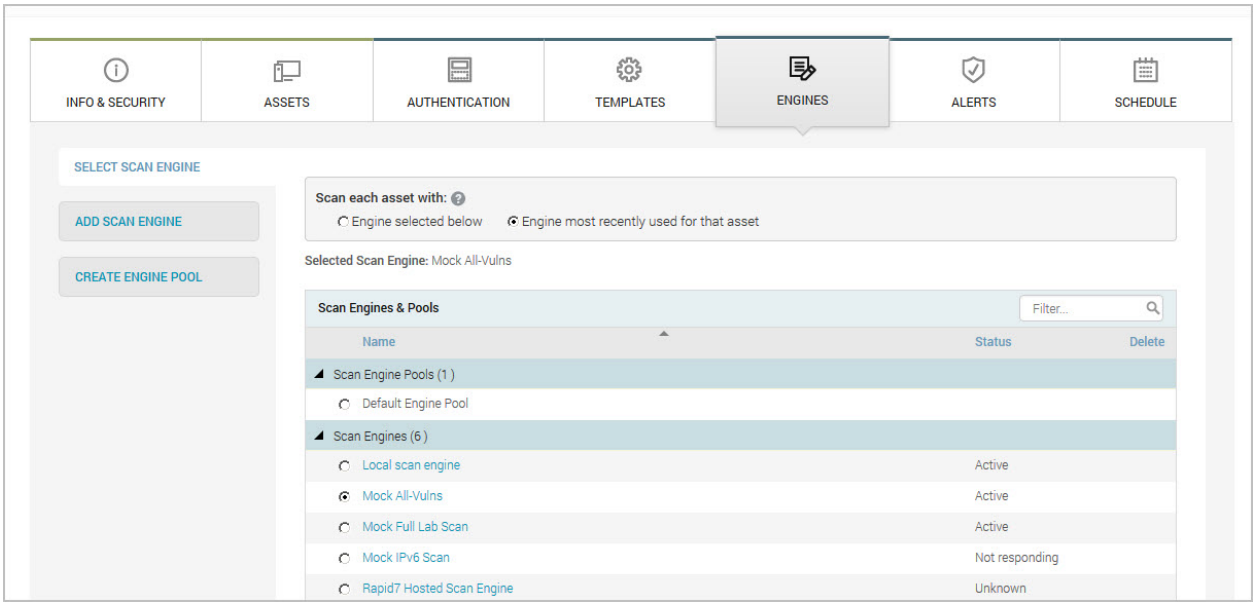
1. In the *Site Configuration*, go to the **Engines** tab.
2. If you want to scan all the assets with the same Scan Engine or Scan Engine Pool, select *Engine selected below*.

OR

Select *Engine most recently used for that asset*. This may result in different assets being scanned by different Scan Engines.

3. Select a Scan Engine or Scan Engine Pool from the list.

Note: Even if you chose to scan with the engine most recently used for this asset, this setting will still be used for any asset that has never been scanned before. Therefore, you should make a choice no matter which option you chose above.



Choosing to scan with the most recently used engine for each asset

If you select the option to scan with the engine most recently used for that asset, the *Scans* page may display multiple Scan Engines in the *Current Scans* table and the *Past Scans* table.

Viewing Scan Engine Status

On the page for a scan, you can view the *Scan Engines Status* table. To learn more, see *Running a manual scan* on page 222.

Configuring distributed Scan Engines

Your organization may distribute Scan Engines in various locations within your network, separate from your Security Console.Unlike the local Scan Engine, which is installed with the Security Console, you need to separately configure distributed engines and pair then with the console, as explained in this section.

Configuring a distributed Scan Engine involves the following steps:

- *Adding an engine* on page 78
- *Pairing the Scan Engine with the Security Console* on page 80
- *Assigning a site to the new Scan Engine* on page 82

Before you configure and pair a distributed Scan Engine

1. Install the Scan Engine. See the installation guide for instructions. You can download it from the Support page in Help.
2. Start the Scan Engine. You can only configure a new Scan Engine if it is running.

Configuring the Security Console to work with a new Scan Engine

By default, the Security Console initiates a TCP connection to Scan Engines over port 40814. If a distributed Scan Engine is behind a firewall, make sure that port 40814 is open on the firewall to allow communication between the Security Console and Scan Engine.

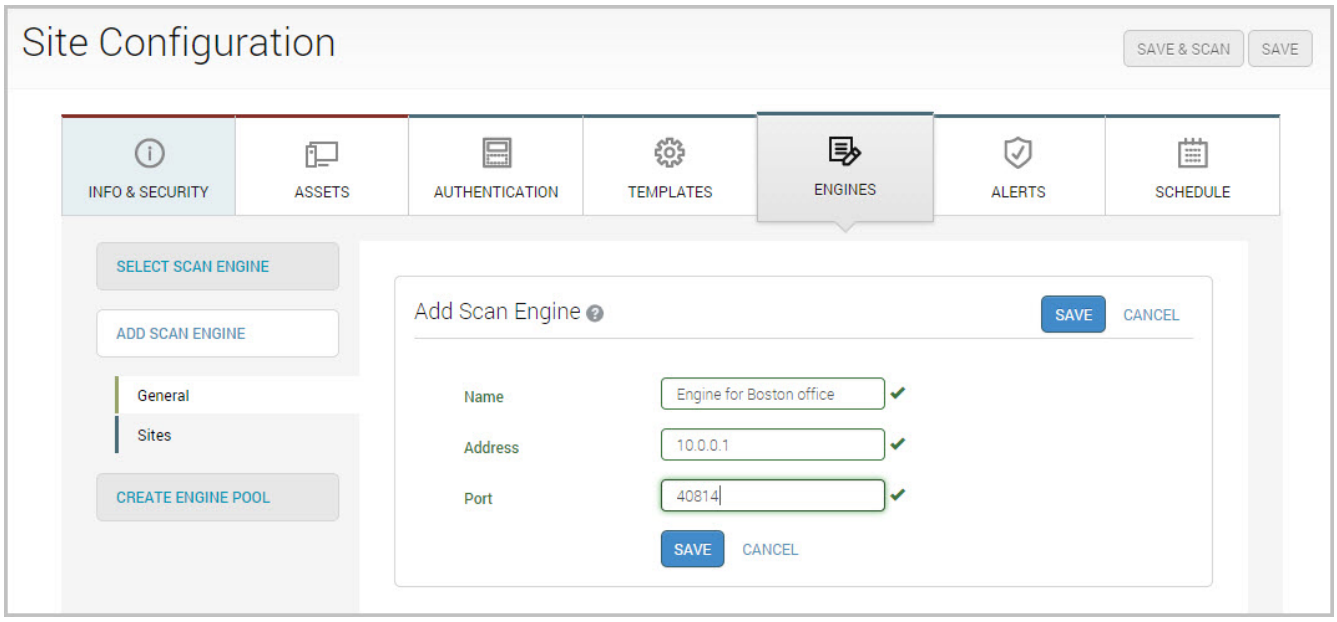
Adding an engine

The first step for integrating the Security Console and the new Scan Engine is adding information about the Scan Engine.

You can add a Scan Engine while you're configuring a site:

If you are adding an engine while configuring a new site, click the **Create site** button on the *Home* page.
If you are adding a new engine option to an existing site, click that site's **Edit** icon in the *Sites* table on the *Home* page.

1. In the *Site Configuration* click the **Engines** tab.
2. Select the **Add Scan Engine** tab and then the **General** tab.
3. Enter a unique name that will make it easy for you to remember the engine.
4. Enter the Scan Engine's address and port number on which it will listen for communication from the Security Console.
5. Click **Save**.



Adding a Scan Engine

After you add the engine, the Security Console creates the *consoles.xml* file. You will need to edit this file in the pairing process.

If you are a Global Administrator, you also have the option to add an engine through the *Administration* tab:

1. Click the **Administration** tab.

2. On the *Administration* page, click **Create** to the right of *Scan Engines*.
3. Click the **General** tab of the *Scan Engine Configuration* panel.
4. Enter a unique name that will make it easy for you to remember the engine.
5. Enter the IP address and port on for the computer on which the engine is installed.
6. If you have already created sites, you can assign sites to the new Scan Engine by going to the *Sites* page of this panel. If you have not yet created sites, you can perform this step during site creation.
7. Click **Save**.

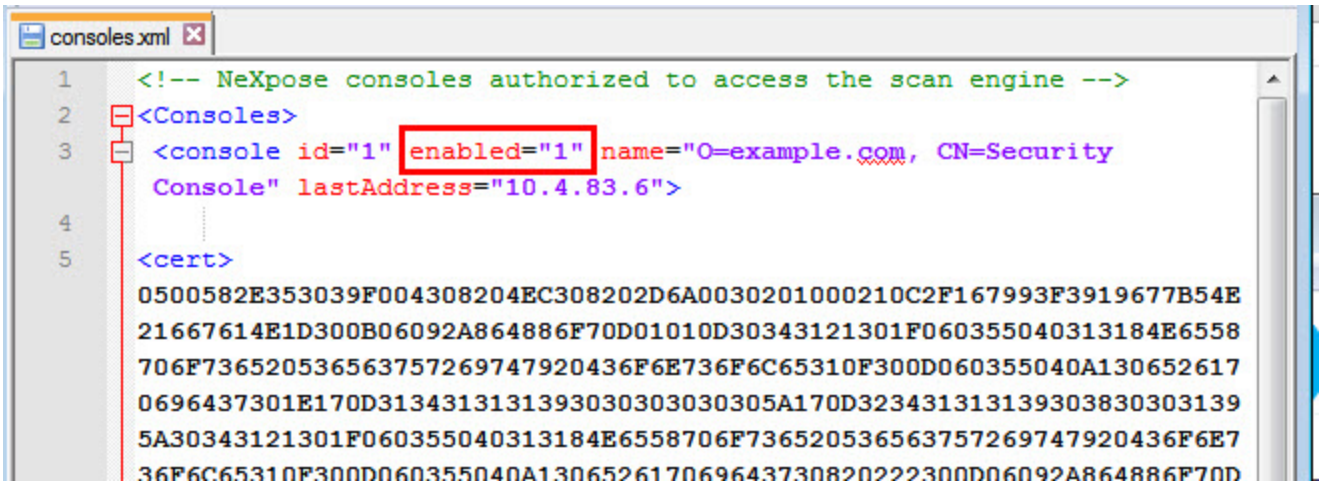
   After you add the engine, the Security Console creates the *consoles.xml* file. You will need to edit this file in the pairing process.

Pairing the Scan Engine with the Security Console

Note: You must log on to the operating system of the Scan Engine as a user with administrative permissions before performing the next steps.

Edit the *consoles.xml* file in the following step to pair the Scan Engine with the Security Console.

1. Open the consoles.xml file using a text editing program. Consoles.xml is located in the [installation_directory]/nse/conf directory on the Scan Engine.
2. Locate the line for the console that you want to pair with the engine. The console will be marked by a unique identification number and an IP address.
3. Change the value for the *Enabled* attribute from *0* to *1*.



The Scan Engine's consoles.xml file showing that the Security Console is enabled

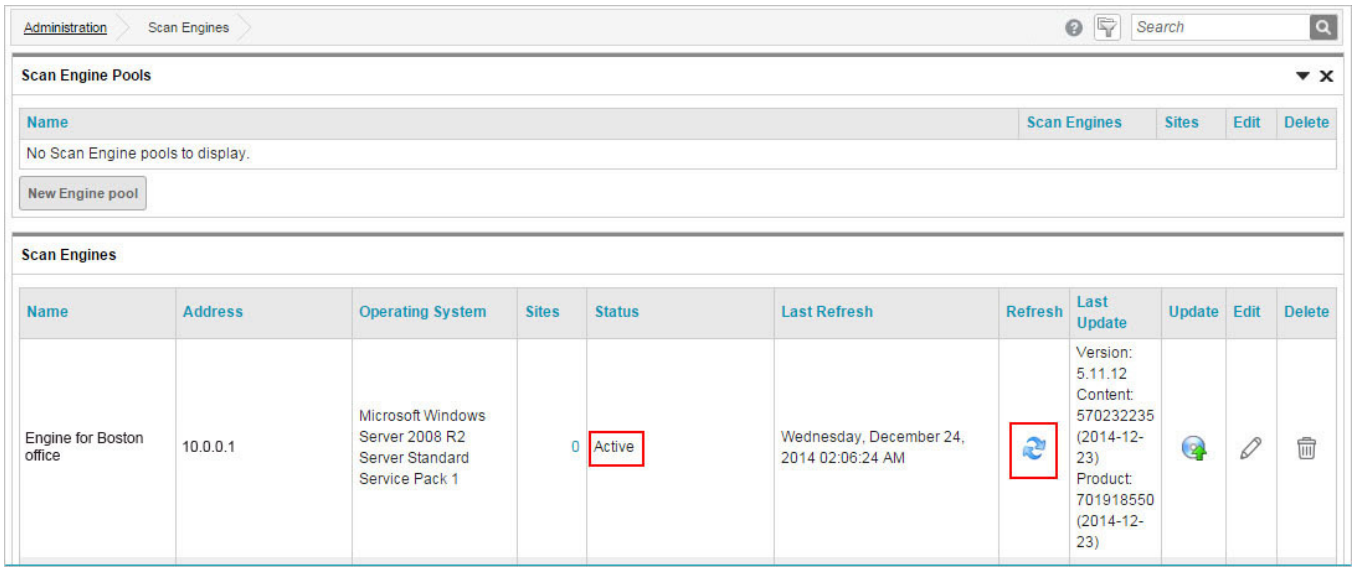
4. Save and close the file.
5. Restart the Scan Engine, so that the configuration change can take effect.

Verify that the console and engine are now paired:

1. Click the **Administration** tab.
2. On the *Administration* page, click **Manage** to the right of *Scan Engines*.
3. On the *Scan Engines* page, locate the Scan Engine that you added.

   Note that the status for the engine is *Unknown*.
4. Click the **Refresh** icon for the engine.

   The status changes to *Active*. You can now assign a site to this Scan Engine and run a scan with it.



*The Scan Engines table with the **Refresh** icon and Active status highlighted*

Note: If you ever change the name of the Scan Engine, you will have to pair it with the Security Console again. The engine name is critical to the pairing process.

On the *Scan Engines* page, you can also perform the following tasks:

- You can edit the properties of any listed Scan Engine by clicking **Edit** for that engine.
- You can delete a Scan Engine by clicking **Delete** for that engine.
- You can manually apply an available update to the scan engine by clicking **Update** for that engine. To perform this task using the command prompt, see *Using the command console* in the administrator's guide.

You can configure certain performance settings for all Scan Engines on the *Scan Engines* page of the Security Console configuration panel. For more information, see *Changing default Scan Engine settings* in the administrator's guide.

Assigning a site to the new Scan Engine

Note: If you have not yet set up a site, create one first. See *Creating and editing sites* on page 60.

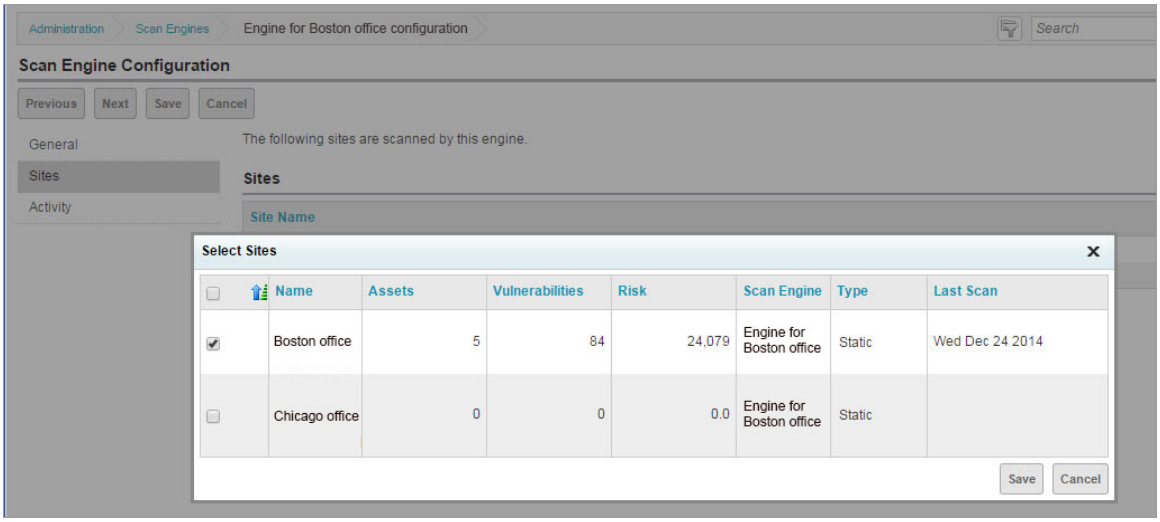
If you are assigning a site to an engine while configuring it, see *Selecting a Scan Engine or engine pool for a site* on page 75.

If you are assigning a site via the *Administration* tab:

1. Go to the *Sites* page of the *Scan Engine Configuration panel* and click **Select Sites**.

   The console displays a box listing all the sites in your network.

2. Click the check boxes for sites you wish to assign to the new Scan Engine and click **Save.**



Assigning a site to a Scan Engine

   The sites appear on the *Sites* page of the *Scan Engine Configuration* panel.

3. Click **Save** to save the new Scan Engine information.

Working with Scan Engine pools

You can improve the speed of your scans for large numbers of assets in a single site by pooling your Scan Engines. With pooling, the work it takes to scan one large site is split across multiple engines to maximize pool utilization.

Additionally, engine pooling can assist in cases of fault tolerance. For example, if one Scan Engine in the pool fails during a scan, it will transfer the scanning tasks of that asset to another engine within the pool.

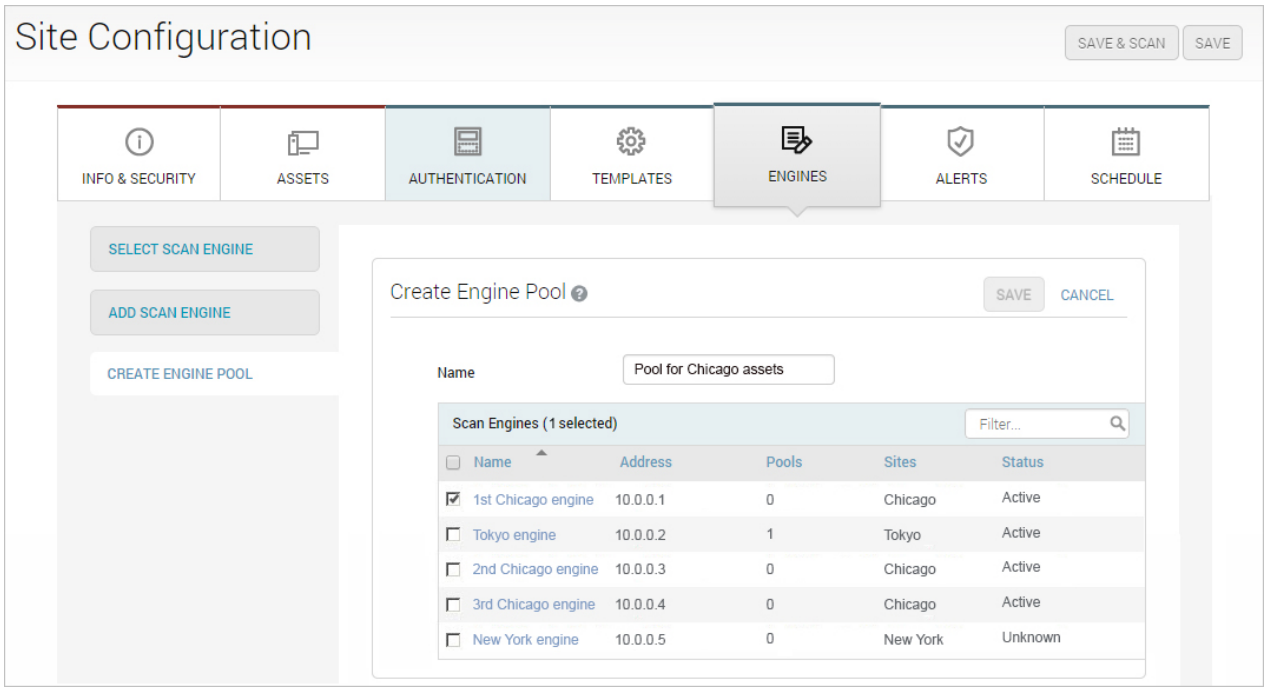
Note: To verify that you are licensed for Scan Engine pooling, See *Finding out what features your license supports* on page 671 .

Creating Scan Engine pools

You can add a Scan Engine while you're configuring a site:

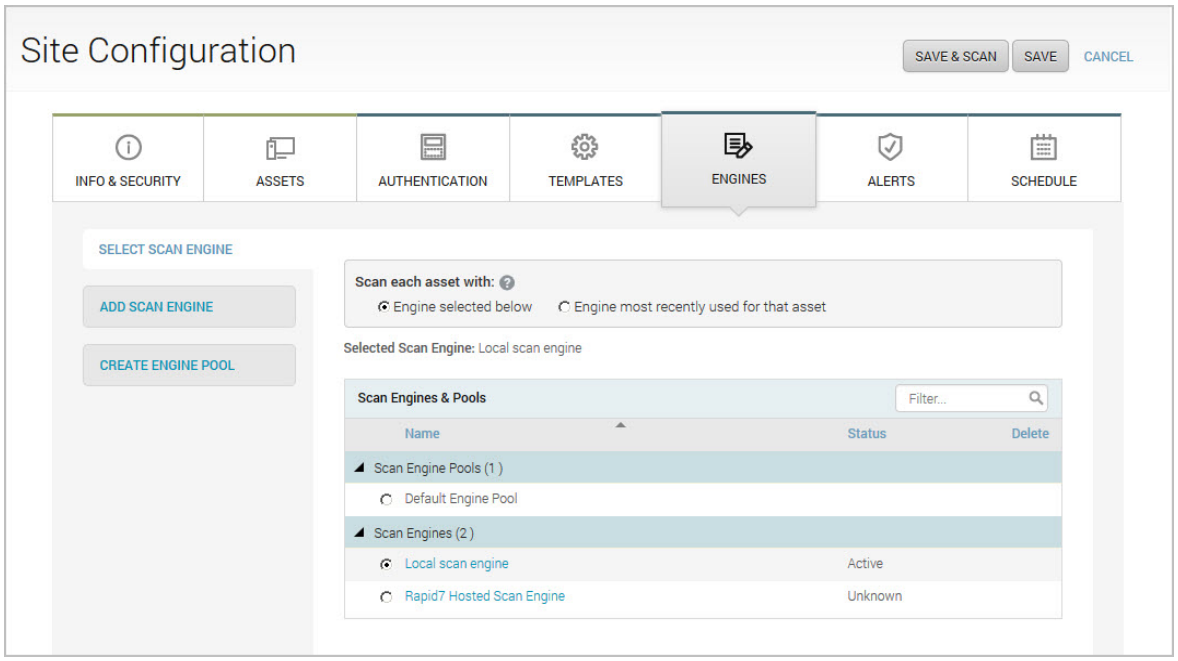
- If you are adding an engine pool while configuring a new site, click the **Create site** button on the *Home* page.
- If you are adding a new engine pool to an existing site, click that site's **Edit** icon in the *Sites* table on the *Home* page.

1. In the Site Configuration, click Engines.
2. Click **Create Engine Pool**.



Creating a Scan Engine Pool

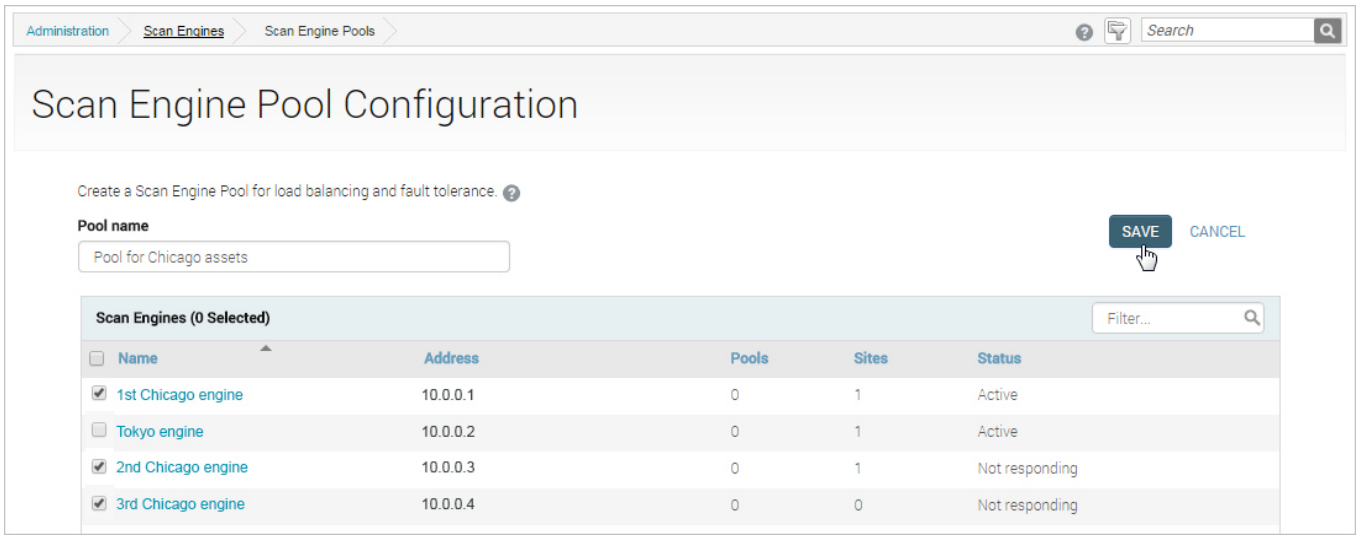
3. Enter a unique name to help you remember the pool.
4. Select the engines you want to include in the pool.
5. Click **Save**. Your new pool will appear on the *Scan Engines & Pools* table, which you can view by clicking the **Select Scan Engine** tab.



The Scan Engines & Pools table

If you are a Global Administrator, you can also create pools using the **Administration** tab:

1. Click the **Administration** tab.
2. Select **Scan Engine Pools** under *Scan Options*.

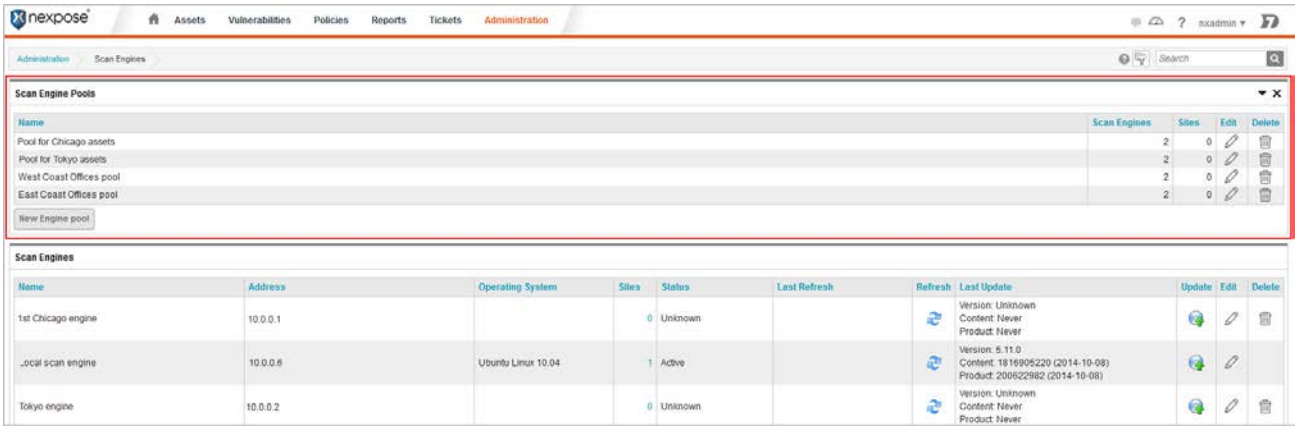


Creating a pool outside of the Site Configuration, via the Administration tab

The *Scan Engine Pool Configuration* page displays all of the engines that you have available (hosted and local engines cannot be used and won't appear), the number of pools they are in, the number of sites associated, and their status.

Note: Only engines with an active status will be effective in your pool. If your engine appears with an unknown or pending authorization status it can be added to a pool, but will not contribute to load balancing. For instructions on how to pair Scan Engines with the Security Console, see *Configuring distributed Scan Engines* on page 78.

3. Enter a unique name to help you remember pool.
4. Select the engines you want to include in the pool.
5. Click **Save**. Your new pool will appear listed on the *Scan Engines* page.



Scan Engine page with pools

Tip: For additional information on optimal deployment settings for Scan Engine pooling, see the section titled *Deploying Scan Engine Pools* in the administrator's guide.

Site optimization for pooling

You may already have the application configured to match single Scan Engines to individual sites. If you decide to start using pooling, you may not achieve optimal results by simply moving those engines into a pool.

For optimal results, you can make the following adjustments to your site configuration:

- Create a few larger sites with more assets rather than many small sites with fewer assets. Scan Engines allocate memory for each site which it is currently scanning. Having fewer sites prevents resource contention and ensures that more memory is available for each scan.

Note: If you do create a large site to replace your smaller ones, you will lose any data from pre-aggregated sites once you delete them.

- Schedule scans to run successively rather than concurrently.
- If you are going to run overlapping scans, stagger their start times as much as possible. This will prevent queued scan tasks from causing delays.

Tip: You can make scans complete more quickly by increasing the scan threads used. If the engine is already at capacity utilization, you can add more RAM to increase the amount of threads. For more information on tuning scan performance see *Tuning performance with simultaneous scan tasks* on page 585.

Selecting a scan template

You may need to scan different types of assets for different types of purposes at different times. A scan **template** is a predefined set of scan attributes that you can select quickly rather than manually define properties, such as target assets, services, and vulnerabilities. For a list of scan templates and suggestions on when to use them, see *Scan templates* on page 684. Nexpose includes a variety of preconfigured scan templates to help you assess your vulnerabilities according to the best practices for a given need.

Using varied templates is a good idea, as you may want to look at your assets from different perspectives. The first time you scan a site, you might just do a discovery scan to find out what is running on your network. Then, you could run a vulnerability scan using the Full Audit template, which includes a broad and comprehensive range of checks. If you have assets that are about to go into production, it might be a good time to scan them with a Denial-of-Service template. Exposing them to unsafe checks is a good way to test their stability without affecting workflow in your business environment. You may also want to apply different templates to different types of assets; for instance, Web audit for Web servers and Web applications.

A Global Administrator can also customize scan templates or create new ones to suit your organization's particular needs. By creating sites of selected assets and applying the most relevant scan template, you can conduct scans that are specific to your needs. See *Configuring custom scan templates* on page 582 for more information. Keep in mind that the scans must balance three critical performance factors: time, accuracy, and resources. If you customize a template to scan more quickly by adding threads, for example, you may pay a price in bandwidth.

Selecting a scan template

If you want to change the scan template for an existing site, click that site's **Edit** icon in the Sites table on the Home page.

If you want to select the scan template while creating a new site, click the **Create site** button on the Home page.

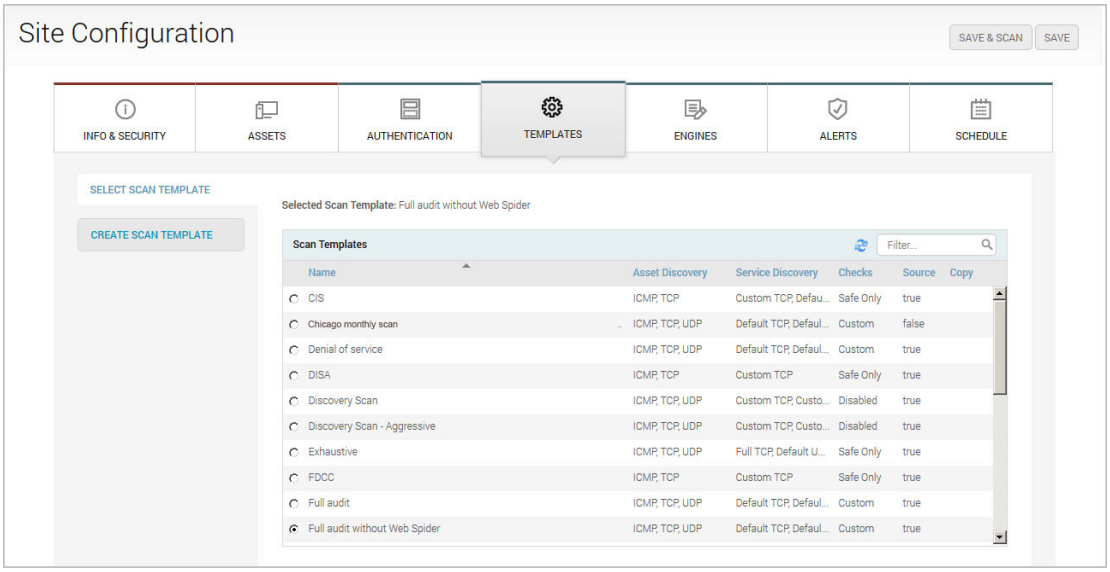
Note: If you created the site through the integration with VMware NSX, you cannot change the scan template, which is automatically assigned as part of the integration process. The template is Full Audit. See *Integrating NSX network virtualization with scans* on page 203.

Selecting an existing scan template

1. In the *Site Configuration*, go to the *Templates* tab.
2. Select an existing scan template from the table.

   The default is *Full audit without Web Spider*. This is a good initial scan, because it provides full coverage of your assets and vulnerabilities, but runs faster than if Web spidering were included.

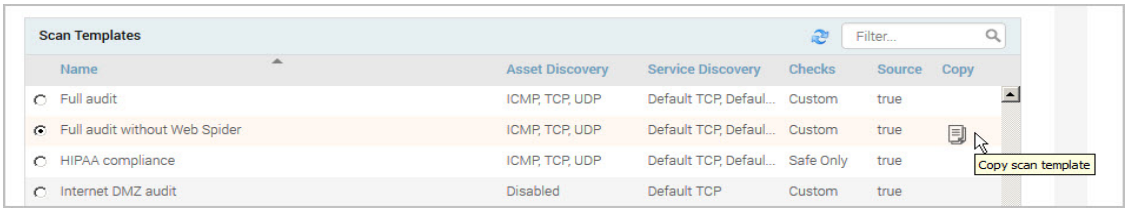
3. Save your changes.



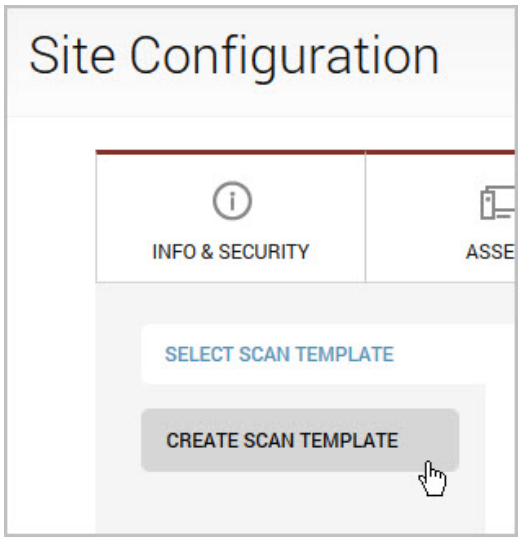
Default scan template selection

Creating a new scan template

1. Click the **Copy** icon next to the listed template you want to base the new one on, or click **Create Scan Template** to start from scratch.



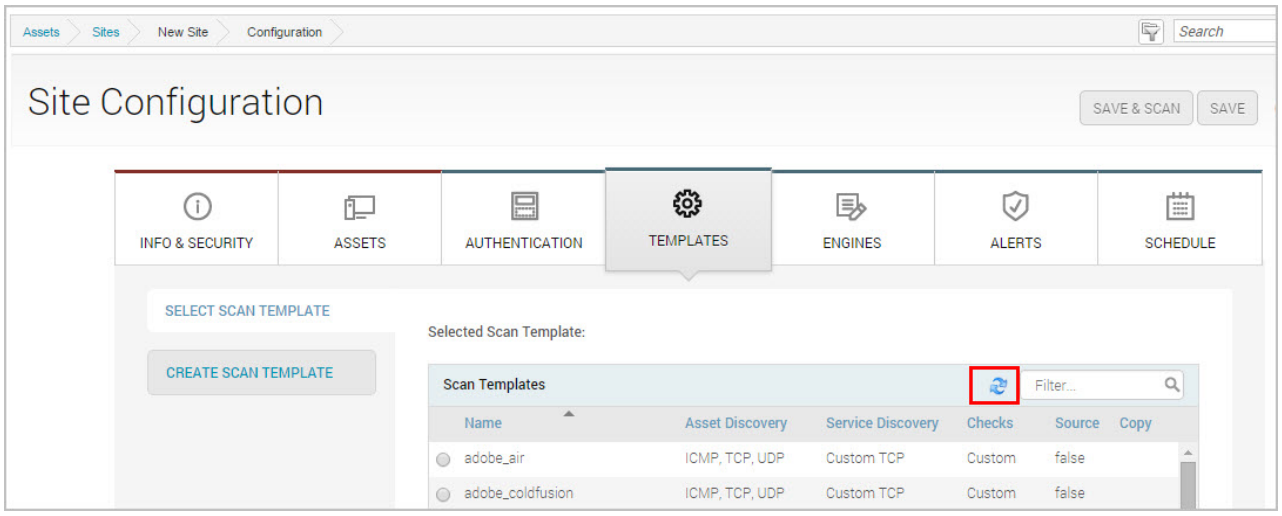
Copying an existing scan template



Creating a new scan template

A new tab will open with the *Scan Template Configuration*.

2. Change the template as desired. See *Configuring custom scan templates* on page 582 for more information.
3. Click **Save**.
4. Return to the tab with the *Scan Template Configuration*.
5. Click the **Refresh** icon at the top of the *Scan Templates* table to make the new template appear.



Refreshing the Scan Templates table display

6. Save your changes.

Targeted scanning: using multiple templates in a site

Nexpose retains all vulnerability results based on different scan templates within a site. This allows you to run targeted scans of your assets with different templates without affecting results that are not part of current scan configuration.

The benefits

When scheduling scans for your site, you can apply different templates to specific scan windows. For example, schedule a recurring scan to run on the day after Patch Tuesday each month with a template configured to verify the latest Microsoft patches. Then schedule scans with a different template to run on other days.

You will can check the same set of assets for different, specific vulnerabilities. If a zero-day threat is reported, customize a template that only includes checks for that vulnerability. After remediating the zero-day, resume scanning with a template that you routinely use for your site.

How targeted scanning works

At the vulnerability level

When you run successive scans for the same vulnerability, even if it was previously scanned with a different template, the most current result replaces previous results in the scan history for the affected site. Take the following example:

1. You run one scan to check for a zero-day vulnerability.
2. Results show that it exists in your environment.
3. You remediate the issue and run the scan again, this time with negative results.
4. After the second scan, your results will no longer show the zero-day vulnerability in your scan history.

At the port level

If your alternating scan templates include different target ports, your results depend on which ports you are scanning for a specific vulnerability, as in the following example:

You run one scan to check for a self-signed certificate, using a template that includes port 80. The results are positive. You run another scan for the same vulnerability, but this time you use a

template that does not include port 80. Regardless of the results of the second scan, your site's scan data will include a positive result for self-signed certificate on port 80.

Configuring scan credentials

In this topic:

- *Shared credentials vs. site-specific credentials* on page 94
- *Credentials and the expert system* on page 94

Related topics:

- *Maximizing security with credentials* on page 96
- *Authentication on Windows: best practices* on page 122
- *Authentication on Unix and related targets: best practices* on page 124
- *Configuring site-specific scan credentials* on page 97
- *Managing shared scan credentials* on page 103
- *Using SSH public key authentication* on page 108
- *Elevating permissions* on page 112
- *Using LM/NTLM hash authentication* on page 116
- *Using PowerShell with your scans* on page 119
- *Configuring scan authentication on target Web applications* on page 133

Scanning with credentials allows you to gather information about your network and assets that you could not otherwise access. You can inspect assets for a wider range of vulnerabilities or security policy violations. Additionally, authenticated scans can check for software applications and packages and verify patches. When you scan a site with credentials, target assets in that site authenticate the Scan Engine as they would an authorized user.

Topics in this section explain how to set up and test credentials for a site as well as shared scan credentials, which you can use in multiple sites. Certain authentication options, such as SSH public key and LM/NTLM hash, require additional steps, which are covered in related topics. You can also learn best practices for getting the most out of credentials, such as expanding authentication with elevated permissions.

Shared credentials vs. site-specific credentials

Two types of scan credentials can be created in the application, depending on the role or permissions of the user creating them:

- *Shared* credentials can be used in multiple sites.
- *Site-specific* credentials can only be used in the site for in which they are configured.

The range of actions that a user can perform with each type depends on the user's role or permissions, as indicated in the following table:

Credentials type	How it is created	Actions that can be performed by a Global Administrator or user with Manage Site permission	Actions that can be performed by a Site Owner
shared	A Global Administrator or user with the Manage Site permission creates it on the *Administration* > *Shared Scan Credentials* page.	Create, edit, delete, assign to a site, restrict to an asset. Enable or disable the use of the credentials in any site.	Enable or disable the use of the credentials in sites to which the Site Owner has access.
site-specific	A Global Administrator or Site Owner creates it in the configuration for a specific site.	Within a specific site to which the Site Owner has access: Create, edit, delete, enable or disable the use of the credentials in that site.	Within a specific site to which the Site Owner has access: Create, edit, delete, enable or disable the use of the credentials in that site.

Credentials and the expert system

The application uses an expert system at the core of its scanning technology in order to chain multiple actions together to get the best results when scanning. For example, if the application is able to use default configurations to get local access to an asset, then it will trigger additional actions using that access. The Nexpose Expert System paper outlines the benefits of this approach and can be found here: http://information.rapid7.com/using-an-expert-system-for-deeper-vulnerability-scanning.html?LS=2744168&CS=web. The effect of the expert system is that you may see scan results beyond those directly expected from the credentials you provided;

for example, if some scan targets cannot be accessed with the specified credentials, but can be accessed with a default password, you will also see the results of those checks. This behavior is similar to the approach of a hacker and enables Nexpose to find vulnerabilities that other scanners may not.

Maximizing security with credentials

The application provides features to protect your credentials from unauthorized use. It securely stores and transmits credentials using encryption so that no end users can retrieve unencrypted passwords or keys once they have been stored for scanning. Global Administrators can assign permission to add and edit credentials to only those users that should have that level of access. For more information, see the topic *Managing users and authentication* in the administrator's guide. When creating passwords, make sure to use standard best practices, such as long, complex strings with combinations of lower- and upper-case letters, numerals, and special characters.

Security best practices on Windows

If you plan to run authenticated scans on Windows assets, keep in mind some security strategies related to automated Windows authentication. Compromised or untrusted assets can be used to steal information from systems that attempt to log onto them with credentials. This attack method threatens any network component that uses automated authentication, such as backup services or vulnerability assessment products.

There are a number of countermeasures you can take to help prevent this type of attack or mitigate its impact. For example, make sure that Windows passwords for Nexpose contain 32 or more characters generated at random. And change these passwords on a regular basis.

See the white paper at https://community.rapid7.com/docs/DOC-2881 for key strategies and mitigation techniques.

Configuring site-specific scan credentials

In this topic:

- *Starting configuration for a new set of site-specific credentials*
- *Configuring the account for authentication*
- *Testing the credentials*
- *Limiting the credentials to a single asset and port*
- *Enabling a previously created set of credentials for use in a site*
- *Editing a previously created set of site credentials*

In this topic, you will learn how set up and test credentials for a site, how to restrict them to a specific asset or port, and how to edit and enable the use of previously created credentials.

When configuring scan credentials in a site, you have two options:

- Create a new set of credentials. Credentials created within a site are called *site-specific* credentials and cannot be used in other sites.
- Enable a set of previously created credentials to be used in the site. This is an option if site-specific credentials have been previously created in your site or if shared credentials have been previously created and then assigned to your site.

Note: To learn about credential types, see *Managing shared scan credentials* on page 103.

Starting configuration for a new set of site-specific credentials

The first action in creating new site-specific scan credentials is naming and describing them. Think of a name and description that will help you recognize at a glance which assets the credentials will be used for. This will be helpful, especially if you have to manage many sets of credentials.

If you want to add credentials while configuring a new site, click the **Create site** button on the *Home* page.

If you want to add credentials for an existing site, click that site's **Edit** icon in the *Sites* table on the *Home* page.

Note: If you created the site through the integration with VMware NSX, you cannot edit scan credentials, which are unnecessary because the integration provides Nexpose with the depth of access to target assets that credentials would otherwise provide. See *Integrating NSX network virtualization with scans* on page 203.

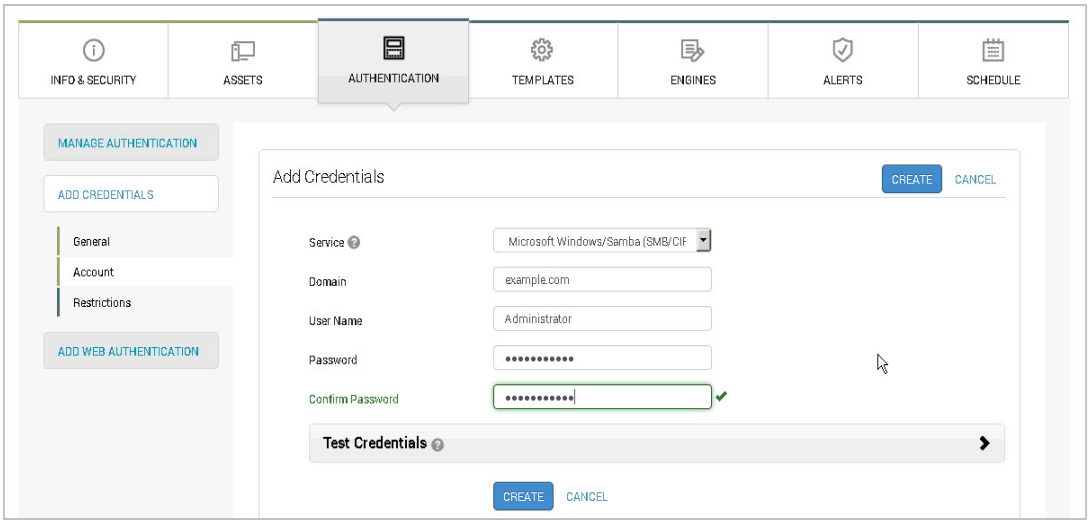
1. Click the **Authentication** link in the site configuration .
2. Click **Add Credentials**.
3. In the *Add Credentials* form, enter a name and description for the new set of credentials.
4. Continue with configuring the account, as described in the next section.

Configuring the account for authentication

If you do not know what authentication service to select or what credentials to use for that service, consult your network administrator.

Note: All credentials are protected with RSA encryption and triple DES encryption before they are stored in the database.

1. Click the **Account** under the **Add Credentials** tab.
2. Select an authentication service or method from the drop-down list.
3. Enter all requested information in the appropriate text fields.



Configuring an account for site credentials

4. If you want to test the credentials or restrict them see the following two sections. Otherwise, click **Create**.

The newly created credentials appear in the *Scan Credentials* table, which you can view by clicking **Manage Authentication**.

Testing the credentials

You can verify that a target asset in your site will authenticate the Scan Engine with the credentials you've entered. It is a quick method to ensure that the credentials are correct before you run the scan.

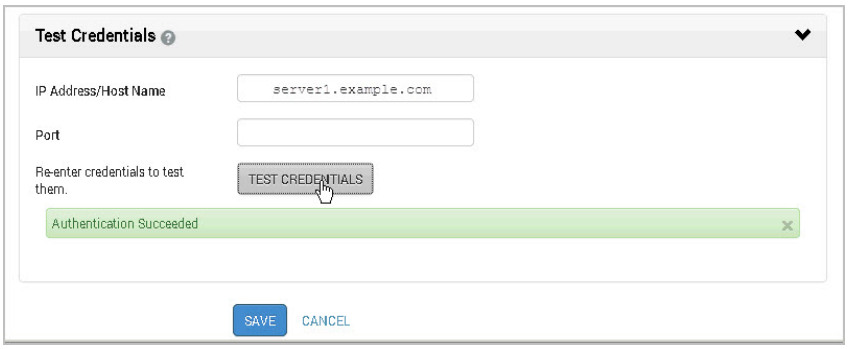
1. In the *Add Credentials* form, expand the *Test Credentials* section by clicking the arrow.
2. Expand the **Test Credentials** section.
3. Enter the name or IP address of the authenticating asset.

Note: If you do not enter a port number, the Security Console will use the default port for the service. For example, the default port for CIFS is 445.

1. To test authentication on a single port, enter a port number.
2. Click **Test credentials**.

Note: If you are testing *Secure Shell (SSH)* or *Secure Shell (SSH) Public Key* credentials and you have assigned elevated permissions, both credentials will be tested. Credentials for authentication on the target are tested first, and a message appears if the credentials failed. Permission elevation failures are reported in a separate message. See *Using SSH public key authentication* on page 108.

3. Note the result of the test. If it was not successful, review and change your entries as necessary, and test them again. The Security Console and scan logs contain information about authentication failure when testing or scanning with these credentials. See *Working with log files* in the administrator's guide.



A successful test of site credentials

4. If you want to restrict the credentials to a specific asset or port, see the following section.

   Otherwise, click **Create**.

Limiting the credentials to a single asset and port

If a particular set of credentials is only intended for a specific asset and/or port, you can restrict the use of the credentials accordingly. Doing so can prevent scans from running unnecessarily longer due to authentication attempts on assets that don't recognize the credentials.

If you restrict credentials to a specific asset and/or port, they will not be used on other assets or ports.

Specifying a port allows you to limit your range of scanned ports in certain situations. For example, you may want to scan Web applications using HTTP credentials. To avoid scanning all Web services within a site, you can specify only those assets with a specific port.

1. Click the **Account** under the **Add Credentials** tab.
2. Enter only the host name or IP address of the asset that you want to restrict the credentials to.

   OR

   Enter host name or IP address of the asset and the number of the port that you want to restrict the credentials to.

Note: If you do not enter a port number, the Security Console will use the default port for the service. For example, the default port for CIFS is 445.

3. When you have finished configuring the set of credentials, click **Create**.

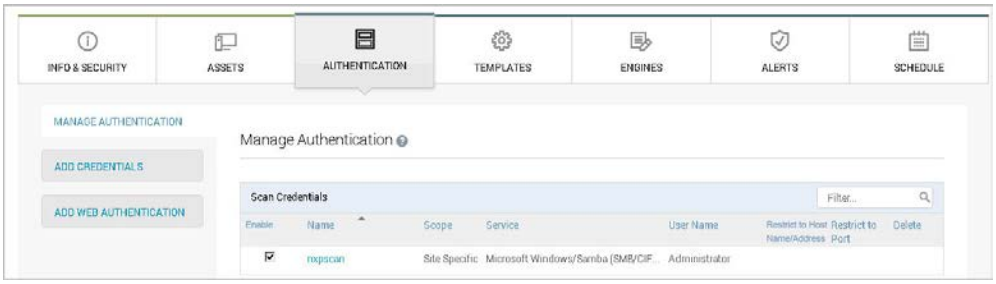
Tip: To verify successful scan authentication on a specific asset, search the scan log for that asset. If the message "*A set of [service_type] administrative credentials have been verified.*" appears with the asset, authentication was successful.

Enabling a previously created set of credentials for use in a site

If a set of credentials is not enabled for a site, the scan will not attempt authentication on target assets with those credentials. Make sure to enable credentials if you want to use them.

1. To enable credentials for an existing site, click that site's **Edit** icon in the *Sites* table on the *Home* page.
2. Click the **Authentication** link in the Site configuration .

   The *Scan Credentials* table lists any site-specific credentials that were created for the site or any shared credentials that were assigned to the site. For more information, see *Managing shared scan credentials* on page 103.
3. Select the **Enable** check box for any set of credentials that you want to scan with.
4. Click the **Save** button for the site configuration.



Enabling a set of credentials for a site

Editing a previously created set of site credentials

Note: You cannot edit shared scan credentials in the *Site Configuration* panel. To edit shared credentials, go to the *Administration* page and select the **manage** link for Shared scan credentials. See *Editing shared credentials that were previously created* on page 107. You must be a Global Administrator or have the Manage Site permission to edit shared scan credentials.

The ability to edit credentials can be very useful, especially if passwords change frequently. You can only edit site-specific credentials in a *Site Configuration* panel.

1. To enable credentials for an existing site, click that site's **Edit** icon in the *Sites* table on the *Home* page.
2. Click the **Authentication** link in the Site configuration .
3. Click the hyperlink name of any set of credentials that you want to edit.
4. Change the configuration as desired. See the following topics for more information:

- *Starting configuration for a new set of site-specific credentials* on page 97
- *Configuring the account for authentication* on page 104
- *Testing the credentials* on page 99
- *Limiting the credentials to a single asset and port* on page 100

5. When you have finished editing the credentials, click **Save**.

Managing shared scan credentials

You can create and manage scan credentials that can be used in multiple sites. Using *shared credentials* can save time if you need to perform authenticated scans on a high number of assets in multiple sites that require the same credentials. It's also helpful if these credentials change often. For example, your organization's security policy may require a set of credentials to change every 90 days. You can edit that set in one place every 90 days and apply the changes to every site where those credentials are used. This eliminates the need to change the credentials in every site every 90 days.

To configure shared credentials, you must have a Global Administrator role or a custom role with Manage Site permissions.

Note: To learn the differences between shared and site-specific credentials, see *Shared credentials vs. site-specific credentials* on page 94.

Creating a set of shared scan credentials

Creating a set of shared scan credentials includes the following actions:

1. *Naming and describing the new set of shared credentials* on page 103
2. *Configuring the account for authentication* on page 104
3. *Restricting the credentials to a single asset and port* on page 105
4. *Assigning shared credentials to sites* on page 106

After you create a set of shared scan credentials you can take the following actions to manage them:

- *Viewing shared credentials* on page 107
- *Editing shared credentials that were previously created* on page 107

Naming and describing the new set of shared credentials

Tip: Think of a name and description that will help Site Owners recognize at a glance which assets the credentials will be used for.

1. Click the **Administration** tab.

2. On the Administration page, click the **create** link for *Shared Scan Credentials*.

   The Security Console displays the *General* page of the *Shared Scan Credentials Configuration* panel.

3. Enter a name for the new set of credentials.
4. Enter a description for the new set of credentials.
5. Continue with configuring the account, as described in the next section.

Configuring the account for authentication

Configuring the account involves selecting an authentication method or service and providing all settings that are required for authentication, such as a user name and password.

If you do not know what authentication service to select or what credentials to use for that service, consult your network administrator.

1. Go to the *Account* page of the *Shared Scan Credentials Configuration* panel.
2. Select an authentication service or method from the drop-down list.
3. Enter all requested information in the appropriate text fields.
4. If you want to test the credentials or restrict them see the following two sections. Otherwise, click **Save**.

Testing shared scan credentials

You can verify that a target asset will authenticate a Scan Engine with the credentials you've entered. It is a quick method to ensure that the credentials are correct before you run the scan.

Tip: To verify successful scan authentication on a specific asset, search the scan log for that asset. If the message "*A set of [service_type] administrative credentials have been verified.*" appears with the asset, authentication was successful.

For shared scan credentials, a successful authentication test on a single asset does not guarantee successful authentication on all sites that use the credentials.

1. Go to the *Account* page of the *Credentials Configuration* panel.
2. Expand the **Test Credentials** section.
3. Select the Scan Engine with which you will perform the test.
4. Enter the name or IP address of the authenticating asset.
5. To test authentication on a single port, enter a port number.

Note: If you do not enter a port number, the Security Console will use the default port for the service. For example, the default port for CIFS is 445.

6. Click **Test credentials**.

   Note the result of the test. If it was not successful, review and change your entries as necessary, and test them again.

7. Upon seeing a successful test result, configure any other settings as desired.
8. If you want to restrict the credentials to a specific asset or port, see the following section. Otherwise, click **Save**.

Restricting the credentials to a single asset and port

If a particular set of credentials is only intended for a specific asset and/or port, you can restrict the use of the credentials accordingly. Doing so can prevent scans from running unnecessarily longer due to authentication attempts on assets that don't recognize the credentials.

If you restrict credentials to a specific asset and/or port, they will not be used on other assets or ports.

Specifying a port allows you to limit your range of scanned ports in certain situations. For example, you may want to scan Web applications using HTTP credentials. To avoid scanning all Web services within a site, you can specify only those assets with a specific port.

1. Go to the *Restrictions* page of the *Shared Scan Credentials Configuration* panel.
2. Enter the host name or IP address of the asset that you want to restrict the credentials to.

   OR

   Enter host name or IP address of the asset and the number of the port that you want to restrict the credentials to.

Note: If you do not enter a port number, the Security Console will use the default port for the service. For example, the default port for CIFS is 445.

3. When you have finished configuring the set of credentials, click **Save**.

Assigning shared credentials to sites

You can assign a set of shared credentials to one or more sites. Doing so makes them appear in lists of available credentials for those site configurations. Site Owners still have to enable the credentials in the site configurations. See *Configuring scan credentials* on page 93.

To assign shared credentials to sites, take the following steps:

1. Go to the *Site assignment* page of the *Shared Scan Credentials Configuration* panel.
2. Select one of the following assignment options:

- **Assign the credentials to all current and future sites**
- **Create a custom list of sites that can use these credentials**

   If you select the latter option, the Security Console displays a button for selecting sites.

3. Click **Select Sites**.

   The Security Console displays a table of sites.

4. Select the check box for each desired site, or select the check box in the top row for all sites. Then click **Add sites**.

   The selected sites appear on the *Site Assignment* page.

5. Configure any other settings as desired. When you have finished configuring the set of credentials, click **Save**.

Viewing shared credentials

1. Click the **Administration** tab.

   The Security Console displays the *Administration* page.

2. Click the **manage** link for *Shared Scan Credentials*.

   The Security Console displays a page with a table that lists each set of shared credentials and related configuration information.

Editing shared credentials that were previously created

The ability to edit credentials can be very useful, especially if passwords change frequently.

1. Click the **Administration** tab.

   The Security Console displays the *Administration* page.

2. Click the **manage** link for *Shared Scan Credentials*.

   The Security Console displays a page with a table that lists each set of shared credentials and related configuration information.

3. Click the name of the credentials that you want to change, or click **Edit** for that set of credentials.

4. Change the configuration as desired. See the following topics for more information:

- *Naming and describing the new set of shared credentials* on page 103
- *Configuring the account for authentication* on page 104
- *Testing shared scan credentials* on page 104
- *Restricting the credentials to a single asset and port* on page 105
- *Assigning shared credentials to sites* on page 106

Using SSH public key authentication

You can use Nexpose to perform credentialed scans on assets that authenticate users with SSH public keys.

This method, also known as asymmetric key encryption, involves the creation of two related keys, or large, random numbers:

- a public key that any entity can use to encrypt authentication information
- a private key that only trusted entities can use to decrypt the information encrypted by its paired public key

When generating a key pair, keep the following guidelines in mind:

- The application supports SSH protocol version 2 RSA and DSA keys.
- Keys must be OpenSSH-compatible and PEM-encoded.
- RSA keys can range between 768 and 16384 bits.
- DSA keys must be 1024 bits.

This topic provides general steps for configuring an asset to accept public key authentication. For specific steps, consult the documentation for the particular system that you are using.

The ssh-keygen process will provide the option to enter a pass phrase. It is recommended that you use a pass phrase to protect the key if you plan to use the key elsewhere.

Generating a key pair

1. Run the ssh-keygen command to create the key pair, specifying a secure directory for storing the new file.

   This example involves a 2048-bit RSA key and incorporates the /tmp directory, but you should use any directory that you trust to protect the file.

   ```
   ssh-keygen -t rsa -b 2048 -f /tmp/id_rsa
   ```

   This command generates the private key files, *id_rsa*, and the public key file, *id_rsa.pub*.

2. Make the public key available for the application on the target asset.
3. Make sure that the computer with which you are generating the key has a .ssh directory. If not, run the mkdir command to create it:

   ```
   mkdir /home/[username]/.ssh
   ```

4. Copy the contents of the public key that you created by running the command in step 1. The file is in /tmp/id_rsa.pub file.

Note: Some checks require root access.

   Append the contents on the target asset of the /tmp/id_rsa.pub file to the .ssh/authorized_keys file in the home directory of a user with the appropriate access-level permissions that are required for complete scan coverage.

   ```
   cat /[directory]/id_rsa.pub >> /home/[username]/.ssh/authorized_keys
   ```

5. Provide the private key.

After you provide the private key you must provide the application with SSH public key authentication.

Providing SSH public key authentication

If you want to add SSH credentials while configuring a new site, click the **Create site** button on the *Home* page.

If you want to add SSH credentials for an existing site, click that site's **Edit** icon in the *Sites* table on the *Home* page.

1. Click the **Authentication** link in the site configuration .
2. Click **Add Credentials**.
3. In the *Add Credentials* form, enter a name and description for a new set of credentials if necessry.
4. Click **Account** under *Add Credentials*.
5. Select *Secure Shell (SSH) Public Key* as the from **Service** drop-down list.

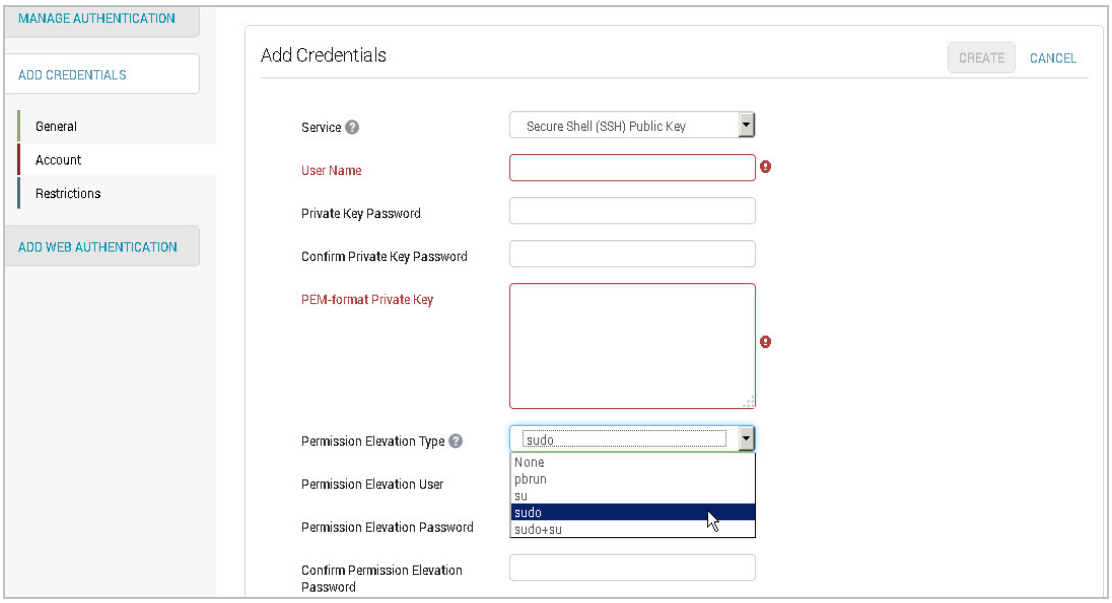
Note: ssh/authorized_keys is the default file for most OpenSSH- and Drop down-based SSH daemons. Consult the documentation for your Linux distribution to verify the appropriate file.

This authentication method is different from the method listed in the drop-down as *Secure Shell (SSH)*. This latter method incorporates passwords instead of keys.

6. Enter the appropriate user name.
7. (Optional) Enter the Private key password used when generating the keys.
8. Confirm the private key password.
9. Copy the contents of that file into the **PEM-format private key** text box. The private key that you created is the /tmp/id_rsa file on the target asset.
10. (Optional) Elevate permissions to *sudo* or *su*.

    You can elevate permissions for both *Secure Shell (SSH)* and *Secure Shell (SSH) Public Key* services.
11. (Optional) Enter the appropriate user name. The user name can be empty for sudo credentials. If you are using su credentials with no user name the credentials will default to root as the user name.

    If the SSH credential provided is a root credential, user ID =0, the permission elevation credentials will be ignored, even if the root account has been renamed. The application will ignore the permission elevation credentials when any account, root or otherwise named, with user ID 0 is specified.
12. When you have finished configuring the credentials, click **Create** if it is a new set or **Save** if it is a previously created set.



SSH Public Key configuration

For additional optional steps, see the following topics:

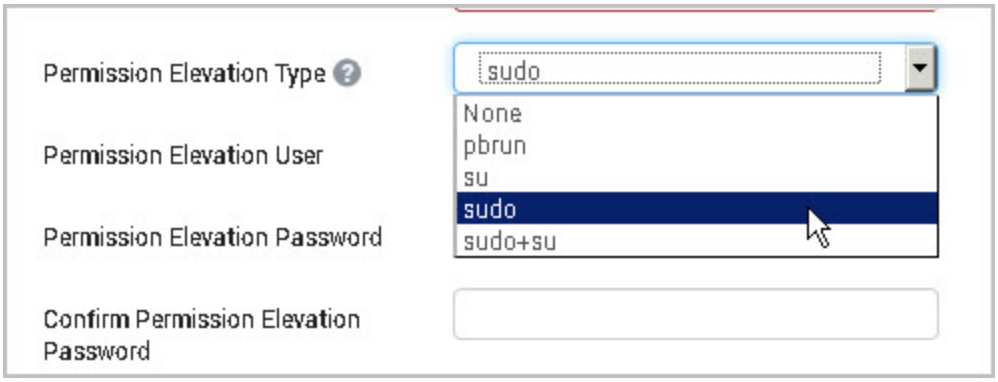
- *Testing the credentials* on page 99
- *Limiting the credentials to a single asset and port* on page 100 *Limiting the credentials to a single asset and port*
- *Elevating permissions* on page 112

Elevating permissions

With SSH authentication you can elevate Scan Engine permissions to administrative or root access, which is required for obtaining certain data. For example, Unix-based CIS benchmark checks often require administrator-level permissions. Incorporating su (*super-user*), sudo (*super-user do*), or a combination of these methods, ensures that permission elevation is secure.

Permission elevation is an option available with the configuration of SSH credentials. Configuring this option involves selecting a permission elevation method. Using sudo protects your administrator password and the integrity of the server by not requiring an administrative password. Using su requires the administrator password.

The option to elevate permissions appears when you create or edit SSH credentials in a site configuration:



Permission elevation

You can choose to elevate permissions using one of the following options:

- **su**- enables you to authenticate remotely using a non-root account without having to configure your systems for remote root access through a service such as SSH. To authenticate using su, enter the password of the user that you are trying to elevate permissions to. For example, if you are trying to elevate permissions to the root user, enter the password for the root user in the password field in *Permission Elevation* area of the *Shared Scan Credential Configuration* panel.
- **sudo**- enables you to authenticate remotely using a non-root account without having to configure your systems for remote root access through a service such as SSH. In addition, it enables system administrators to explicitly control what programs an authenticated user can run using the sudo command. To authenticate using sudo, enter the password of the user that you are trying to elevate permission from. For example, if you are trying to elevate permission to the root user and you logged in as jon_smith, enter the password for jon_smith in the password field in *Permission Elevatio*n area of the *Shared Scan Credential Configuration* panel.
- **sudo+su**- uses the combination of sudo and su together to gain information that requires privileged access from your target assets. When you log on, the application will use sudo authentication to run commands using su, without having to enter in the root password anywhere. The sudo+su option will not be able to access the required information if access to the su command is restricted.
- **pbrun**- uses BeyondTrust PowerBroker to allow Nexposeto run whitelisted commands as root on Unix and Linux scan targets. To use this feature, you need to configure certain settings on your scan targets. See the following section.

Configuring your scan environment to support pbrun permission elevation

Before you can elevate scan permissions with pbrun, you will need to create a configuration file and deploy it to each target host. The configuration provides the conditions that Nexpose needs to scan successfully using this method:

- Nexpose can execute the user's shell, as indicated by the $SHELL environment variable, with pbrun.
- pbrun does not require Nexpose to provide a password.
- pbrun runs the shell as root.

The following excerpt of a sample configuration file shows the settings that meet these conditions:

```
RootUsers = {"user_name" };

RootProgs = {"bash"};

if (pbclientmode == "run" &&

     user in RootUsers &&

     basename(command) in RootProgs) {


     # setup the user attribute of the delegated task

     runuser = "root";

     rungroup = "!g!";

     rungroups = {"!G!"};

     runcwd = "!~!";


     # setup the runtime environment of the delegated task

     setenv("SHELL", "!!!");

     setenv("HOME", "!~!");
```

```
        setenv("USER", runuser);

        setenv("USERNAME", runuser);

        setenv("LOGNAME", runuser);

        setenv("PWD", runcwd);

        setenv("PATH", "/bin:/usr/bin:/usr/local/bin:/sbin:/usr/sbin");


        # setup the log data

        CleanUp();


        accept;

}
```

Using system logs to track permission elevation

Administrators of target assets can control and track the activity of su and sudo users in system logs. When attempts at permission elevation fail, error messages appear in these logs so that administrators can address and correct errors and run the scans again.

Using LM/NTLM hash authentication

Nexpose can pass LM and NTLM hashes for authentication on target Windows or Linux CIFS/SMB services. With this method, known as “pass the hash,” it is unnecessary to “crack” the password hash to gain access to the service.

Several tools are available for extracting hashes from Windows servers. One solution is Metasploit, which allows automated retrieval of hashes. For information about Metasploit, go to www.rapid7.com.

When you have the hashes available, take the following steps:

If you want to add credentials while configuring a new site, click the **Create site** button on the *Home* page.

If you want to add credentials for an existing site, click that site's **Edit** icon in the *Sites* table on the *Home* page.

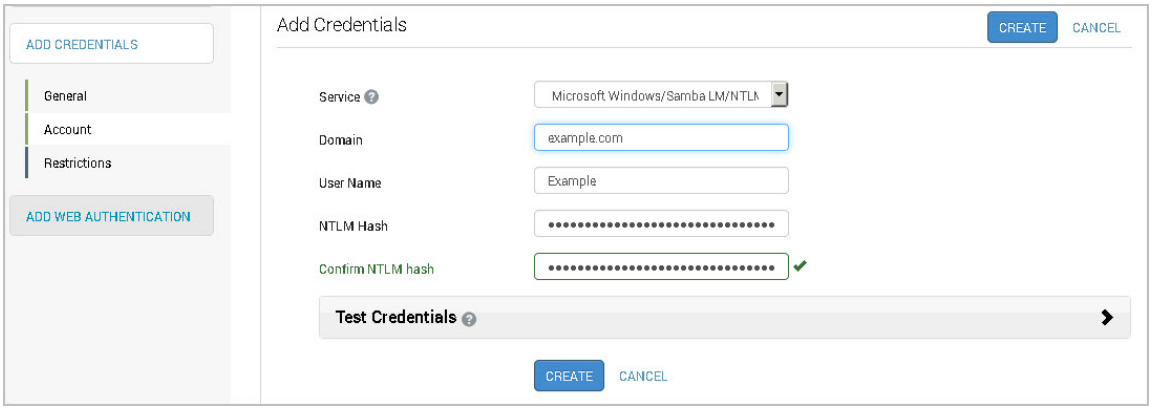
1. Select **Authentication**.
2. Click **Add Credentials**.
3. In the *Add Credentials* form, enter a name and description for a new set of credentials if necessary.
4. Click **Account** under *Add Credentials*.
5. Select *Microsoft Windows/Samba LM/NTLM Hash (SMB/CIFS)* from the **Service** drop-down list.
6. (Optional) Enter the appropriate domain.
7. Enter a user name.
8. Enter or paste in the LM hash followed by a colon (:) and then the NTLM hash. Make sure there are no spaces in the entry. The following example includes hashes for the password *test*:

```
01FC5A6BE7BC6929AAD3B435B51404EE:0CB6948805F797BF2A82807973B89537
```

9. Alternatively, using the NTLM hash alone is acceptable as most servers disregard the LM response:

```
0CB6948805F797BF2A82807973B89537
```

10. When you have finished configuring the credentials, click **Create** if it is a new set or **Save** if it is a previously created set.



NTLM hash

For additional optional steps, see the following topics:

- *Testing the credentials* on page 99
- *Limiting the credentials to a single asset and port* on page 100 *Limiting the credentials to a single asset and port*

Using PowerShell with your scans

Windows PowerShell is a command-line shell and scripting language that is designed for system administration and automation. As of PowerShell 2.0, you can use Windows Remote Management to run commands on one or more remote computers. By using PowerShell and Windows Remote Management with your scans, you can scan as though logged on locally to each machine. PowerShell support is essential to some policy checks in SCAP 1.2, and more efficiently returns data for some other checks.

In order to use Windows Remote Management with PowerShell, you must have it enabled on all the machines you will scan. If you have a large number of Windows assets to scan, it may be more efficient to enable it through group policy on your Windows domain.

For information on how to enable Windows Remote Management with PowerShell in a Windows domain, the following resources may be helpful:

- http://blogs.msdn.com/b/wmi/archive/2009/03/17/three-ways-to-configure-winrm-listeners.aspx
- http://www.briantist.com/how-to/powershell-remoting-group-policy/
- http://blogg.alltomdeployment.se/2013/02/howto-enable-powershell-remoteing-in-windows-domain/

Additionally, when using Windows Remote Management with PowerShell via HTTP, you need to allow unencrypted traffic.

To allow unencrypted traffic:

1. In Windows Group Policy Editor, go to:

   Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service

2. Select **Allow unencrypted traffic**.

3. Set the policy to *Enabled*.

   OR

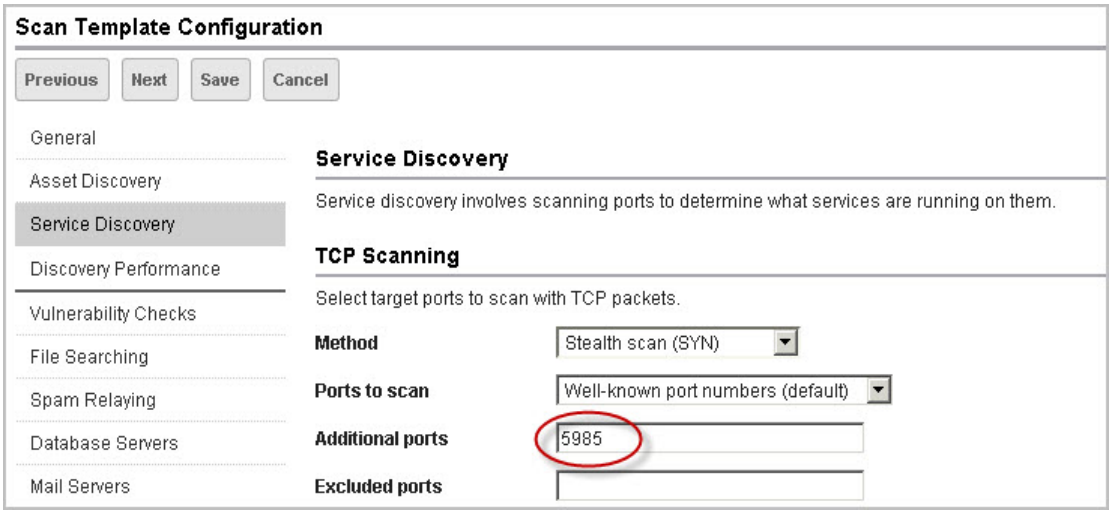
   From a command prompt, run:

   ```
   winrm set winrm/config/service @{AllowUnencrypted="true"}
   ```

For scans to use Windows Remote Management with PowerShell, port 5985 must be available to the scan template. The scan templates for DISA, CIS, and USGCB policies have this port included by default; for others you will need to add it manually.

To add the port to the scan template:

1. Go to the *Administration* page and select **Manage** in **Templates**.
2. Select the scan template you are using.
3. In the *Service Discovery* tab, add **5985** to the *Additional ports* in the *TCP Scanning* section.



Adding port 5985

You also need to specify the appropriate service and credentials.

To specify the service and credentials, take the following steps:

If you want to add credentials while configuring a new site, click the **Create site** button on the *Home* page.

If you want to add credentials for an existing site, click that site's **Edit** icon in the *Sites* table on the *Home* page.

1. Select **Authentication**.
2. Click **Add Credentials**.
3. In the *Add Credentials* form, enter a name and description for a new set of credentials if necessary.
4. Click **Account** under *Add Credentials*.
5. Select the **Microsoft Windows/Samba (SMB/CIFS)** service.
6. Enter the domain, user name, and password for the service.
7. When you have finished configuring the credentials, click **Create** if it is a new set or **Save** if it is a previously created set.

For additional optional steps, see the following topics:

- *Testing the credentials* on page 99
- *Limiting the credentials to a single asset and port* on page 100 *Limiting the credentials to a single asset and port*

The application will automatically use PowerShell if the correct port is enabled, and if the correct Microsoft Windows/Samba (SMB/CIFS) credentials are specified.

If you have PowerShell enabled, but don't want to use it for scanning, you may need to define a custom port list that does not include port 5985.

To disable access to the port:

1. Go to the *Administration* page and select **Manage** in **Templates**.
2. Select the scan template you are using.
3. In the *Service Discovery* tab, in *TCP Scanning*, for *Ports to Scan*, select **Custom (only use "Additional ports")**.
4. In **Additional ports**, specify a list of ports that does not include port 5985.

Authentication on Windows: best practices

When scanning Windows assets, we recommend that you use domain or local administrator accounts in order to get the most accurate assessment. Administrator accounts have the right level of access, including registry permissions, file-system permissions, and either the ability to connect remotely using Common Internet File System (CIFS) or Windows Management Instrumentation (WMI) read permissions. In general, the higher the level of permissions for the account used for scanning, the more exhaustive the results will be. If you do not have access, or want to limit the use of domain or local administrator accounts within the application, then you can use an account that has the following permissions:

- The account should be able to log on remotely and not be limited to Guest access.
- The account should be able to read the registry and file information related to installed software and operating system information.

Note: If you are not using administrator permissions then you will not be granted access to administrator shares and non-administrative shares will need to be created for read access to the file system for those shares.

Nexpose and the network environment should also be configured in the following ways:

- For scanning domain controllers, you must use a domain administrator account because local administrators do not exist on domain controllers.
- Make sure that no firewalls are blocking traffic from the Nexpose Scan Engine to port 135, either 139 or 445 (see note), and a random high port for WMI on the Windows endpoint. You can set the random high port range for WMI using WMI Group Policy Object (GPO) settings.

Note: Port 445 is preferred as it is more efficient and will continue to function when a name conflict exists on the Windows network.

- If using a domain administrator account for your scanning, make sure that the domain administrator is also a member of the local administrators group. Otherwise, domain administrators will get treated as non-administrative users. If domain administrators are not members of local administrators, they may have limited to no access, and also User Account Control (UAC) will block their access unless the next step is taken.
- If you are using a local administrator with UAC, you must add a DWORD registry key value `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy` and set the value to **1**. Make sure it is a DWORD and not a string.
- If running an antivirus tool on the Scan Engine host, make sure that antivirus whitelists the application and all traffic that the application is sending to the network and receiving from the network. Having antivirus inspecting the traffic can lead to performance issues and potential false-positives.
- Verify that the account being used can log on to one or more of the assets being assessed by using the Test Credentials feature in the application.
- If you are using CIFS, make sure that assets being scanned have Remote Registry service enabled. If you are using WMI, then the Remote Registry service is not required.

If your organization's policies restrict or prevent any of the listed configuration methods, or if you are not getting the results you expect, contact Technical Support.

Authentication on Unix and related targets: best practices

For scanning Unix and related systems such as Linux, it is possible to scan most vulnerabilities without root access. You will need root access for a few vulnerability checks, and for many policy checks. If you plan to scan with a non-root user, you need to make sure the account has specified permissions, and be aware that the non-root user will not find certain checks.The following sections contain guidelines for what to configure and what can only be found with root access. Due to the complexity of the checks and the fact they are updated frequently, this list is subject to change.

To ensure near-comprehensive vulnerability coverage when scanning as a non-root user, you need to either:

- Elevate permissions so that you can run commands as root without using an actual root account.

OR

- Configure your systems such that your non-root scanning user has permissions on specified commands and directories.

The following sections describe the configuration for these options.

Configuring your scan environment to support permission elevation

One way to elevate scan permissions without using a root user or performing a custom configuration is to use permission elevation, such as sudo or pbrun. These options require specific configuration (for instance, for pbrun, you need to whitelist the user's shell), but do not require you to customize permissions as described in *Commands the application runs* below. For more information on permission elevation, see *Authentication on Unix and related targets: best practices* on page 124.

Commands the application runs

The following section contains guidelines for what commands the application runs when scanning. The vast majority of these commands can be run without root. As indicated above, this list is subject to change as new checks are added.

The majority of the commands are required for one of the following:

- getting the version of the operating system
- getting the versions of installed software packages
- running policy checks implemented as shell scripts

Note: The application expects that the commands are part of the $PATH variable and there are no non-standard $PATH collisions.

The following commands are required for all Unix/Linux distributions:

- ifconfig
- java
- sha1
- sha1sum
- md5
- md5sum
- awk
- grep
- egrep
- cut
- id
- ls

Nexpose will attempt to scan certain files, and will be able to perform the corresponding checks if the user account has the appropriate access to those files. The following is a list of files or directories that the account needs to be able to access:

- /etc/group
- /etc/passwd
- grub.conf
- menu.lst
- lilo.conf
- syslog.conf
- /etc/permissions
- /etc/securetty
- /var/log/postgresql
- /etc/hosts.equiv
- .netrc
- '/', '/dev', '/sys', and '/proc' "/home" "/var" "/etc"
- /etc/master.passwd
- sshd_config

For Linux, the application needs to read the following files, if present, to determine the distribution:

- /etc/debian_release
- /etc/debian_version
- /etc/redhat-release
- /etc/redhat_version
- /etc/os-release
- /etc/SuSE-release
- /etc/fedora-release
- /etc/slackware-release
- /etc/slackware-version
- /etc/system-release
- /etc/mandrake-release
- /etc/yellowdog-release
- /etc/gentoo-release
- /etc/UnitedLinux-release
- /etc/vmware-release
- /etc/slp.reg
- /etc/oracle-release

On any Unix or related variants (such as Ubuntu or OS X), there are specific commands the account needs to be able to perform in order to run specific checks. These commands should be whitelisted for the account.

The account needs to be able to perform the following commands for certain checks:

- cat
- find

- mysqlaccess
- mysqlhotcopy
- sh
- sysctl
- dmidecode
- perlsuid
- apt-get
- rpm

For the following types of distributions, the account needs execute permissions as indicated.

Debian-based distributions (e.g. Ubuntu):

- uname
- dpkg
- egrep
- cut
- xargs

RPM-based distributions (e.g. Red Hat, SUSE, or Oracle):

- uname
- rpm
- chkconfig

Mac OS X:

- /usr/sbin/softwareupdate
- /usr/sbin/system_profiler
- sw_vers

Solaris:

- showrev
- pkginfo
- ndd

Blue Coat:

- show version

F5:

- either "version", "show", or "tmsh show sys version"

Juniper:

- uname
- show version

VMware ESX/ESXi:

- vmware -v
- rpm
- esxupdate -a query || esxupdate query

AIX:

- lslpp -cL to list packages
- oslevel

Cisco:

Required for vulnerability scanning:

- show version (**Note:** this is used on multiple Cisco platforms, including IOS, PIX, ASA, and IOR-XR)

Required for policy scanning:

- show running-config all
- show line
- show snmp community
- show snmp group
- show snmp user
- show clock
- show ip ssh
- show ip interface
- show cdp
- show tech-support password

FreeBSD:

- freebsd-version is needed to fingerprint FreeBSD versions 10 and later
- The user account needs permissions to execute cat /var/db/freebsd-update/tag on FreeBSD version earlier than 10.
- FreeBSD package fingerprinting requires:
  - pkg info
  - pkg_info

Vulnerability Checks that require RootExecutionService

For certain vulnerability checks, root access is required. If you choose to scan with a non-root user, be aware that these vulnerabilities will not be found, even if they exist on your system.The following is a list of checks that require root access:

Note: You can search for the Vulnerability ID in the search bar of the Security Console to find the description and other details.

Vulnerability Title	Vulnerability ID
Solaris Serial Login Prompts	solaris-serial-login-prompts
Solaris Loose Destination Multihoming	solaris-loose-dst-multihoming
Solaris Forward Source Routing Enabled	solaris-forward-source-route
Solaris Echo Multicast Reply Enabled	solaris-echo-multicast-reply
Solaris ICMP Redirect Errors Accepted	solaris-redirects-accepted
Solaris Reverse Source Routing Enabled	solaris-reverse-source-route
Solaris Forward Directed Broadcasts Enabled	solaris-forward-directed-broadcasts
Solaris Timestamp Broadcast Reply Enabled	solaris-timestamp-broadcast-reply
Solaris Echo Broadcast Reply Enabled	solaris-echo-broadcast-reply
Solaris Empty Passwords	solaris-empty-passwords
OpenSSH config allows SSHv1 protocol*	unix-check-openssh-ssh-version-two*
.rhosts files exist	unix-rhosts-file
Root's umask value is unsafe	unix-umask-unsafe
.netrc files exist	unix-netrc-files
MySQL mysqlhotcopy Temporary File Symlink Attack	unix-mysql-mysqlhotcopy-temp-file
Partition Mounting Weakness	unix-partition-mounting-weakness

* *OpenSSH config allows SSHv1 protocol/unix-check-openssh-ssh-version-two* is conceptually the same as another check, *SSH server supports SSH protocol v1 clients/ssh-v1-supported*, which does not require root.

Configuring scan authentication on target Web applications

Scanning Web applications at a granular level of detail is especially important, since publicly accessible Internet hosts are attractive targets for attack. By giving the scan inside access with authentication, you can inspect Web assets for critical vulnerabilities such as SQL injection and cross-site scripting.

Two authentication methods are available for Web applications:

- *Web site form authentication:* Many Web authentication applications challenge users to log on with forms. With this method, the Security Console retrieves a logon form from the Web application. You specify credentials in that form that the Web application will accept. Then, a Scan Engine submits those credentials to a Web site before scanning it. See *Creating a logon for Web site form authentication* on page 134.

  In some cases, it may not be possible to use a form. For example, a form may use a CAPTCHA test or a similar challenge that is designed to prevent logons by computer programs. Or, a form may use JavaScript, which is not supported for security reasons. If these circumstances apply to your Web application, you may be able to authenticate the application with the following method.

- *Web site session authentication:* The Scan Engine sends the target Web server an authentication request that includes an HTTP header—usually the session cookie header—from the logon page. See *Creating a logon for Web site session authentication with HTTP headers* on page 138

The authentication method you use depends on the Web server and authentication application you are using. It may involve some trial and error to determine which method works better. It is advisable to consult the developer of the Web site before using this feature.

Note: For HTTP servers that challenge users with Basic authentication or Integrated Windows authentication (NTLM), configure a set of scan credentials using the service called *Web Site HTTP Authentication*. To use this service, select **Add Credentials** and then **Account**in the *Authentication* tab of the site configuration. See *Configuring site-specific scan credentials* on page 97.

.

Creating a logon for Web site form authentication

Start the configuration for the HTML form authetication:

If you create a logon while configuring a new site, click the **Create site** button on the *Home* page.

If you want to create a logon for an existing site, click that site's **Edit** icon in the *Sites* table on the *Home* page.

1. Click the **Authentication** link in the Site Configuration.
2. Click **Add Web Authentication**.
3. In the *Add Web Application Authentication* form, select **Add HTML form** from the **Type** drop-down list.
4. Enter a name for the new HTML form logon settings.

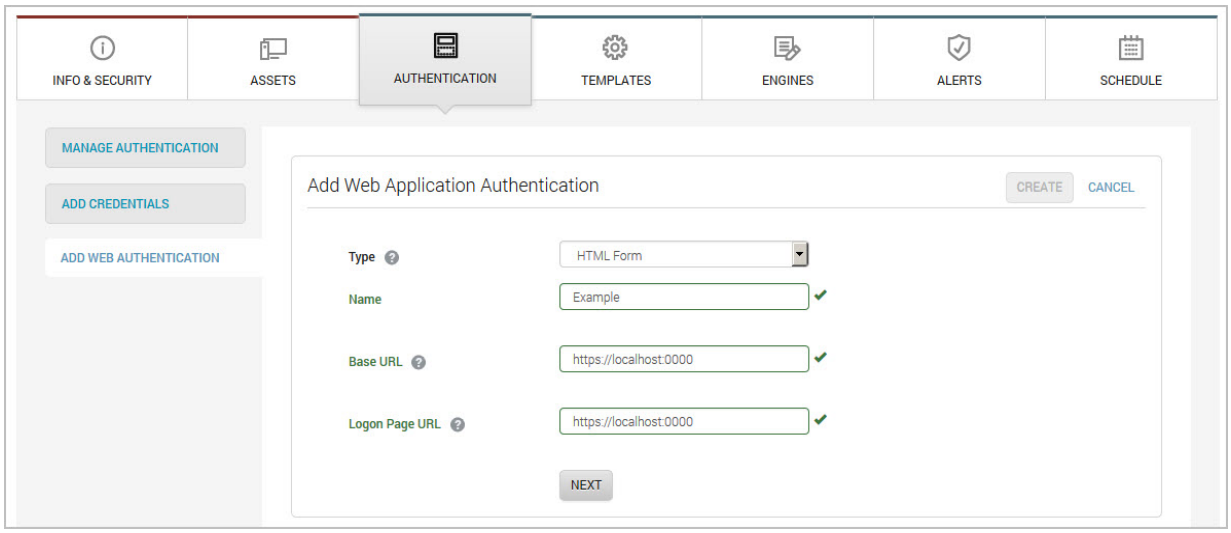
Tip: If you do not know any of the required information for configuring a Web form logon, consult the developer of the target Web site.

5. In the **Base URL** text box, enter the main address from which all paths in the target Web site begin.

   The credentials you enter for logging on to the site will apply to any page on the site, starting with the base URL. Include the protocol with the address. Example: http://example.com or https://example.com

6. In the **Logon Page URL** text box, enter the page that contains the form for logging onto the Web site. It should also include the protocol.

   Examples: http://example.com/logon.html



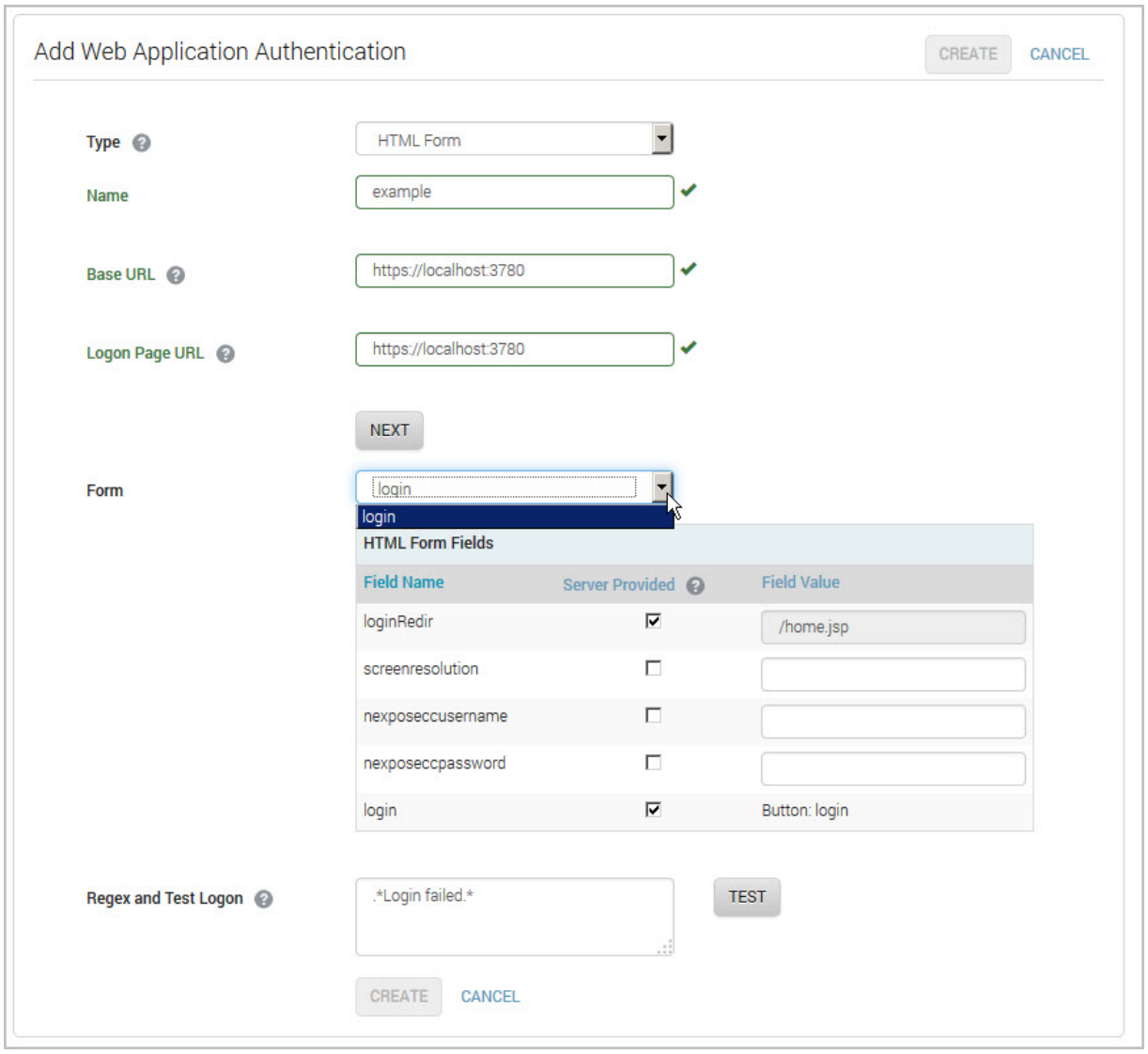
Entering Web application URLs

7. Click **Next**.

   The Security Console contacts the Web server to retrieve any available forms. If it fails to make contact or retrieve any forms, it displays a failure notification. If it retrieves forms, it displays additional configuration steps.

Customize the logon form (if necessary):

1. From the **Form** drop-down list, select the form for logging onto the Web application. Based on your selection, a table of fields appears for that particular form.



Editing the form

2. Change the value for any field if necessary.

Note: If the original value was provided by the Web server, you must first clear the check box before entering a new value. *Only* change the value to match what the server will accept at logon. If you are not certain of what value to use, contact your Web administrator.

3. Click **Save**.

   The Security Console displays the field table with any changed values according to your edits. Repeat the editing steps for any other values that you want to change.

When all the fields are configured according to your preferences, continue with creating a regular expression for logon failure and testing the logon:

1. Change the regular expression (regex) if you want to use one that is different from the default value.

   The default value works in most logon cases. If you are unsure of what regular expression to use, consult the Web administrator. For more information, see *Using regular expressions* on page 678.

2. Click **Test logon** to make sure that the Scan Engine can successfully log on to the Web application.

   If the Security Console displays a success notification, click **Save**.

   If logon failure occurs, change any settings as necessary and try again.

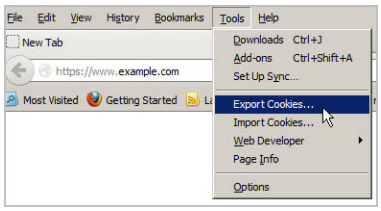
Tip: To find an appropriate regex, try logging onto the target Web site with incorrect credentials. If the site displays a message such as *Logon failed* or *Invalid credentials*, you can use that string for the regex.

Creating a logon for Web site session authentication with HTTP headers

When using HTTP headers to authenticate the Scan Engine, make sure that the session ID header is valid between the time you save this ID for the site and when you start the scan. For more information about the session ID header, consult your Web administrator.

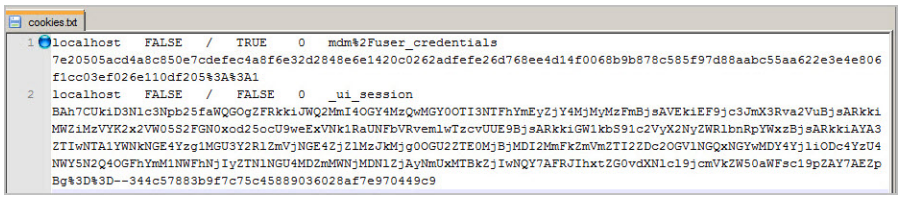
Not every Web site supports the storage of cookies, so it is helpful to verify that header authentication is possible on your target Web site before you use this method. Verification involves exporting the cookie values from the target Web site. Various tools are available for this task. For example, if you use Firefox as your browser, you can install the Cookie Exporter, Cookie Importer, and Firebug addons. The following steps incorporate Firefox as the browser for illustration:

1. After installing Cookie Exporter, Cookie Importer, and Firebug, restart Firefox and enable cookies.
2. Log onto the target Web site.
3. From the Firefox *Tools* menu, select **Export Cookies...** and save the exported cookies to a .txt file.



Exporting cookies from Firefox

4. Open the .txt file and delete all but the session cookies, since you'll need those for authentication. One header defines the credentials, and the other defines the session. Save the updated file.



The exported cookies file with all but the session cookies removed.

5. Restart the browser and clear your browser history.
6. From the Firefox *Tools* menu, select **Import Cookies...** Firefox displays a message indicating that two cookies were imported.
7. Navigate to the target Web site. If header authentication is possible, you will bypass the logon page, and you will immediately be authenticated.

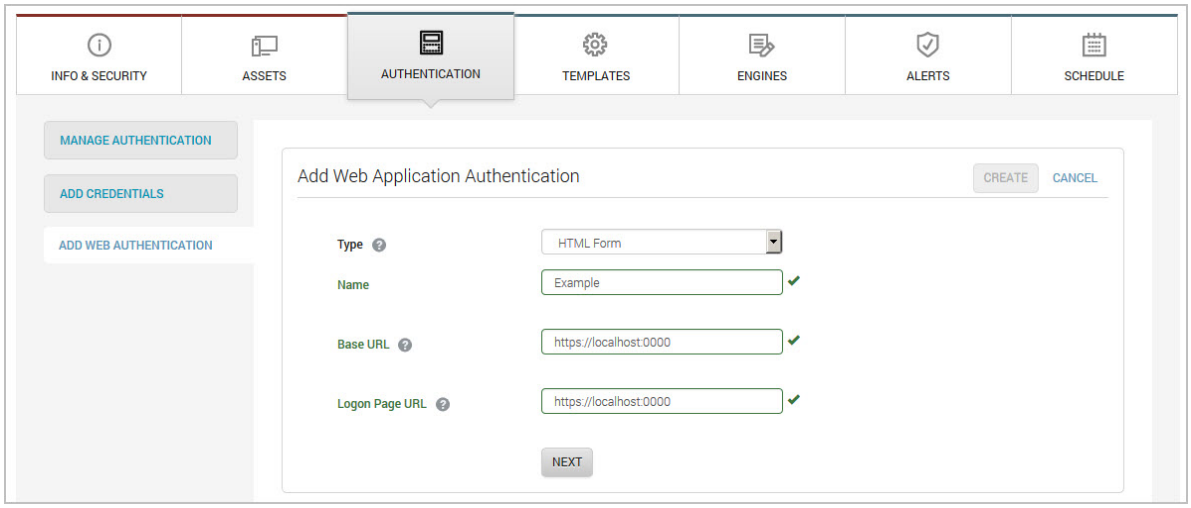
After verifying that header authentication is possible, start the HTTP headers configuration:

If you want to configure HTTP headers while configuring a new site, click the **Create site** button on the *Home* page.

If you want to configure HTTP headers for an existing site, click that site's **Edit** icon in the *Sites* table on the *Home* page.

1. Click the **Authentication** link in the site configuration .
2. Click **Add Web Authentication**.
3. In the *Add Web Application Authentication* form, select **HTTP Headers** from the **Type** drop-down list.
4. Enter a name for the new header settings.

5. In the **Base URL** text box, enter the main address from which all paths in the target Web site begin.



Web App URLs

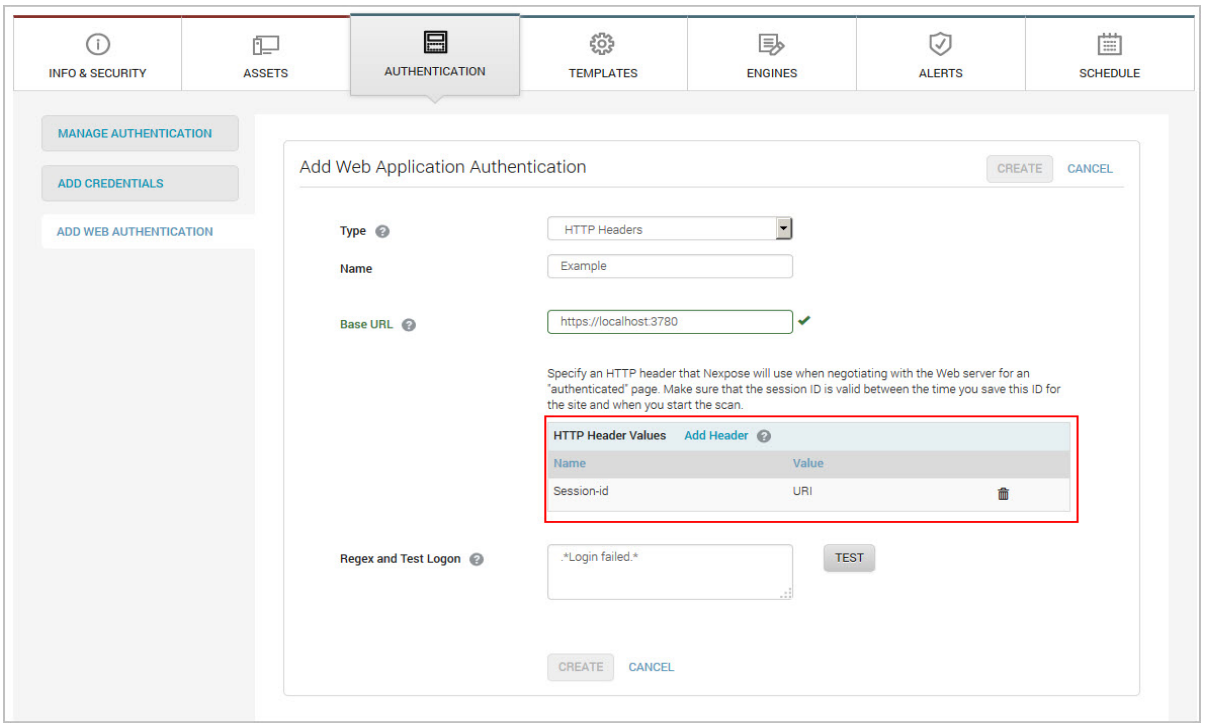
Continue with adding a header:

Tip: If you do not know any of the required information for configuring a Web form logon, consult the developer of the target Web site.

1. In the *HTTP Header Values* table, click the **Add Header** hyperlink.
2. In the pop-up dialog box, enter a name/value pair for the header and click the **Add Header** button.

- *Name* corresponds to a specific data type, such as the Web host name, Web server type, session identifier, or supported languages. The name can only include letters and numerals. It cannot include spaces or special characters.
- *Value* corresponds to the actual value string that the console sends to the server for that data type. For example, the value for a session ID (SID) might be a uniform resource identifier (URI).

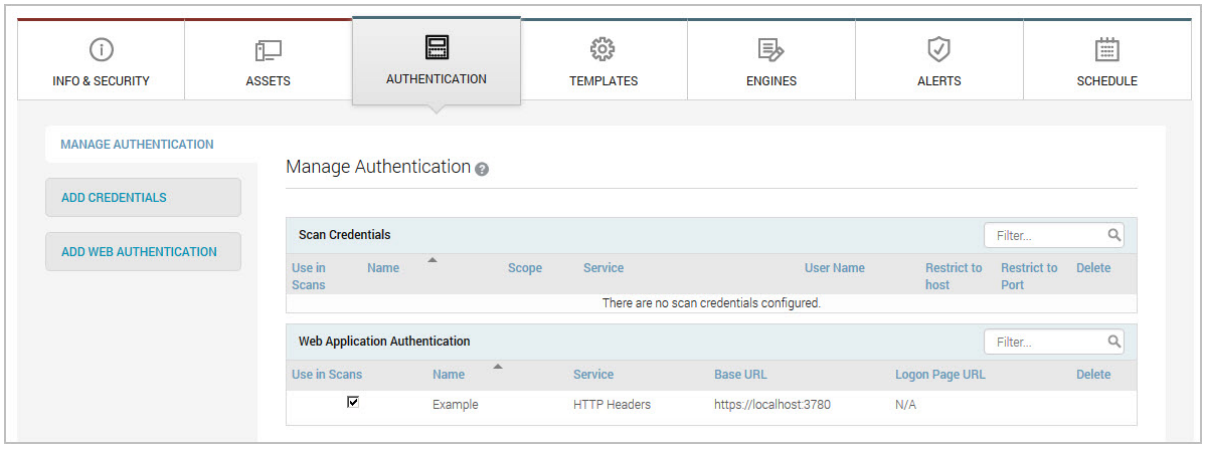
  For example, a name/value pair may specify a name/value pair for a session ID. The name might be *Session-id*, and the value might be *URI*.



Name/value pair

If you are not sure what header to use, consult your Web administrator.

After you enter the name/value pair, it appears in the *HTTP Header Values* table.



HTTP Header Values table

Continue with creating a regular expression for logon failure and testing the logon:

1. Change the regular expression (regex) if you want to use one that is different from the default value.

The default value works in most logon cases. If you are unsure of what regular expression to use, consult the Web administrator. For more information, see *Using regular expressions* on page 678.

2. Click **Test logon** to make sure that the Scan Engine can successfully log on to the Web application.

   If the Security Console displays a success notification, click **Save**.

   If logon failure occurs, change any settings as necessary and try again.

Setting up scan alerts

When a scan is in progress, you may want to know as soon as possible if certain things happen. For example, you may want to know when the scan finds a severe or critical vulnerability or if the scan stops unexpectedly. You can have the application alert you about scan events that are particularly important to you.

This feature is not a required part of the site configuration, but it's a convenient way to keep track of your scan when you don't have access to the Security Console Web interface or are simply not checking activity on the console.

Note: Alerts are sent in cleartext and are not encrypted.

If you want to add an alert for an existing site, click that site's **Edit** icon in the *Sites* table on the *Home* page.

If you want to add an alert while creating a new site, click the **Create site** button on the *Home* page.

To set up alerts:

1. Click the **Alerts** tab of the *Site Configuration*.
2. Click **Create alert**.

   The *New Alert* form appears.
3. The **Enable** check box is selected by default to ensure that an alert is generated. You can clear the check box at any time to disable the alert if you prefer not to receive that alert temporarily without having to delete it.
4. Enter a name for the alert.
5. Enter a value in the *Maximum Alerts to Send* field if you want to limit the number of this type of alert that you receive during the scan.
6. Select the check boxes for types of events that you want to generate alerts for.

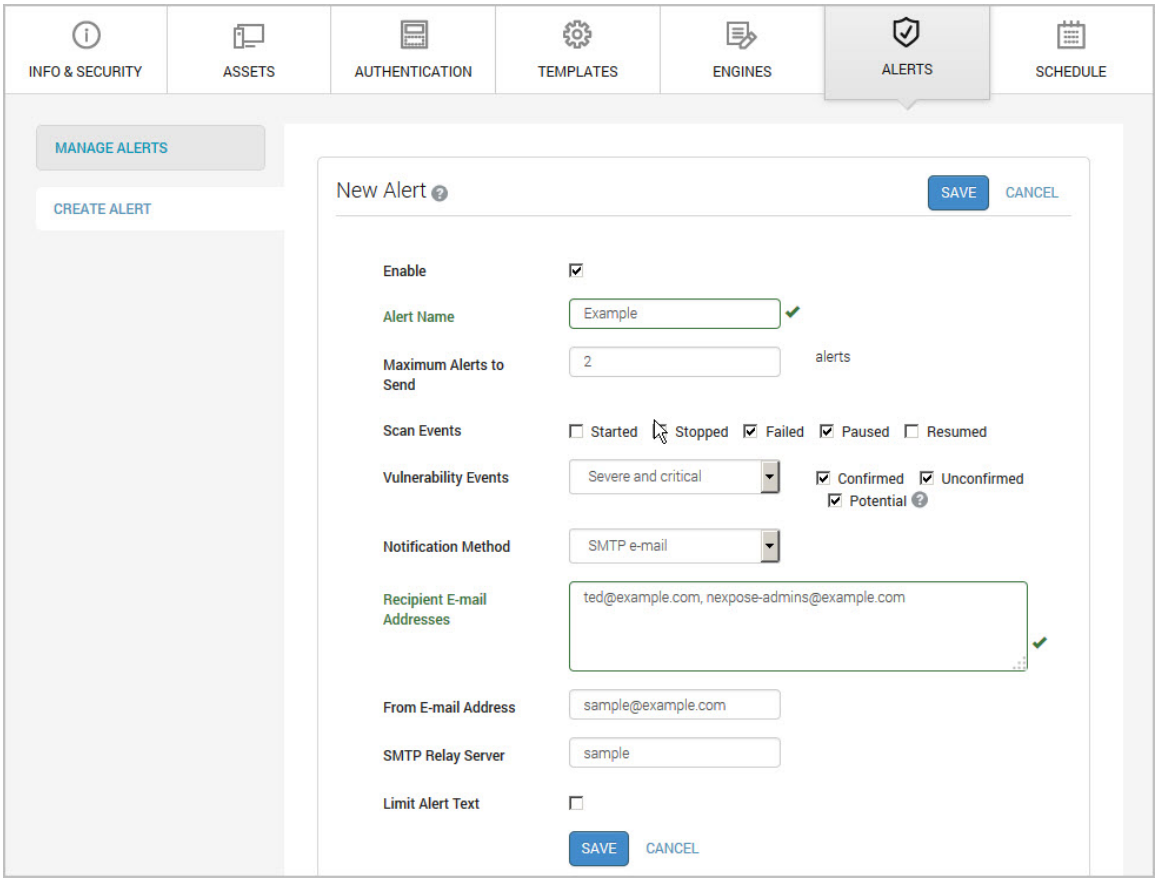
   For example, if you select **Paused** and **Resumed**, an alert is generated every time the application pauses or resumes a scan.

7. Select a severity level for vulnerabilities that you want to generate alerts for. For information about severity levels, see *Viewing active vulnerabilities* on page 265.

8. Select the **Confirmed**, **Unconfirmed**, and **Potential** check boxes to receive those alerts.

Note: If a vulnerability can be verified, a "confirmed" vulnerability is reported. If the system is unable to verify a vulnerability known to be associated with that asset, it reports an "unconfirmed" or "potential" vulnerability. The difference between these latter two classifications is the level of probability. Unconfirmed vulnerabilities are more likely to exist than potential ones, based on the asset's profile.

9. Select a notification method from the drop-down box. Alerts can be sent via SMTP e-mail, SNMP message, or Syslog message. Your selection will control which additional fields appear below this box.



Creating an alert

Scheduling scans

- *Best practices for scheduling scans* on page 145
- *Scheduling scans to run with different templates* on page 146
- *Steps for scheduling a scan* on page 147
- *Selecting a schedules for a site* on page 148

Depending on your security policies and routines, you may schedule certain scans to run on a monthly basis, such as patch verification checks, or on an annual basis, such as certain compliance checks. It's a good practice to run discovery scans and vulnerability checks more often—perhaps every week or two weeks, or even several times a week, depending on the importance or risk level of these assets.

Best practices for scheduling scans

Scheduling scans requires care. Generally, it's a good idea to scan during off-hours, when more bandwidth is free and work disruption is less likely. On the other hand, your workstations may automatically power down at night, or employees may take laptops home. In this case, you may need to scan those assets during office hours. Make sure to alert staff of an imminent scan, as it may tax network bandwidth or appear as an attack.

If you plan to run scans at night, find out if backup jobs are running, as these can eat up a lot of bandwidth.

Your primary consideration in scheduling a scan is the scan window: How long will the scan take?

Many factors can affect scan times:

- A scan with an Exhaustive template will take longer than one with a Full Audit template for the same number of assets. An Exhaustive template includes more ports in the scope of a scan.
- A scan with a high number of services to be discovered will take additional time.
- Checking for patch verification or policy compliance is time-intensive because of logon challenges on the target assets.
- A site with a high number of assets will take longer to scan.
- A site with more live assets will take longer to scan than a site with fewer live assets.
- Network latency and loading can lengthen scan times.
- Scanning Web sites presents a whole subset of variables. A big, complex directory structure or a high number of pages can take a lot of time.

If you schedule a scan to run on a repeating basis, note that a future scheduled scan job will not start until the preceding scheduled scan job has completed. If the preceding job has not completed by the time the next job is scheduled to start, an error message appears in the scan log. To verify that a scan has completed, view its status. See *Running a manual scan* on page 222.

Note: You cannot save a site configuration with overlapping schedules. Make sure any given scan time doesn't even partially conflict with that of another.

Scheduling scans to run with different templates

By alternating scan templates in a site, you can check the same set of assets for different needs. For example, you may schedule a recurring scan to run on a fairly routine basis with a template that is specifically tuned for the assets in a particular site. Then you can schedule a monthly scan to run with a special template for verifying Microsoft patches that have been applied after Patch Tuesday. Or you can schedule a monthly or quarterly scan with an internal PCI template to monitor compliance.

Steps for scheduling a scan

- If you want to set a schedule for an existing site, click that site's **Edit** icon in the *Sites* table on the *Home* page.
- If you want to set a schedule while creating a new site, click the **Create site** button on the *Home* page.

1. Click the **Schedules** tab of the *Site Configuration*.
2. Click **Create Schedule**.
3. Select the check box labeled **Enable schedule**.

   The Security Console displays options for a start date and time, maximum scan duration in minutes, and frequency of repetition.

4. Enter a start date in mm/dd/yyyy format.

   OR

   Select a date from the calendar that appears when you click inside the text box.

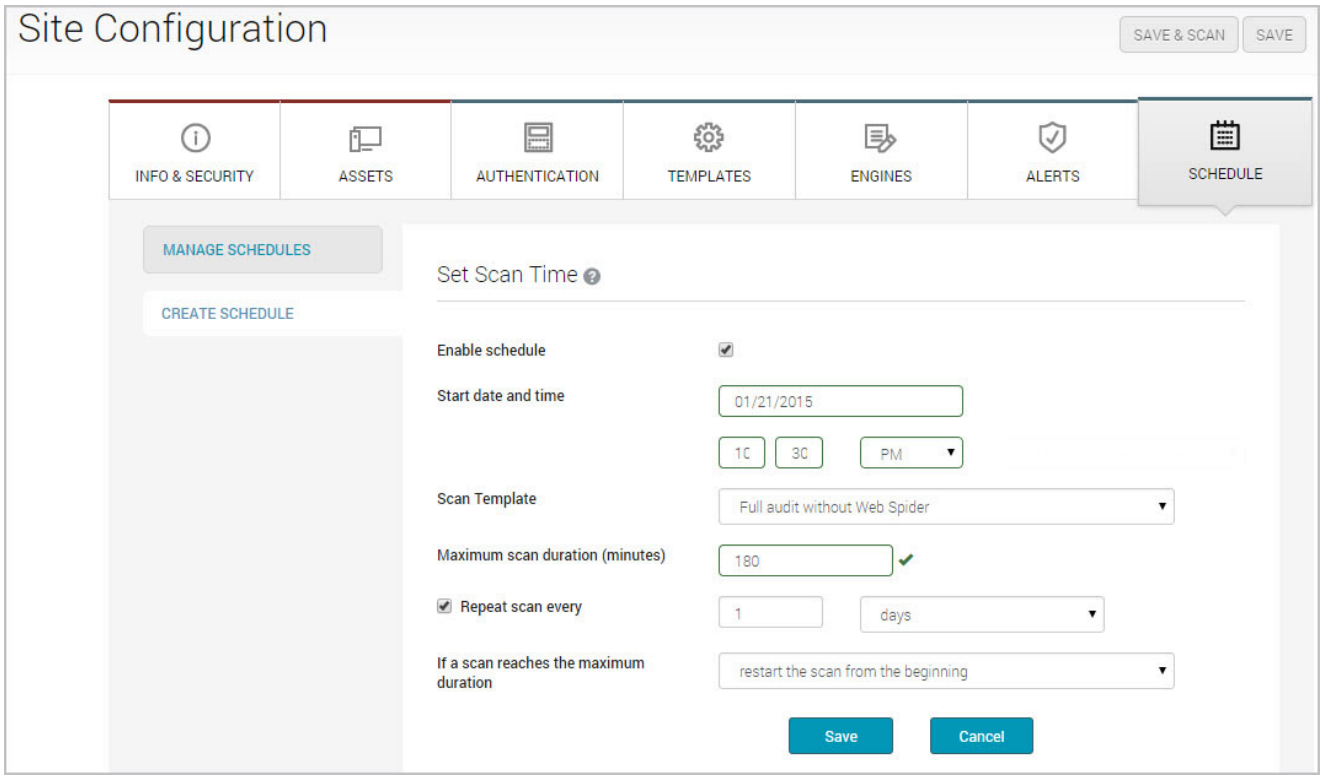
5. Enter a start time in HH:MM format, and select AM or PM.
6. Select a template for the scheduled scan. See *Scheduling scans to run with different templates* on page 146 for more information.

   Note: If you created the site through the integration with VMware NSX, you cannot you cannot use multiple scan templates because the Full Audit is automatically assigned as part of the integration process. See *Integrating NSX network virtualization with scans* on page 203.

7. If you want to set a maximum duration, enter a numeral for the number of minutes the scan can run. When the scan reaches the duration limit, it will pause. If you don't enter a value, the scan will simply run until it completes.
8. Select an option for what you want the scan to do after reaches the duration limit:

   If you select the option to continue where the scan left off, the paused scan will continue at the next scheduled start time.

   If you select the option to restart the paused scan from the beginning, the paused scan will stop and then start from the beginning at the next scheduled start time.



Scheduling a recurring scan

9. To make it a recurring scan, select the **Repeat scan every** check box. Select a number and time unit.
10. Click **Save**.

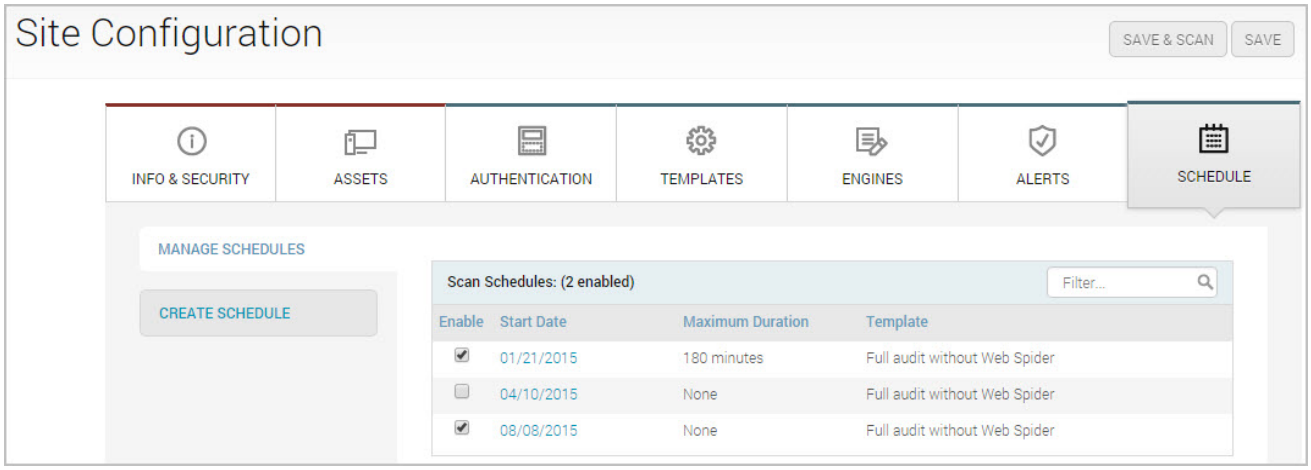
    The newly scheduled scan appears in the *Scan Schedules* table, which you can access by clicking **Manage Schedules**.

Tip: You can edit a schedule by clicking its hyperlink in the table.

Selecting a schedules for a site

You may want to suspend a scheduled scan. For example, a particular set of assets may be undergoing maintenance at a time when a scan is scheduled. You can enable and disable schedules as your needs dictate.

1. Click **Manage Schedules** in the *Schedules* tab of the *Site Configuration*.
2. Select a check box to enable a schedule, and clear a check box to disable it.
3. Configure any other site settings as desired.
4. Click **Save & Scan** or **Save** depending on your needs.



Enabling and disabling schedules

Scan blackouts

Scan blackouts allow you to prevent scans from taking place during specified times when you need to keep the network available for other traffic. For example, if your company makes extensive backups on Fridays, you could create a recurring blackout period from 9 am to 9 pm every Friday to prevent scans from running at that time.

There are two types of scan blackouts:

- **Global blackouts** apply throughout your Nexpose workspace. Global blackouts are created and managed from the *Administration* page. They can only be created and managed by Global Administrators.
- **Site-level blackouts** apply only for specific sites. They are created and managed from the *Site Configuration*. Site-level blackouts can be created and managed by Global Administrators or by Site Managers for that site.

During a blackout period, any scheduled scans will not start. If anyone tries to start a manual scan during a blackout period, they will see a message informing them of the blackout period. Global Administrators will have the option to scan anyway. Others will be unable to proceed with the scan.

If a scan is already in progress when a blackout period begins, the scan will be paused by the system for the duration of the blackout period. The scan will resume once the blackout period is over, in most cases. The exception is if a scheduled scan is paused by the system for a blackout and meets its maximum duration during the blackout period. In that case, the scan duration will take precedence and the blackout duration will not resume.

Note: Each scan takes approximately 30 seconds to shut down, and the scans shut down sequentially. There will be network activity at the beginning of the blackout period while the scans shut down. If you are creating a blackout period because you cannot have network activity during a certain time period, set the blackout to begin earlier to allow for all the scans to shut down.

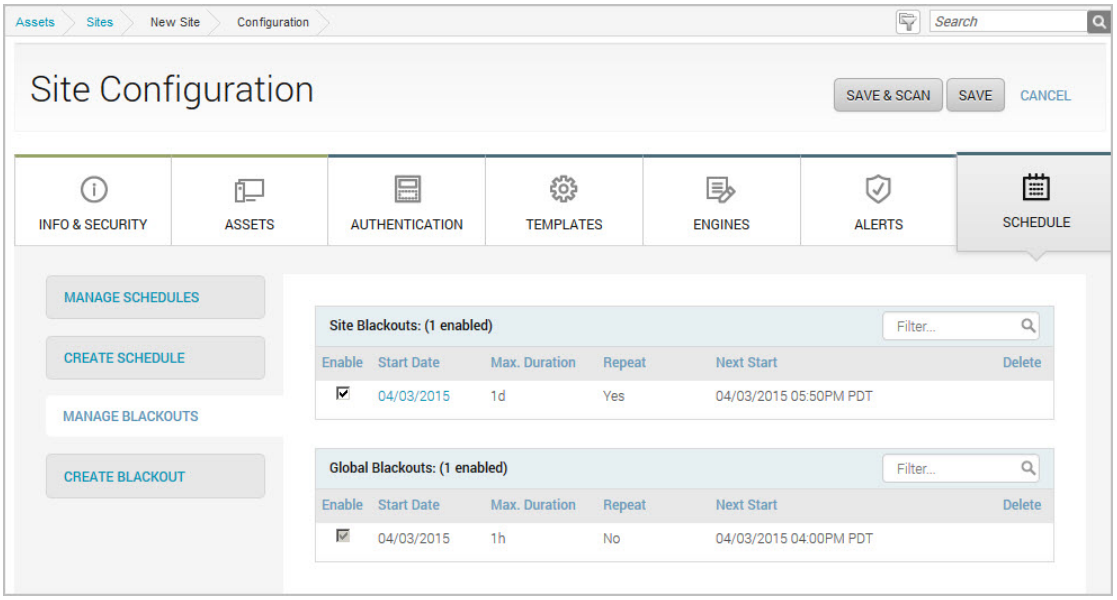
Creating a site-level blackout

As mentioned above, in order to create a site-level blackout, you must be a Site Manager for that site, or a Global Administrator.

Before creating a new site-level blackout, you may want to review the existing site-level and global blackouts that may apply to this site. Doing so will help you avoid creating overlapping or conflicting blackouts.

To review existing blackouts that may affect a site:

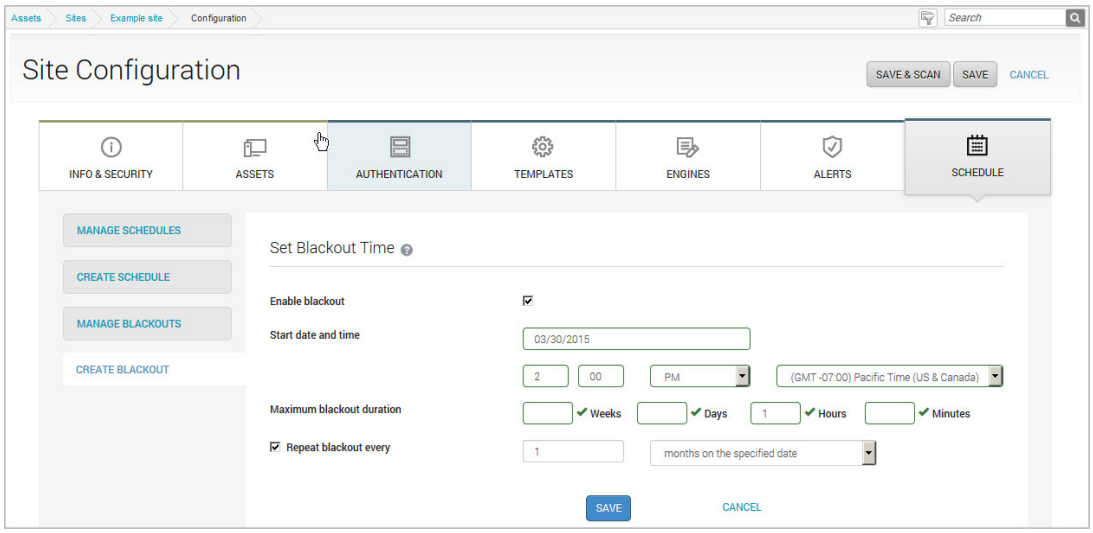
1. In the *Site Configuration*, go to the **Schedule** tab.
2. In the left navigation, select **Manage Blackouts**.
3. Review the existing blackout periods. The page shows both site-level and global blackouts.



Viewing existing blackouts that affect a site

To create a site-level blackout:

1. In the *Site Configuration*, go to the **Schedule** tab.
2. In the left navigation, select **Create Blackout**.
3. Specify the desired settings: Start date and time, maximum duration, whether to repeat the blackout, and, if so, a repetition schedule. Select or clear the **Enable blackout** checkbox to determine whether the blackout will take effect.
4. Click **Save** on the *Create Blackout* page.
5. Click **Save** on the *Site Configuration*.



Creating a site-level blackout

Managing site-level blackouts

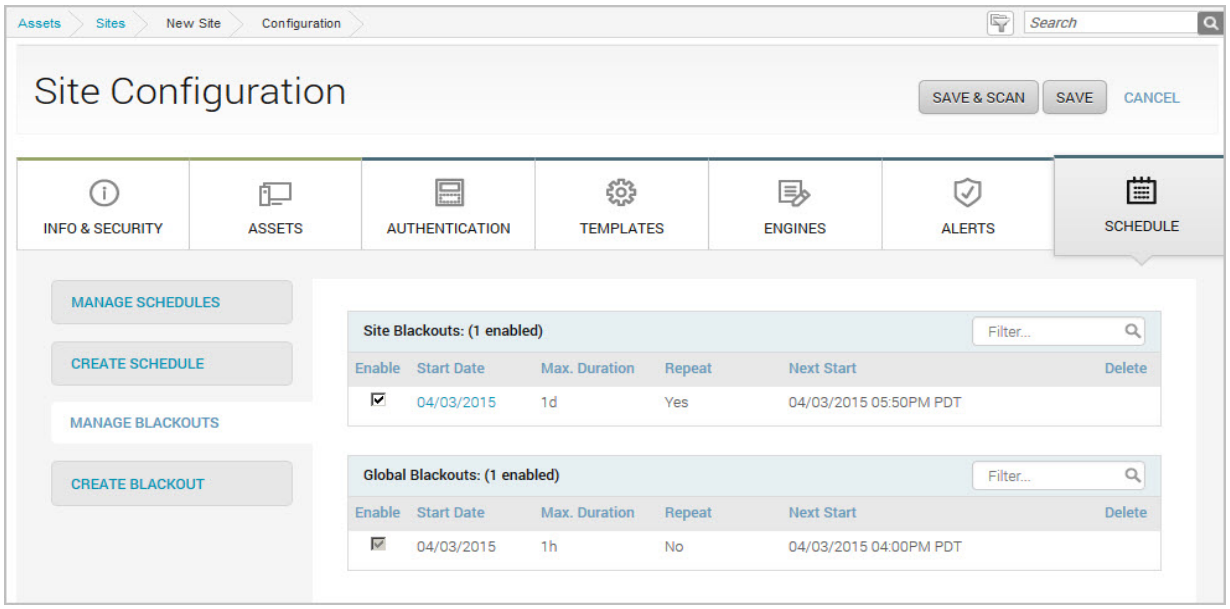
In the *Site Configuration*, Site Managers and Global Administrators can edit site-level blackouts and view global blackouts.

Note: If you modify a blackout that is currently in effect, it will be stopped and any running scans will resume.

To manage site-level blackouts:

1. In the *Site Configuration*, go to the **Schedule** tab.
2. In the left navigation, select **Manage Blackouts**.
3. You can view the list of site-level and global blackouts.

- To enable or disable a site-level blackout, select or clear the **Enable** check box. Global blackouts can only be edited on the **Administration** page by Global Administrators.
- To edit a site-level blackout, click the start date. Edit the settings. Click **Save** on the *Create Blackout* page and on the *Site Configuration*.



Managing site level blackouts

Creating a global blackout

Only Global Administrators can create global blackouts.

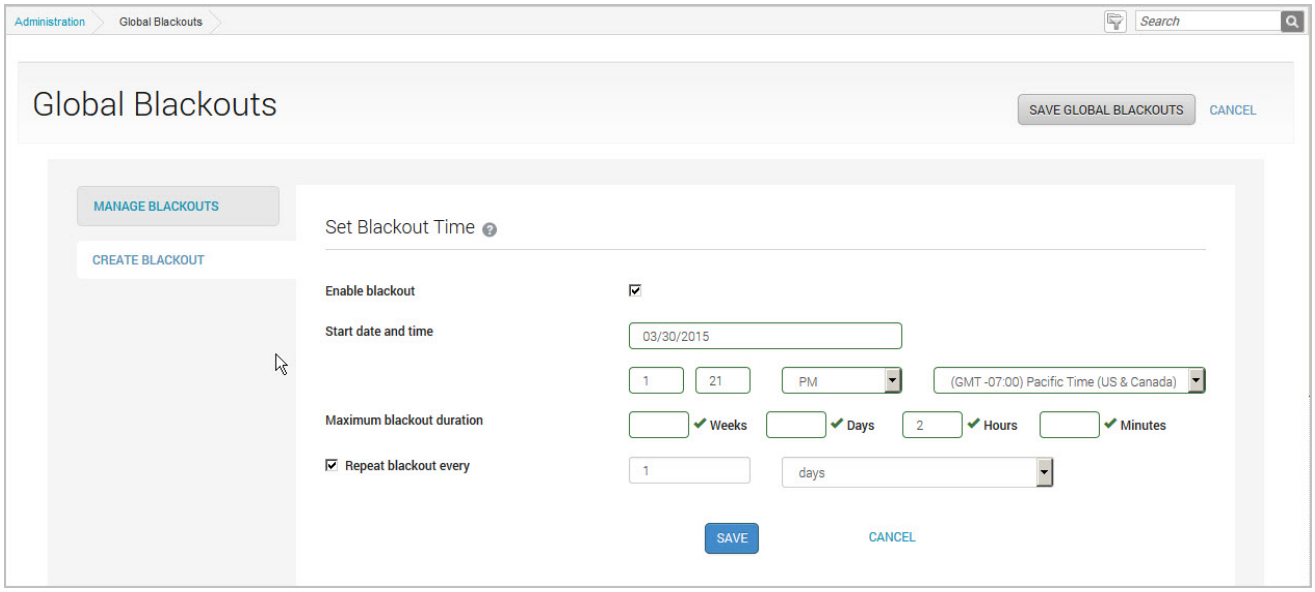
Before creating a global blackout, you may want to review the existing global blackouts in order to avoid creating a new one that overlaps or conflicts.

To review existing global blackouts:

1. Go to the *Administration* page.
2. In *Scan Options*, go to *Global Blackouts* and select **Manage**.
3. Review the existing global blackout periods.

To create a global blackout:

1. Go to the *Administration* page.
2. In *Scan Options*, next to *Global Blackouts*, select **Create**.
3. Specify the desired settings: Start date and time, maximum duration, whether to repeat the blackout, and, if so, a repetition schedule. Select or clear the **Enable blackout** checkbox to determine whether the blackout will take effect.
4. Click **Save** on the *Create Blackout* page.
5. Click **Save Global Blackouts**.



Creating a global blackout

Managing global blackouts

Only Global Administrators can manage global blackouts.

Note: If you modify a blackout that is currently in effect, it will be stopped and any running scans will resume.

To manage existing global blackouts:

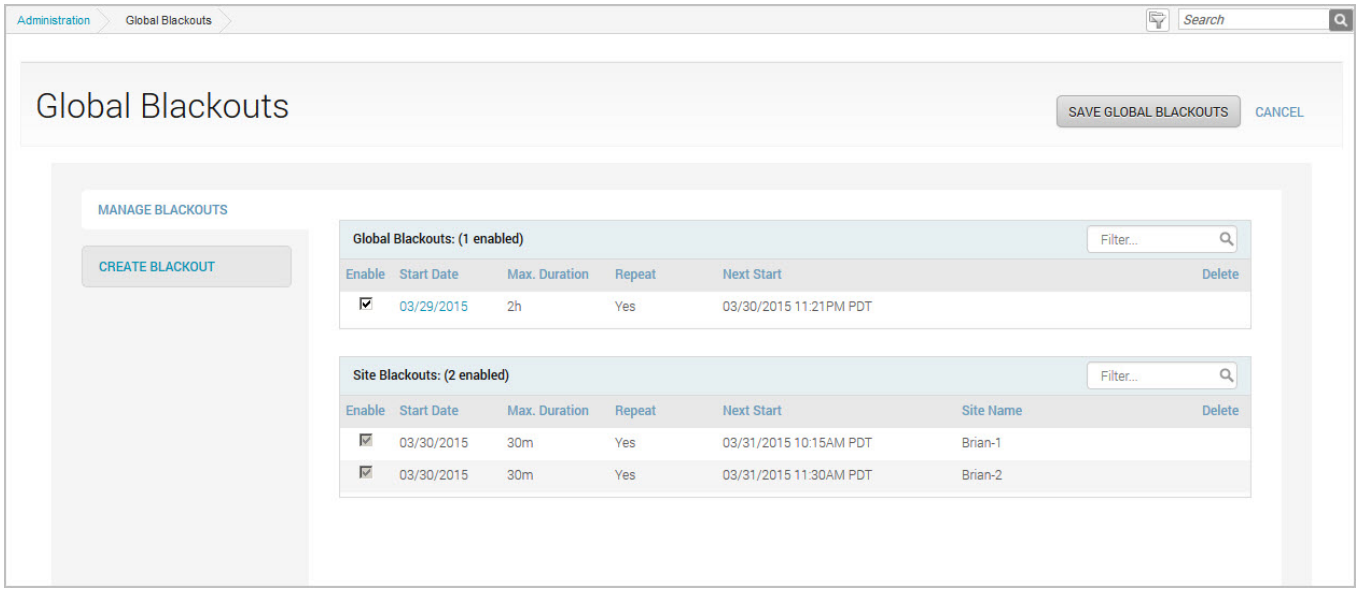
1. Go to the *Administration* page.
2. In *Scan Options*, go to *Global Blackouts* and select **Manage**.
3. Review the existing global blackout periods.

To enable or disable a global blackout:

1. Select or clear the **Enable** check box.
2. Site blackouts can be administered from the *Scan Configuration* for that site.

To edit a global blackout:

1. Click the start date for the blackout you want to edit.
2. Edit the desired settings: Start date and time, maximum duration, whether to repeat the blackout, and, if so, a repetition schedule. Select or clear the **Enable blackout** checkbox to determine whether the blackout will take effect.
3. Click **Save** on the *Manage Blackouts* page.
4. Click **Save Global Blackouts**.



Managing global blackouts

Deleting sites

To manage disk space and ensure data integrity of scan results, administrators can delete unused sites. By removing unused sites, inactive results do not distort scan results and risk posture in reports. In addition, unused sites count against your license and can prevent the addition of new sites. Regular site maintenance helps to manage your license so that you can create new sites.

Note: To delete a site, you must have access to the site and have *Manage Sites* permission. The **Delete** button is hidden if you do not have permission.

To delete a site:

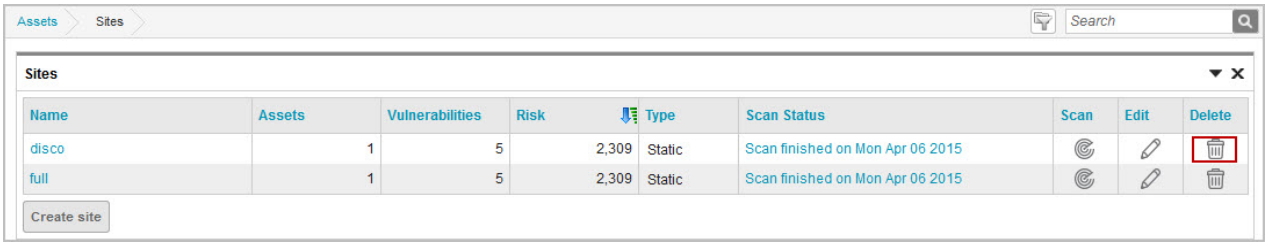
1. Access the *Sites* panel:

- Click the **Assets** tab and then click on the number of sites at the top.

Note: You cannot delete a site that is being scanned. You receive this message “Scans are still in progress. If you want to delete this site, stop all scans first”.

The *Sites* panel displays the sites that you can access based on your permissions.

2. Click the **Delete** button to remove a site.



Deleting a s site from the Sites panel

All reports, scan templates, and scan engines are disassociated. Scan results are deleted.

If the delete process is interrupted then partially deleted sites will be automatically cleared.

Managing dynamic discovery of assets

- *What is Dynamic Discovery, and why use it?* on page 157
- *Verifying that your license enables relevant features* on page 158
- *Discovering mobile devices* on page 159
- *Discovering Amazon Web Services instances* on page 164
- *Discovering assets through DHCP log queries* on page 169
- *Discovering virtual machines managed by VMware vCenter or ESX/ESXi* on page 167

What is Dynamic Discovery, and why use it?

It may not be unusual for your organization's assets to fluctuate in number, type, and state, on a fairly regular basis. As staff numbers grow or recede, so does the number of workstations. Servers go on line and out of commission. Employees who are traveling or working from home plug into the network at various times using virtual private networks (VPNs).

This fluidity underscores the importance of having a dynamic asset inventory. Relying on a manually maintained spreadsheet is risky. There will always be assets on the network that are not on the list. And, if they're not on the list, they're not being managed. Result: added risk.

One way to manage a "dynamic inventory," is to run discovery scans on a regular basis. See *Configuring asset discovery* on page 588. This approach is limited in that each scan provides a snapshot of your asset inventory at the time of the scan. Another approach, Dynamic Discovery, allows you to discover and track assets without running a scan. It involves initiating a connection with a server or API that manages an asset environment, such as one for virtual machines, and then receiving periodic updates about changes in that environment. This approach has several benefits:

- As long as the discovery connection is active, the application periodically discovers assets "in the background," without manual intervention on your part.
- You can create dynamic sites that update automatically based on dynamic asset discovery. See *Configuring a dynamic site* on page 200. Whenever you scan these sites, you are scanning the most current set of assets.
- You can concentrate scanning resources for vulnerability checks instead of running discovery scans.

Verifying that your license enables relevant features

For connections to Amazon Web Services, DHCP log servers, and VMware servers, your Nexpose must enable the Dynamic Discovery option.

For ActiveSync connections that allow you to discover mobile devices, your license must enable the Mobile option.

To verify that your license enables Virtual Discovery:

1. Click the **Administration** tab.

   The Security Console displays the *Administration* page.

2. Click the **Manage** link for *Security Console*.

   The Security Console displays the *Security Console Configuration* panel.

3. Click the **Licensing** link.

   The Security Console displays the *Licensing* page.

4. See if the *Dynamic Discovery* or *Mobile* feature is checked, depending on your needs.

Discovering mobile devices

- *Preparing for Dynamic Discovery of mobile devices* on page 160
- *Creating and managing Dynamic Discovery connections* on page 170
- *Initiating Dynamic Discovery* on page 183
- *Using filters to refine Dynamic Discovery* on page 186
- *Configuring a dynamic site* on page 200

An increasing number of users are connecting their personal mobile devices to corporate networks. These devices increase and expand attack surfaces in your environment with vulnerabilities that allow attackers to bypass security restrictions and perform unauthorized actions or execute arbitrary code.

You can discover devices with Apple iOS or Google Android operating systems that are connected to Microsoft Exchange over ActiveSync. All versions of iOS and Android are supported.

The Security Console discovers mobile devices that are managed with Microsoft Exchange ActiveSync protocol. The Dynamic Discovery feature currently supports Exchange versions 2010 and 2013 and Office 365.

You can connect to the mobile data via one of three Microsoft Windows server configurations:

- a connection to an Exchange server via LDAP/Active Directory (AD)
- a Windows Remote Management (WinRM) gateway connecting to an on-premise Exchange server via the PowerShell framework
- a WinRM gateway connecting to a Cloud-based Office 365 server

The advantage of using one of the WinRM configurations is that asset data discovered through one of these methods includes the most recent time that each mobile device was synchronized with the Exchange server. This can be useful if you do not want your reports to include data from old devices that are no longer in use on the network. You can create a dynamic asset group for mobile devices with old devices filtered out. See *Performing filtered asset searches* on page 324.

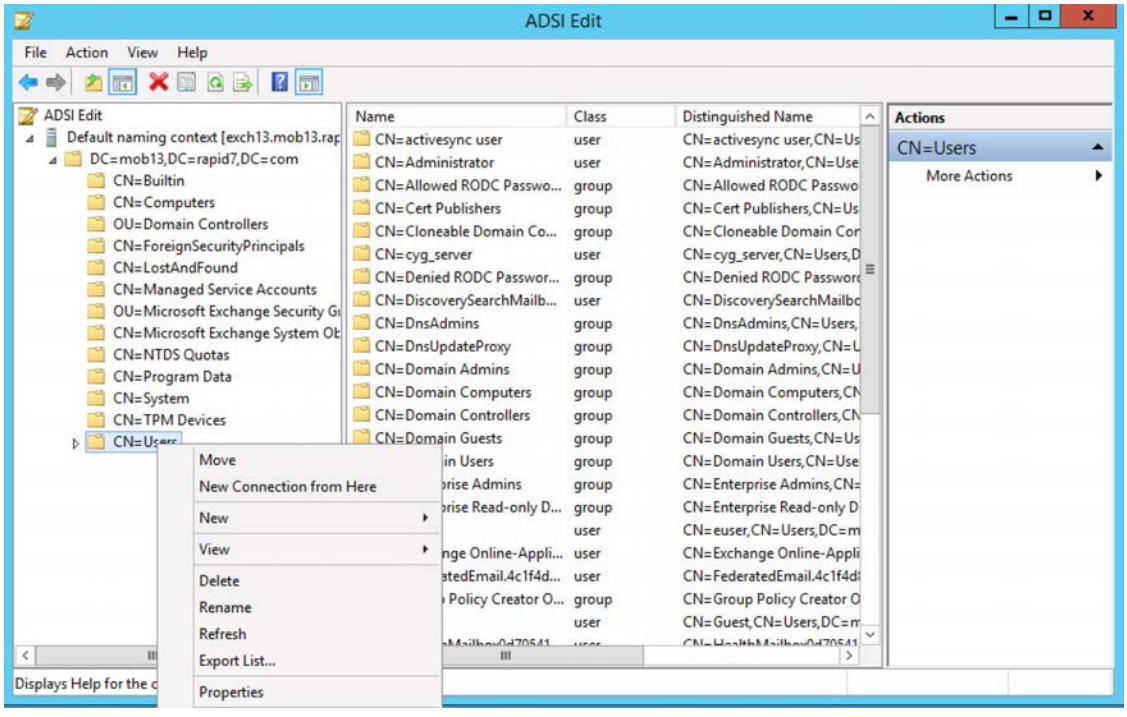
Preparing for Dynamic Discovery of mobile devices

Depending on which Windows server configuration you are using, you will need to take some preliminary steps to prepare your target environment for discovery.

LDAP/AD

For the discovery connection, the Security Console requires credentials for a user with read permission on the mobile device objects in Active Directory. The user must be a member of the Organization Management Security Group in Microsoft Exchange or a user that has been granted read access to the mobile device objects.This allows the Security Console to perform LDAP queries.

Take the following steps on the AD server to grant account Read-only permissions to the AD Organizational Unit(s) (OU) that contain users with ActiveSync (Mobile) devices:



Selecting the Users OU in ADSI Edit

1. Start the Active Directory Service Interfaces Editor (ADSI Edit) and connect to the AD environment.
2. Select the OU that contains users with ActiveSync (Mobile) devices. In this example, the Users OU contains users with ActiveSync devices.
3. Right-click the Users OU and select **Properties**.
4. Select the **Security** tab.
5. Click the **Add** button and add the user account that the Security Console will use for connecting to the AD server.
6. Select the user and click **Advanced**.
7. Select the user and click **Edit** .
8. From the **Applies to** drop-down list, select *Descendant msExchActiveSyncDevice objects*.

Repeat the previous steps for any additional OUs containing ActiveSync (Mobile) devices.

WinRM

The setup requirements and steps in the target environment are practically identical for PowerShell and Office 365 configurations:

Servers and credentials

- WinRM gateway server with a user account that has WinRM permissions
- Exchange server with an administrator account or a user account that has View-Only Organizational Management or higher role

Note: The WinRM gateway may also be the Exchange server or Nexpose, if the Security Console is running on Windows.

Setting up the WinRM gateway

Note: Consult a Windows server administrator if you are unfamiliar with these procedures.

The WinRM gateway must have an available https WinRM listener at port 5986. Typical steps to enable this include the following:

1. Verify that the server has a Server Authentication certificate installed that is not expired or self-signed. For more information, see https://technet.microsoft.com/en-us/library/cc731183.aspx .
2. Enable the WinRM https listener:

```
C:\> winrm quickconfig -transport:https
```

3. Increase the WinRM memory limit with a PowerShell command (Minimum setting is 1024 MB; but 2048 MB is recommended.):

```
[PS] C:\> set-item wsman:localhost\Shell\MaxMemoryPerShellMB 2048
```

4. Open port 5986 on the Windows firewall:

```
C:\> netsh advfirewall firewall add rule name=
"Windows Remote Management (HTTPS-In)" dir=in action=allow protocol=TCP
localport=5986
```

The following instructions are available for enabling WinRM for an account other than administrator: http://docs.scriptrock.com/kb/using-winrm-without-admin-rights.html

Network connectivity

- The Security Console must be able to connect to the WinRM gateway via port 5986 over https or WS-Management protocol.
- The WinRM gateway must be able to connect to the Exchange server over port 80 and perform necessary kerberos authentication.

Troubleshooting WinRM connection issues

If WinRM fails using a domain controller as WinRM gateway, see the blog at http://www.projectleadership.net/blogs_details.php?id=3154 for assistance. Typically, running `setspn -L [server_name]` returns two WinRM configurations; but, in this case, none are displayed.

If the PowerShell script fails with error *Process is terminated due to StackOverflowException.*, the WinRM memory limit is insufficient. Increase the setting by running the PowerShell command:

```
[PS] C:\> set-item wsman:localhost\Shell\MaxMemoryPerShellMB 2048
```

Troubleshooting Exchange connectivity

To verify and troubleshoot Exchange connectivty, open the PowerShell Windows WinRM gateway server with the WinRM credentials. Then run the following Powershell command with your Exchange user credentials and the Exchange server fully qualified domain name for your organization:

```
$cred = Get-Credential
$s = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
http://exchangeserver.domain.com/ -credential $cred
Import-PSSession $s
Get-ActiveSyncDevice
```

This will display a window to enter the credentials. If the *New-PSSession* fails this indicates that the remote PowerShell connection to the Exchange server failed.

If the *Get-ActiveSyncDevices* command returns *not devices*, this may indicate that your Exchange account has insufficient permission to perform the query.

Troubleshooting connections with the Office 365 configuration

The Office 365 configuration works exactly like the PowerShell configuration, except that it communicates with Microsoft's Exchange server in the Cloud and connects to the gateway somewhat differently via PowerShell.

Use the following script to troubleshoot Office365 exchange connectivity:

```
$cred = Get-Credential
$s = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
https://outlook.office365.com/powershell -credential $cred -
Authentication Basic -AllowRedirection
Import-PSSession $s
Get-ActiveSyncDevice
```

After preparing your network for discovery, see *Creating and managing Dynamic Discovery connections* on page 170.

General best practices for managing mobile discovery

To optimize discovery results on a continuing basis, observe some best practices for managing your environment:

Test your environment

Test your ActiveSync environment to verify all components are working and communicating properly. This will help improve your coverage.

Create device access rules

Creating rules for ActiveSync devices in your network further expands your control. You can, for example, create rules for approving quarantined devices.

Manage and increase device partnerships

Individual users in your organization may use multiple devices, each with its own partnership or set of ActiveSync attributes created during the initial synchronization. Additionally, users routinely upgrade from one version of a device to another, which also increases the potential number of partnerships to support. Managing these partnerships is important for tracking ActiveSync devices in your environment. It involves the removal of old devices from the Exchange server, which can help create a more accurate mobile risk assessment.

Discovering Amazon Web Services instances

- *Preparing for Dynamic Discovery in an AWS environment* on page 165
- *Creating and managing Dynamic Discovery connections* on page 170
- *Initiating Dynamic Discovery* on page 183
- *Using filters to refine Dynamic Discovery* on page 186
- *Configuring a dynamic site* on page 200

If your organization uses Amazon Web Services (AWS) for computing, storage, or other operations, Amazon may occasionally move your applications and data to different hosts. By initiating Dynamic Discovery of AWS instances and setting up dynamic sites, you can scan and report on these instances on a continual basis. The connection occurs via the AWS API.

In the AWS context, an *instance* is a copy of an Amazon Machine Image running as a virtual server in the AWS cloud. The scan process correlates assets based on instance IDs. If you terminate an instance and later recreate it from the same image, it will have a new instance ID. That means that if you scan a recreated instance, the scan data will not be correlated with that of the preceding incarnation of that instance. The results will be two separate instances in the scan results.

Preparing for Dynamic Discovery in an AWS environment

Before you initiate Dynamic Discovery and start scanning in an AWS environment, you need to:

- be aware of how your deployment of Nexpose components affects the way Dynamic Discovery works
- create an AWS IAM user or IAM role
- create an AWS policy for your IAM user or IAM role

Inside or outside the AWS network?

In configuring an AWS discovery connection, it is helpful to note some deployment and scanning considerations for AWS environments.

It is a best practice to scan AWS instances with a distributed Scan Engine that is deployed within the AWS network, also known as the Elastic Compute Cloud (EC2) network. This allows you to scan private IP addresses and collect information that may not be available with public IP addresses, such as internal databases. If you scan the AWS network with a Scan Engine deployed inside your own network, and if any assets in the AWS network have IP addresses identical to assets inside your own network, the scan will produce information about assets in your own network with the matching addresses, not the AWS instances.

Note: The AWS network is behind a firewall, as are the individual instances or assets in the network, so there are two firewalls to negotiate for AWS scans.

If the Security Console and Scan Engine that will be used for scanning AWS instances are located outside of the AWS network, you will only be able to scan EC2 instances with Elastic IP (EIP) addresses assigned to them. Also, you will not be able to manually edit the asset list in your site configuration or in a manual scan window. Dynamic Discovery will include instances without EIP addresses, but they will not appear in the asset list for the site configuration. Learn more about EIP addresses.

The location of the Security Console relative to the AWS network will affect how you identify it as a trusted entity in the AWS network. See the following two topics.

Outside the network: Creating an IAM user

If your Security Console is located outside the AWS network, the AWS Application Programming Interface (API) must be able to recognize it as a trusted entity before allowing it to connect and discover AWS instances. To make this possible, you will need to create IAM user, which is an AWS identity for the Security Console, with permissions that support Dynamic Discovery. When

you create an IAM user, you will also create an access key that the Security Console will use to log onto the API.

Learn about IAM users and how to create them.

Note: When you create an IAM user, make sure to select the option to create an access key ID and secret access key. You will need these credentials when setting up the discovery connection. You will have the option to download these credentials. Be careful to download them in a safe, secure location.

Note: When you create an IAM user, make sure to select the option to create a custom policy.

Inside the network: Creating an IAM role

If your Security Console is installed on an AWS instance and, therefore, inside the AWS network, you need to create an IAM role for that instance. A role is simply a set of permissions. You will not need to create an IAM user or access key for the Security Console.

Learn about IAM users and how to create them.

Note: When you create an IAM role, make sure to select the option to create a custom policy.

Creating a custom policy for your IAM user or role

When creating an IAM user or role, you will have to apply a policy to it. A policy defines your permissions within the AWS environment. Amazon requires your AWS policy to include minimal permissions for security reasons. To meet this requirement, select the option create a custom policy.

You can create the policy in JSON format using the editor in the AWS Management Console. The following code sample indicates how the policy should be defined:

```
{
"Version": "2012-10-17",
"Statement": [
{ "Sid": "Stmt1402346553000", "Effect": "Allow", "Action":
[ "ec2:DescribeInstances", "ec2:DescribeImages",
"ec2:DescribeAddresses" ], "Resource": [ "*" ] }
]
}
```

Discovering virtual machines managed by VMware vCenter or ESX/ESXi

- *Preparing the target VMware environment for Dynamic Discovery* on page 167
- *Creating and managing Dynamic Discovery connections* on page 170
- *Initiating Dynamic Discovery* on page 183
- *Using filters to refine Dynamic Discovery* on page 186
- *Configuring a dynamic site* on page 200

An increasing number of high-severity vulnerabilities affect virtual targets and devices that support them, such as the following:

- management consoles
- management servers
- administrative virtual machines
- guest virtual machines
- hypervisors

Merely keeping track of virtual assets and their various states and classifications is a challenge in itself. To manage their security effectively you need to keep track of important details: For example, which virtual machines have Windows operating systems? Which ones belong to a particular resource pool? Which ones are currently running? Having this information available keeps you in synch with the continual changes in your virtual asset environment, which also helps you to manage scanning resources more efficiently. If you know what scan targets you have at any given time, you know what and how to scan.

In response to these challenges the application supports dynamic discovery of virtual assets managed by VMware vCenter or ESX/ESXi.

Once you initiate Dynamic Discovery it continues automatically as long as the discovery connection is active.

Preparing the target VMware environment for Dynamic Discovery

To perform dynamic discovery in VMware environments, Nexpose can connect to either a vCenter server or directly to standalone ESX(i) hosts.

The application supports direct connections to the following vCenter versions:

- vCenter 4.1
- vCenter 4.1, Update 1
- vCenter 5.0

The application supports direct connections to the following ESX(i) versions:

- ESX 4.1
- ESX 4.1, Update 1
- ESXi 4.1
- ESXi 4.1, Update 1
- ESXi 5.0

The preceding list of supported ESX(i) versions is for *direct connections to standalone hosts.* To determine if the application supports a connection to an ESX(i) host that is managed by vCenter, consult VMware's interoperability matrix at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php.

You must configure your vSphere deployment to communicate through HTTPS. To perform Dynamic Discovery, the Security Console initiates connections to the vSphere application program interface (API) via HTTPS.

If Nexpose and your target vCenter or virtual asset host are in different subnetworks that are separated by a device such as a firewall, you will need to make arrangements with your network administrator to enable communication, so that the application can perform Dynamic Discovery.

Make sure that port 443 is open on the vCenter or virtual machine host because the application needs to contact the target in order to initiate the connection.

When creating a discovery connection, you will need to specify account credentials so that the application can connect to vCenter or the ESX/ESXi host. Make sure that the account has permissions at the root server level to ensure all target virtual assets are discoverable. If you assign permissions on a folder in the target environment, you will not see the contained assets unless permissions are also defined on the parent resource pool. As a best practice, it is recommended that the account have read-only access.

Make sure that virtual machines in the target environment have VMware Tools installed on them. Assets can be discovered and will appear in discovery results if they do not have VMware Tools installed. However, with VMware Tools, these target assets can be included in dynamic sites. This has significant advantages for scanning. See *Configuring a dynamic site* on page 200.

Discovering assets through DHCP log queries

- *Preparing the target environment for Dynamic Discovery through DHCP Directory Watcher method* on page 170
- *Creating and managing Dynamic Discovery connections* on page 170
- *Initiating Dynamic Discovery* on page 183
- *Using filters to refine Dynamic Discovery* on page 186
- *Configuring a dynamic site* on page 200

This connection extends your visibility into your asset inventory by exposing assets that may not be otherwise apparent. Scan Engines query DHCP server logs, which dynamically update with fresh asset information every five seconds. The engines pass the results of these queries to the Security Console. For each DHCP connection, you assign a specific Scan Engine.

The method discovers assets that the DHCP server has detected, or assets that have renewed their IP addresses, *after* the connection is initiated.

You can leverage the number of distributed Scan Engines to communicate with multiple DHCP servers and to connect with these servers in less accessible locations, such as behind firewalls or on the network perimeter.

Note: The DHCP method only discovers assets that have not yet been discovered by Nexpose through a different method or through a scan.

Two DHCP collection options are available:

- *Directory Watcher* monitors a specified directory on a DHCP server host and uploads new DHCP entries added to the directory at 10-second intervals. Use this method for log files that roll over to new files, such as Microsoft DHCP or Internet Information Services (IIS) files.
- *Syslog* operates like a syslog server, listening on a TCP or UDP port to receive syslog messages. Use this method if you are managing DHCP information with an Infoblox Trinzic appliance.

Preparing the target environment for Dynamic Discovery through DHCP Directory Watcher method

Note: The current implementation of DHCP discovery with the *Directory Watcher* method supports Microsoft Server 2008 and 2012.

Make sure your Microsoft DHCP configuration enables logging. Also, it is strongly recommended that you move the log files to a directory that is separate from the DHCP database files. Microsoft DHCP stores log data in a separate file for each day of the week and overwrites each file on a weekly basis.

Tip: The default directory path of the DHCP log file is in Windows 2008 is %windir%\System32\Dhcp. The path in Windows 2012 is %systemroot%\System32\Dhcp.

Creating and managing Dynamic Discovery connections

This action provides Nexpose the information it needs to contact a server or process that manages the asset environment.

You must have Global Administrator permissions to create or manage Dynamic Discovery connections. See the topic *Managing users and authentication* in the administrator's guide.

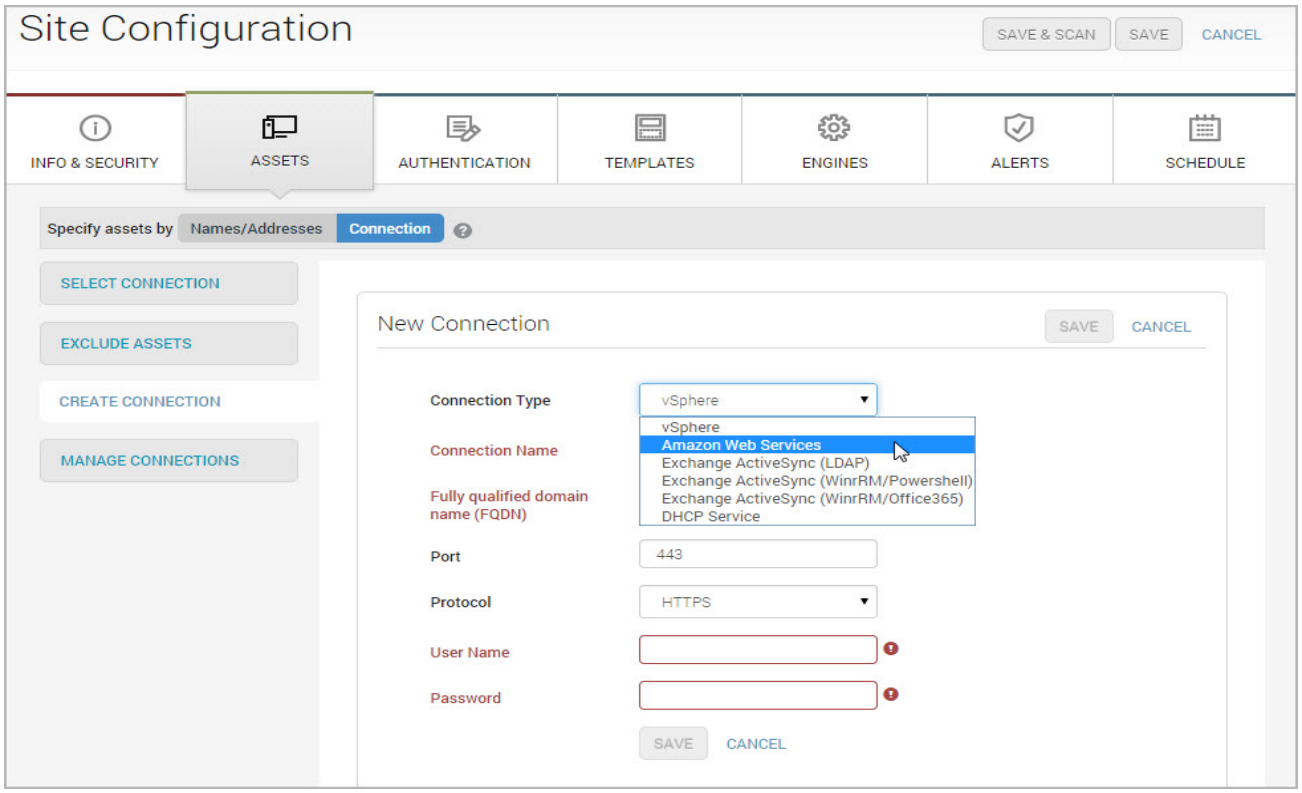
Creating a connection in a site configuration

If you want to create a connection while configuring a new site, click the **Create site** button on the *Home* page.

If you want to create a connection for an existing site, click that site's **Edit** icon in the *Sites* table on the *Home* page.

1. Click the **Assets** link in the site configuration .

2. Select **Connection** as the option for specifying assets.
3. Click **Create Connection**.
4. Select a connection type:
    - *Exchange ActiveSync (LDAP)* is for mobile devices managed by an Active Directory (AD) server.
    - *Exchange ActiveSync (WinRM/PowerShell)* is for mobile devices managed by an on-premise Exchange server accessed with PowerShell.
    - *Exchange ActiveSync (WinRM/Office 365)* is for mobile devices managed by Cloud-based Exchange server running Microsoft Office 365.
    - *vSphere* is for environments managed by VMware vCenter or ESX/ESXi.
    - *AWS* is for environments managed by Amazon Web Services.
    - *DHCP Service* is for assets that Scan Engines discover by collecting log data from DHCP servers.



Selecting a discovery connection type

Enter the information for a new connection with Exchange ActiveSync (LDAP):

1. Enter a unique name for the new connection on the *General* page.
2. Enter the name of the Active Directory (AD) server to which the Security Console will connect.
3. Select a protocol from the drop-down list.

   LDAPS, which is LDAP over SSL, is the more secure option and is recommended if it is enabled on your AD server.
4. Enter a user name and password for a member of the *Organization Management* Security Group in Microsoft Exchange.

   This account will enable the Security Console to discover mobile devices connected to the AD server.
5. Click **Save**. The connection appears in the **Connection** drop-down list, which you can view by clicking **Select Connection**.

6. Continue with *Initiating Dynamic Discovery* on page 183.

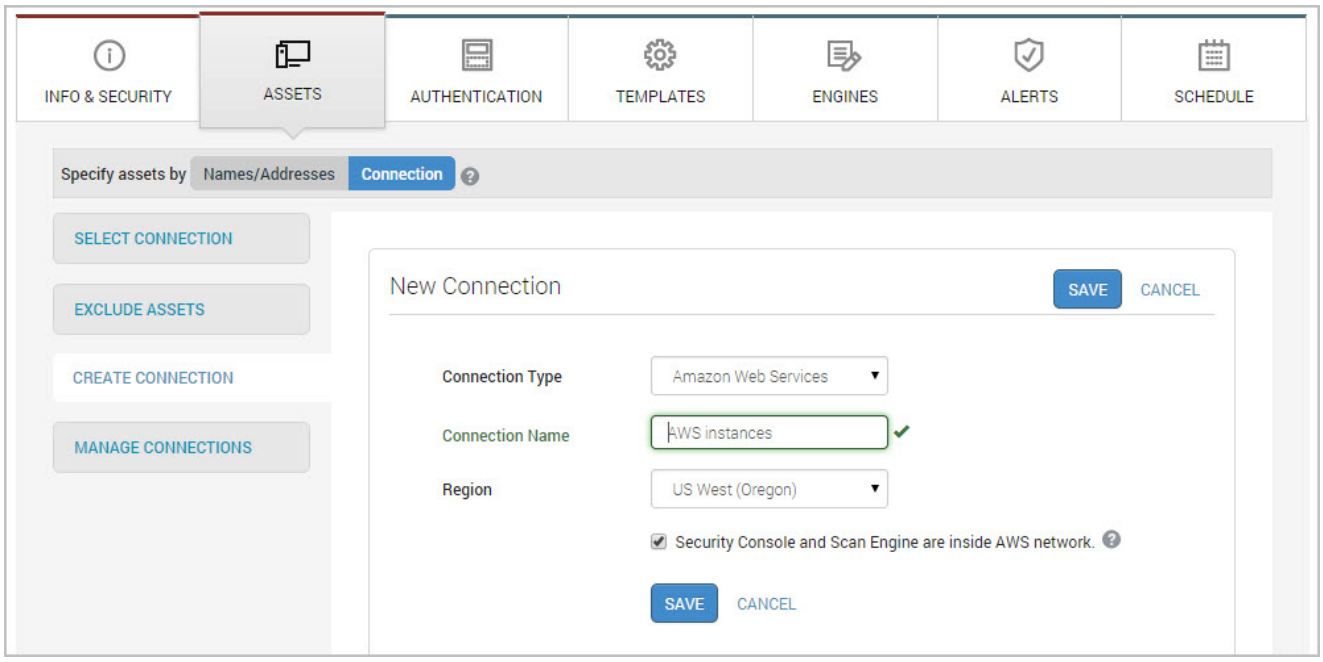
Enter the information for a new connection with Exchange ActiveSync (WinRM/PowerS/hell or WinRM/Office 365):

1. Enter a unique name for the new connection on the *General* page.
2. Enter the name of the of the WinRM gateway server to which the Security Console will connect.
3. Enter a user name and password for an account that has WinRM permissions for the gateway server.
4. Enter the fully qualified domain name of the Exchange server that manages the mobile device information.
5. Enter a user name and password for an administrator account or a user account that has View-Only Organizational Management or higher role of the *Organization Management* Security Group in Microsoft Exchange.
6. Click **Save**. The connection appears in the **Connection** drop-down list, which you can view by clicking **Select Connection**.
7. Continue with *Initiating Dynamic Discovery* on page 183.

Enter the information for a new connection (AWS):

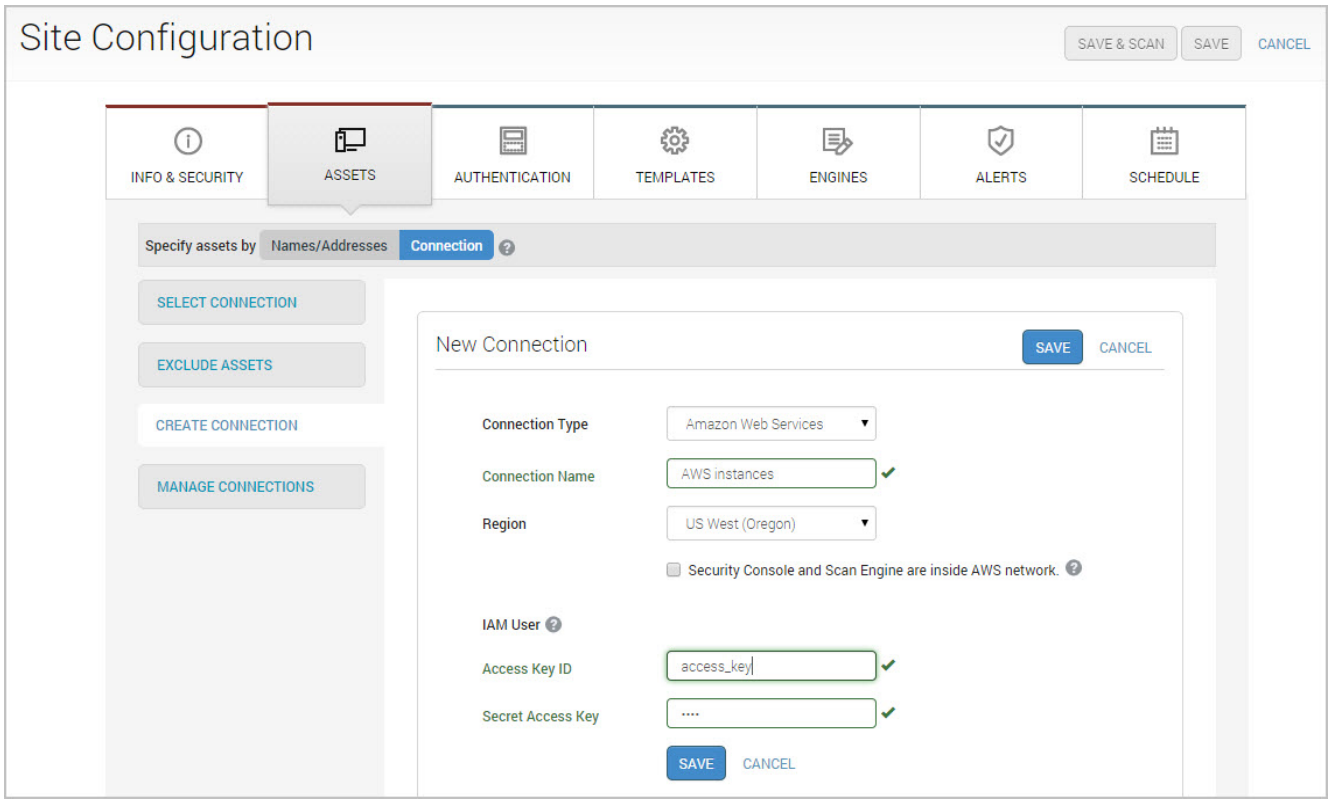
1. Enter a unique name for the new connection on the *General* page.

2. From the drop-down list, select the geographic region where your AWS instances are deployed.
3. If your Security Console and the Scan Engine you will use to scan the AWS environment are deployed inside the AWS network, select the check box. This will make the application to scan private IP addresses. See *Inside or outside the AWS network?* on page 165.
4. If you indicate that the Security Console and Scan Engine are inside the AWS network, the Credentials link disappears from the left navigation pane. You do not need to configure credentials, since the AWS API recongizes the IAM role of the AWS instance that the Security Console is installed on. In this case, simply click **Save** and ignore the following steps.



Setting up a connection with Nexpose components in the AWS network

5. Enter an Access Key ID and Secret Access Key with which the application will log on to the AWS API.



Setting up a connection with Nexpose components outside of the AWS network

6. Click **Save**. The connection appears in the **Connection** drop-down list, which you can view by clicking **Select Connection**.
7. Continue with *Initiating Dynamic Discovery* on page 183.

Enter the information for a new connection (vSphere).

1. Enter a unique name for the new connection on the *General* page.
2. Enter a fully qualified domain name for the server that the Security Console will contact in order to discover assets.
3. Enter a port number and select the protocol for the connection.

4. Enter a user name and password with which the Security Console will log on to the server. Make sure that the account has access to any virtual machine that you want to discover.
5. Click **Save**. The connection appears in the **Connection** drop-down list, which you can view by clicking **Select Connection**.
6. Continue with *Initiating Dynamic Discovery* on page 183.

Enter the information for a new connection (DHCP-*Directory Watcher*).

1. Enter a unique name for the new connection.
2. Select an event source type.
3. Select the *Directory Watcher* collection method.
4. Enter a network path to the folder containing the DHCP server logs to be queried. Use the format *//server/path/to/folder*. The server can be either a host name or IP address.
5. Select the Scan Engine that will collect the DHCP server log information.
6. Enter the administrative user name and password for accessing the DHCP server.
7. Click **Save**. The connection appears in the **Connection** drop-down list, which you can view by clicking **Select Connection**.
8. Continue with *Initiating Dynamic Discovery* on page 183.

Enter the information for a new connection (DHCP-*Syslog*).

Note: Syslog is the only available collection method for the Infoblox Trinzic event source.

1. Enter a unique name for the new connection.
2. Select an event source type.
3. Select the *Syslog* collection method.

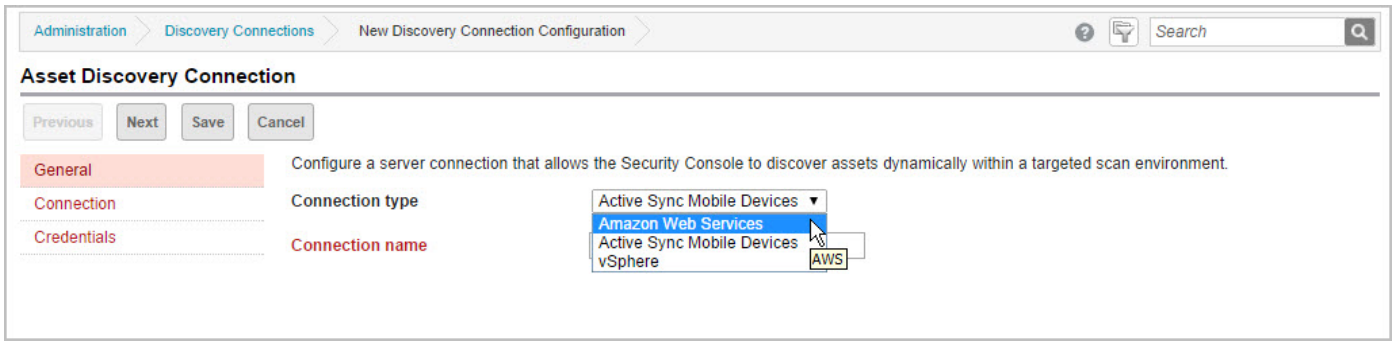
4. Enter the number for the port that the syslog parser listens on for log entries related to asset information.
5. Select the protocol for the port that the syslog parser listens on for log entries related to asset information.
6. Select the Scan Engine that will collect the DHCP server log information.
7. Click **Save**. The connection appears in the **Connection** drop-down list, which you can view by clicking **Select Connection**.
8. Continue with *Initiating Dynamic Discovery* on page 183.

Creating a connection outside of a site configuration

1. Click the **Administration** tab.
2. On the *Administration* page, under *Discovery Options*, click the **create** link for *Connections*.

   The Security Console displays the *General* page of the *Asset Discovery Connection* panel.
3. On the *General* page, select a connection type:

- *Exchange ActiveSync (LDAP)* is for mobile devices managed by an Active Directory (AD) server.
- *Exchange ActiveSync (WinRM/PowerShell)* is for mobile devices managed by an on-premise Exchange server accessed with PowerShell.
- *Exchange ActiveSync (WinRM/Office 365)* is for mobile devices managed by Cloud-based Exchange server running Microsoft Office 365.
- *vSphere* is for environments managed by VMware vCenter or ESX/ESXi.
- *AWS* is for environments managed by Amazon Web Services.
- *DHCP Service* is for assets that Scan Engines discover by collecting log data from DHCP servers.



Selecting a discovery connection type outside of a site configuration

Enter the information for a new connection (mobile devices)

1. Enter a unique name for the new connection on the *General* page.
2. Click **Connection**.

   The Security Console displays the *Connection* page.
3. Enter the name of the Active Directory (AD) server to which the Security Console will connect.
4. Select a protocol from the drop-down list.

   LDAPS, which is LDAP over SSL, is the more secure option and is recommended if it is enabled on your AD server.
5. Click **Credentials**.

   The Security Console displays the *Credentials* page.
6. Enter a user name and password for a member of the *Organization Management* Security Group in Microsoft Exchange.

   This account will enable the Security Console to discover mobile devices connected to the AD server.
7. Click **Save**.
8. Continue with *Initiating Dynamic Discovery* on page 183.

Enter the information for a new connection (AWS)

1. Enter a unique name for the new connection on the *General* page.
2. Click **Connection**.

   The Security Console displays the *Connection* page.
3. From the drop-down list, select the geographic region where your AWS instances are deployed.
4. If your Security Console and the Scan Engine you will use to scan the AWS environment are deployed inside the AWS network, select the check box. This will make the application to scan private IP addresses. See *Inside or outside the AWS network?* on page 165.
5. If you indicate that the Security Console and Scan Engine are inside the AWS network, the Credentials link disappears from the left navigation pane. You do not need to configure credentials, since the AWS API recongizes the IAM role of the AWS instance that the Security Console is installed on. In this case, simply click **Save** and ignore the following steps.
6. Click **Credentials**.

   The Security Console displays the *Credentials* page.
7. Enter an Access Key ID and Secret Access Key with which the application will log on to the AWS API.
8. Click **Save**.
9. Continue with *Initiating Dynamic Discovery* on page 183.

Enter the information for a new connection (vSphere)

1. Enter a unique name for the new connection on the *General* page.
2. Click **Service**.

   The Security Console displays the *Service* page.

3. Enter a fully qualified domain name for the server that the Security Console will contact in order to discover assets.
4. Enter a port number and select the protocol for the connection.
5. Click **Credentials**.

   The Security Console displays the *Credentials* page.
6. Enter a user name and password with which the Security Console will log on to the server. Make sure that the account has access to any virtual machine that you want to discover.
7. Click **Save**.
8. Continue with *Initiating Dynamic Discovery* on page 183.

Enter the information for a new connection (DHCP-*Directory Watcher*)

1. Enter a unique name for the new connection on the *General* page.
2. Click **Service**.
3. On the *Service* page, select an event source.
4. Select *Directory Watcher* as the collection method.
5. Enter a network path to the folder containing the DHCP server logs to be monitored. Use the format *//server/path/to/folder*. The server can be either a host name or IP address.
6. Select the Scan Engine that will collect the DHCP server log information.
7. Click **Credentials**.
8. On the *Credentials* page, enter the administrative user name and password for accessing the DHCP server.
9. Click **Save**.
10. Continue with *Initiating Dynamic Discovery* on page 183.

Tip: If you create a connection and later change it to reference a different DHCP server, your asset discovery results will change. Therefore, if it is important to you to associate assets with specific DHCP servers in Nexpose, consider associating the name of the connection with the

DHCP server and changing that name if you change the referenced server. Also, note that you cannot create duplicate DHCP connections.

Enter the information for a new connection (DHCP-*Syslog*)

Note: Syslog is the only available data collection method for the Infoblox Trinzic event source.

1. Enter a unique name for the new connection on the *General* page.
2. Click **Service**.
3. On the *Service* page, select an event source type.
4. Select the *Syslog* collection method.
5. Select the number of the port that the syslog parser listens on for log entries related to asset information.
6. Select the protocol for the port that the syslog parser listens on for log entries related to asset information.
7. Select the Scan Engine that will collect the DHCP server log information.
8. Click **Save**.
9. Continue with *Initiating Dynamic Discovery* on page 183.

Viewing and changing available connections

To view available connections or change a connection configuration take the following steps:

1. Go to the *Administration* page.
2. Click **manage** for *Discovery Connections*.

   The Security Console displays the *Discovery Connections* page.

3. Click **Edit** for a connection that you wish to change.
4. Enter information in the *Asset Discovery Connection* panel.
5. Click **Save**.
6. Continue with *Initiating Dynamic Discovery* on page 183.

OR

1. Click the **Dynamic Discovery** link that appears in the upper-right corner of the Security Console Web interface, below the user name.

   The Security Console displays the *Filtered asset discovery* page.

2. Click the **Manage** for connections.

   The Security Console displays the *Asset Discovery Connection* panel

3. Enter the information in the appropriate fields.
4. Click **Save**.
5. Continue with *Initiating Dynamic Discovery* on page 183.

On the *Discovery Connections* page, you can also delete connections or export connection information to a CSV file, which you can view in a spreadsheet for internal purposes.

You cannot delete a connection that has a dynamic site or an in-progress scan associated with it. Also, changing connection settings may affect asset membership of a dynamic site. See *Configuring a dynamic site* on page 200. You can determine which dynamic sites are associated with any connection by going to the *Discovery Management* page. See *Monitoring Dynamic Discovery* on page 199.

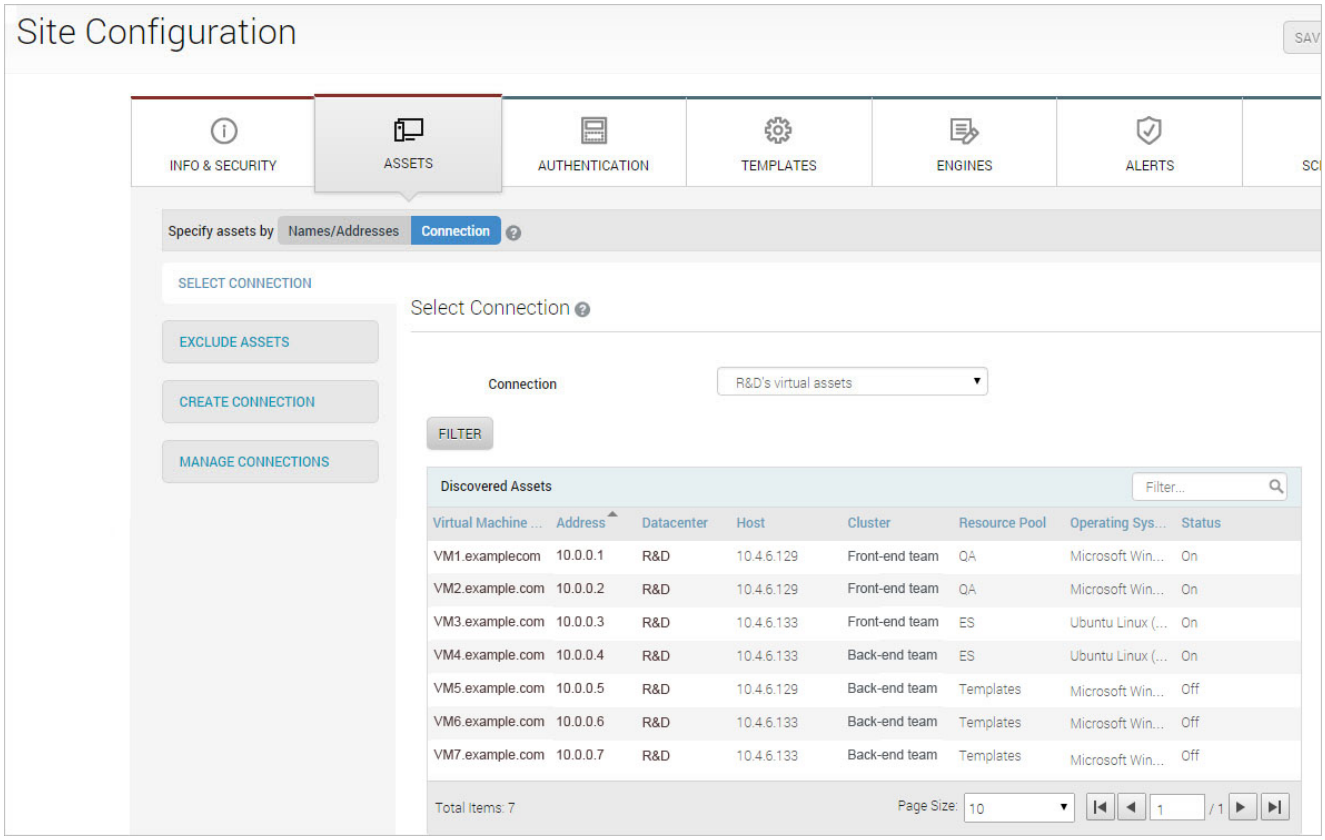
If you change a connection by using a different account, it may affect your discovery results depending which virtual machines the new account has access to. For example: You first create a connection with an account that only has access to all of the advertising department's virtual machines. You then initiate discovery and create a dynamic site. Later, you update the connection configuration with credentials for an account that only has access to the human resources department's virtual machines. Your dynamic site and discovery results will still include the advertising department's virtual machines; however, information about those machines will no longer be dynamically updated. Information is only dynamically updated for machines to which the connecting account has access.

Initiating Dynamic Discovery

This action involves having the Security Console contact the server or API and begin discovering virtual assets. After the application performs initial discovery and returns a list of discovered assets, you can refine the list based on criteria filters, as described in the following topic. To perform Dynamic Discovery, you must have the *Manage sites* permission. See *Configuring roles and permissions* in the administrator's guide.

1. After creating a connection (see *Creating a connection in a site configuration* on page 170) , click **Select Connection**.
2. Select the desired option from the drop-down list.

Nexpose establishes the connection and performs discovery. A table appears and lists information about each discovered asset.



Assets displayed in a VMware connection

Note: Assets discovered through a dynamic connection also appear on the *Assets* page. See *Comparing scanned and discovered assets* on page 242

Initiating discovery outside of a site configuration

1. Click the **Adminitration** tab.
2. On the *Administration* page, under *Discovery Options*, click the **create** link for *Connections*.

   The Security Console displays the *General* page of the *Asset Discovery Connection* panel.
3. Select the appropriate discovery connection name from the drop-down list labeled Connection.
4. Click **Discover Assets**.

Note: With new, changed, or reactivated discovery connections, the discovery process must complete before new discovery results become available. There may be a slight delay before new results appear in the Web interface.

Nexpose establishes the connection and performs discovery. A table appears and lists the following information about each discovered asset.

Displayed values for discovered assets

For mobile devices, the table includes the following:

- the operating system of the mobile device
- the account user name for the mobile device
- the last time the device synced with the Exchange server (WinRM/PowerShell and WinRM/Office 365 only)

For AWS connections, the table includes the following:

- the name of the AWS instance (asset)
- the instance's IP address
- the instance ID
- the instance's Availability Zone, which is a location within a geographic region that is insulated from failures in other Availability Zones and provides low-latency network connectivity to other Availability Zones in the same region
- the instance's geographic region
- the instance type, which defines its memory, CPU, storage capacity, and hourly cost
- the instance's operating system
- the operational state of the instance

For VMware connections, the table includes the following:

- the asset’s name
- the asset’s IP address
- the VMware datacenter in which the asset is managed
- the asset’s host computer
- the cluster to which the asset belongs
- the resource pool path that supports the asset
- the asset’s operating system
- the asset’s power status

For DHCP connections, the table includes the following:

- the asset's host name
- the asset's IP address
- the asset's MAC address

After performing the initial discovery, the application continues to discover assets as long as the discovery connection remains active. The Security Console displays a notification of any inactive discovery connections in the bar at the top of the Security Console Web interface. You can also check the status of all discovery connections on the Discovery Connections page. See *Creating and managing Dynamic Discovery connections* on page 170.

If you create a discovery connection but don't initiate discovery with that connection, or if you initiate a discovery but the connection becomes inactive, you will see an advisory icon in the top, left corner of the Web interface page. Roll over the icon to see a message about inactive connections. The message includes a link that you can click to initiate discovery.

After Nexpose discovers assets, they also appear in the Discovered by Connection table on the Assets page. See *Locating and working with assets* on page 240 for more information.

Using filters to refine Dynamic Discovery

You can use filters to refine Dynamic Discovery results based on specific discovery criteria. For example, you can limit discovery to assets that are managed by a specific resource pool or those with a specific operating system.

Note: If a set of filters is associated with a dynamic site, and if you change filters to include more assets than the maximum number of scan targets in your license, you will see an error message instructing you to change your filter criteria to reduce the number of discovered assets.

Using filters has a number of benefits. You can limit the sheer number of assets that appear in the discovery results table. This can be useful in an environment with a high number of virtual assets. Also, filters can help you discover very specific assets. You can discover all assets within an IP address range, all assets that belong to a particular resource pool, or all assets that are powered on or off. You can combine filters to produce more granular results. For example, you can discover all of Windows 7 virtual assets on a particular host that are powered on.

For every filter that you select, you also select an operator that determines how that filter is applied. Then, depending on the filter and operator, you enter a string or select a value for that operator to apply.

You can create dynamic sites based on different sets of discovery results and track the security issues related to these types of assets by running scans and reports. See *Configuring a dynamic site* on page 200.

Selecting filters for mobile devices

Three filters are available for mobile device connections:

- Operating System
- User
- Last Sync Time (WinRM/PowerShell and WinRM/Office 365 connections only)

Operating System

With the *Operating System* filter, you can discover assets based on their operating systems. This filter works with the following operators:

- *contains* returns all assets with operating systems whose names contain an entered string.
- *does not contain* returns all assets with operating systems whose names do not contain an entered string.

User

With the *User* filter, you can discover assets based on their associated user accounts. This filter works with the following operators:

- *contains* returns all assets with user accunts whose names contain an entered string.
- *does not contain* returns all assets with user accounts whose names do not contain an entered string.
- *is* returns all assets with user accounts whose names match an entered string exactly.
- *is not* returns all assets with user accounts whose names do not match an entered string.
- *starts with* returns all assets with user accounts whose names begin with the same characters as an entered string.

Last Sync Time

Note: This filter is only available with WinRM/PowerShell and WinRM/Office 365 Dynamic Discovery connections.

With the *Last Synch Time* filter, you can track mobile devices based on the most recent time they synchronized with the Exchange server. This filter can be useful if you do not want your reports to include data from old devices that are no longer in use on the network. It works with the following operators.

- *earlier than* returns all mobile devices that synchronized earlier than a number of preceding days that you enter in a text box.
- *within the last* returns all mobile devices that synchronized within a number of preceding days that you enter in a text box.

Selecting filters and operators for AWS connections

Eight filters are available for AWS connections:

- Availability Zone
- Guest OS family
- Instance ID
- Instance Name
- Instance state
- Instance Type
- Region

Availability Zone

With the *Availability Zone* filter, you can discover assets located in specific Availability Zones. This filter works with the following operators:

- *contains* returns all assets that belong to Availability Zones whose names contain an entered string.
- *does not contain* returns all assets that belong to Availability Zones whose names do not contain an entered string.

Guest OS family

With the *Guest OS family* filter, you can discover assets that have, or do not have, specific operating systems. This filter works with the following operators:

- *contains* returns all assets that have operating systems whose names contain an entered string.
- *does not contain* returns all assets that have operating systems whose names do not contain an entered string.

Instance ID

With the *Instance ID* filter, you can discover assets that have, or do not have, specific Instance IDs. This filter works with the following operators:

- *contains* returns all assets whose instance names whose instance IDs contain an entered string.
- *does not contain* returns all assets whose instance IDs do not contain an entered string.

Instance name

With the *Instance Name* filter, you can discover assets that have, or do not have, specific Instance IDs. This filter works with the following operators:

- *is* returns all assets whose instance names match an entered string exactly.
- *is not* returns all assets whose instance names do not match an entered string.
- *contains* returns all assets whose instance names contain an entered string.
- *does not contain* returns all assets whose instance names do not contain an entered string.
- *starts with* returns all assets whose instance names begin with the same characters as an entered string.

Instance state

With the *Instance state* filter, you can discover assets (instances) that are in, or are not in, a specific operational state. This filter works with the following operators:

- *is* returns all assets that are in a state selected from a drop-down list.
- *is not* returns all assets that are not in a state selected from a drop-down list.

Instance states include *Pending*, *Running*, *Shutting down*, *Stopped*, or *Stopping*.

Instance type

With the *Instance type* filter, you can discover assets that are, or are not, a specific instance type. This filter works with the following operators:

- *is* returns all assets that are a type selected from a drop-down list.
- *is not* returns all assets that are not a type selected from a drop-down list.

Instance types include *c1.medium*, *c1.xlarge*,*c3.2xlarge*, *c3.4xlarge*, or *c3.8xlarge*.

Note: Dynamic Discovery search results may also include m1.small or t1.micro instance types, but Amazon does not currently permit scanning of these types.

IP address range

With the *IP address range* filter, you can discover assets that have IP addresses, or do not have IP addresses, within a specific range. This filter works with the following operators:

- *is* returns all assets with IP addresses that falls within the entered IP address range.
- *is not* returns all assets whose IP addresses do not fall into the entered IP address range.

When you select the *IP address range* filter, you will see two blank fields separated by the word *to*. Enter the start of the range in the left field, and end of the range in the right field. The format for the IP addresses is a "dotted quad." Example: *192.168.2.1 to 192.168.2.254*

Region

With the *Region type* filter, you can discover assets that are in, or are not in, a specific geographic region. This filter works with the following operators:

- *is* returns all assets that are in a region selected from a drop-down list.
- *is not* returns all assets that are in a not a region selected from a drop-down list.

Regions include *Asia Pacific (Singapore)*, *Asia Pacific (Sydney)*, *Asia Pacific (Tokyo)*, *EU (Ireland)*, or *South American (Sao Paulo)*.

Selecting filters and operators for VMware connections

Eight filters are available for VMware connections:

- Cluster
- Datacenter
- Guest OS family
- Host
- IP address range
- Power state
- Resource pool path
- Virtual machine name

Cluster

With the *Cluster* filter, you can discover assets that belong, or don't belong, to specific clusters. This filter works with the following operators:

- *is* returns all assets that belong to clusters whose names match an entered string exactly.
- *is not* returns all assets that belong to clusters whose names do not match an entered string.
- *contains* returns all assets that belong to clusters whose names contain an entered string.
- *does not contain* returns all assets that belong to clusters whose names do not contain an entered string.
- *starts with* returns all assets that belong to clusters whose names begin with the same characters as an entered string.

Datacenter

With the *Datacenter* filter, you can discover assets that are managed, or are not managed, by specific datacenters. This filter works with the following operators:

- *is* returns all assets that are managed by datacenters whose names match an entered string exactly.
- *is not* returns all assets that are managed by datacenters whose names do not match an entered string.

Guest OS family

With the *Guest OS family* filter, you can discover assets that have, or do not have, specific operating systems. This filter works with the following operators:

- *contains* returns all assets that have operating systems whose names contain an entered string.
- *does not contain* returns all assets that have operating systems whose names do not contain an entered string.

Host

With the *Host* filter, you can discover assets that are guests, or are not guests, of specific host systems. This filter works with the following operators:

- *is* returns all assets that are guests of hosts whose names match an entered string exactly.
- *is not* returns all assets that are guests of hosts whose names do not match an entered string.
- *contains* returns all assets that are guests of hosts whose names contain an entered string.
- *does not contain* returns all assets that are guests of hosts whose names do not contain an entered string.
- *starts with* returns all assets that are guests of hosts whose names begin with the same characters as an entered string.

IP address range

With the *IP address range* filter, you can discover assets that have IP addresses, or do not have IP addresses, within a specific range. This filter works with the following operators:

- *is* returns all assets with IP addresses that falls within the entered IP address range.
- *is not* returns all assets whose IP addresses do not fall into the entered IP address range.

When you select the *IP address range* filter, you will see two blank fields separated by the word *to*. Enter the start of the range in the left field, and end of the range in the right field. The format for the IP addresses is a "dotted quad." Example: *192.168.2.1 to 192.168.2.254*

Power state

With the *Power state* filter, you can discover assets that are in, or are not in, a specific power state. This filter works with the following operators:

- *is* returns all assets that are in a power state selected from a drop-down list.
- *is not* returns all assets that are not in a power state selected from a drop-down list.

Power states include *on*, *off*, or *suspended*.

Resource pool path

With the *Resource pool path* filter, you can discover assets that belong, or do not belong, to specific resource pool paths. This filter works with the following operators:

- *contains* returns all assets that are supported by resource pool paths whose names contain an entered string.
- *does not contain* returns all assets that are supported by resource pool paths whose names do not contain an entered string.

You can specify any level of a path, or you can specify multiple levels, each separated by a hyphen and right arrow: ->. This is helpful if you have resource pool path levels with identical names.

For example, you may have two resource pool paths with the following levels:

Human Resources

Management

Workstations

Advertising

Management

Workstations

The virtual machines that belong to the *Management* and *Workstations* levels are different in each path. If you only specify *Management* in your filter, the application will discover all virtual machines that belong to the *Management* and *Workstations* levels in both resource pool paths.

However, if you specify *Advertising -> Management -> Workstations*, the application will only discover virtual assets that belong to the *Workstations* pool in the path with *Advertising* as the highest level.

Virtual machine name

With the *Virtual machine name* filter, you can discover assets that have, or do not have, a specific name. This filter works with the following operators:

- *is* returns all assets whose names match an entered string exactly.
- *is not* returns all assets whose names do not match an entered string.
- *contains* returns all assets whose names contain an entered string.
- *does not contain* returns all assets whose names do not contain an entered string.
- *starts with* returns all assets whose names begin with the same characters as an entered string.

Selecting filters and operators for DHCP connections

Three filters are available for VMware connections:

- Host name
- IP address
- MAC address

Host

With the *Host* filter, you can discover assets based on host names. This filter works with the following operators:

- *is* returns all assets with host names that match an entered string exactly.
- *is not* returns all assets with host names that do not match an entered string.
- *contains* returns all assets with host names that contain an entered string.
- *does not contain* returns all assets with host names that do not contain an entered string.
- *starts with* returns all assets with host names that begin with the same characters as an entered string.

IP address range

With the *IP address range* filter, you can discover assets that have IP addresses, or do not have IP addresses, within a specific range. This filter works with the following operators:

- *is* returns all assets with IP addresses that falls within the entered IP address range.
- *is not* returns all assets whose IP addresses do not fall into the entered IP address range.

When you select the *IP address range* filter, you will see two blank fields separated by the word *to*. Enter the start of the range in the left field, and end of the range in the right field. The format for the IP addresses is a "dotted quad." Example: *192.168.2.1 to 192.168.2.254*

MAC address

With the *MAC address* filter, you can discover assets based on MAC addresses. This filter works with the following operators:

- *is* returns all assets with MAC addresses that match an entered string exactly.
- *is not* returns all assets with MAC addresses that do not match an entered string.
- *contains* returns all assets with MAC addresses that contain an entered string.
- *does not contain* returns all assets with MAC addresses that do not contain an entered string.
- *starts with* returns all assets with MAC addresses that begin with the same characters as an entered string.

Combining discovery filters

If you use multiple filters, you can have the application discover assets that match all the criteria specified in the filters, or assets that match any of the criteria specified in the filters.

The difference between these options is that the *all* setting only returns assets that match the discovery criteria in all of the filters, whereas the *any* setting returns assets that match any given filter. For this reason, a search with *all* selected typically returns fewer results than *any*.

For example, a target environment includes 10 assets. Five of the assets run Ubuntu, and their names are Ubuntu01, Ubuntu02, Ubuntu03, Ubuntu04, and Ubuntu05. The other five run Windows, and their names are Win01, Win02, Win03, Win04, and Win05. Suppose you create two filters. The first discovery filter is an operating system filter, and it returns a list of assets that

run Windows. The second filter is an asset filter, and it returns a list of assets that have “Ubuntu” in their names.

If you discover assets with the two filters using the *all* setting, the application discovers assets that run Windows and have “Ubuntu” in their asset names. Since no such assets exist, no assets will be discovered. However, if you use the same filters with the *any* setting, the application discovers assets that run Windows or have “Ubuntu” in their names. Five of the assets run Windows, and the other five assets have “Ubuntu” in their names. Therefore, the result set contains all of the assets.

Configuring and applying filters

Note: If a virtual asset doesn’t have an IP address, it can only be discovered and identified by its host name. It will appear in the discovery results, but it will not be added to a dynamic site. Assets without IP addresses cannot be scanned.

After you initiate discovery as described in the preceding section, and the Security Console displays the results table, take the following steps to configure and apply filters:

Configure the filters.

1. Click **Add Filters**.

   A filter row appears.

2. Select a filter type from the left drop-down list.

3. Select an operator from the right drop-down list.

4. Enter or select a value in the field to the right of the drop-down lists.

5. To add a new filter, click the **+** icon.

   A new filter row appears. Set up the new filter as described in the preceding step.

6. Add more filters as desired. To delete any filter, click the appropriate **-** icon.

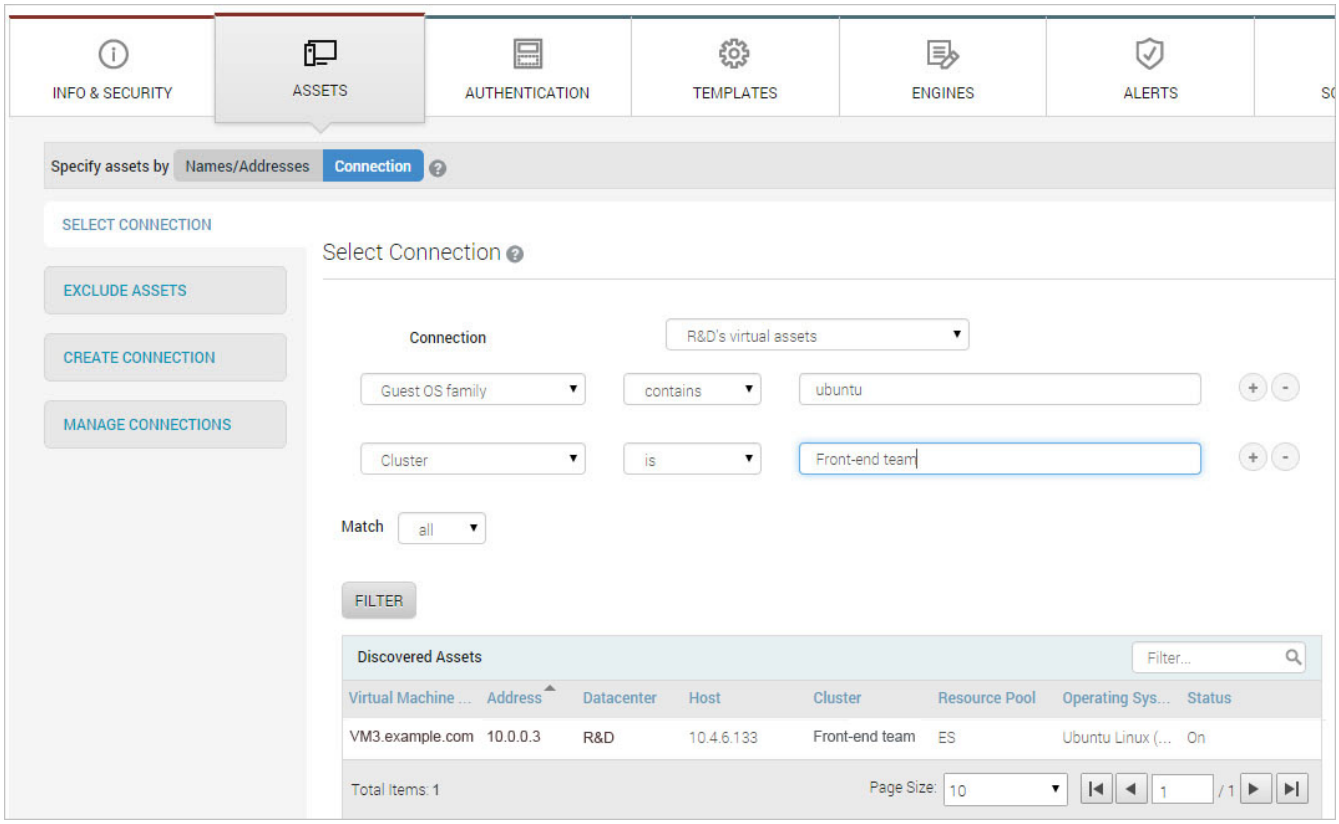
   After you configure the filters, you can apply them to the discovery results.

   Or, click **Reset** to clear all filters and start again.

Apply the filters.

1. Select the option to match *any* or *all* of the filters from the drop-down list below the filters.
2. Click **Filter**.

The discovery results table now displays assets based on filtered discovery.



Applying Dynamic Discovery filters within a site configuration

Monitoring Dynamic Discovery

Since discovery is an ongoing process as long as the connection is active, you may find it useful to monitor events related to discovery. The *Discovery Statistics* page includes several informative tables:

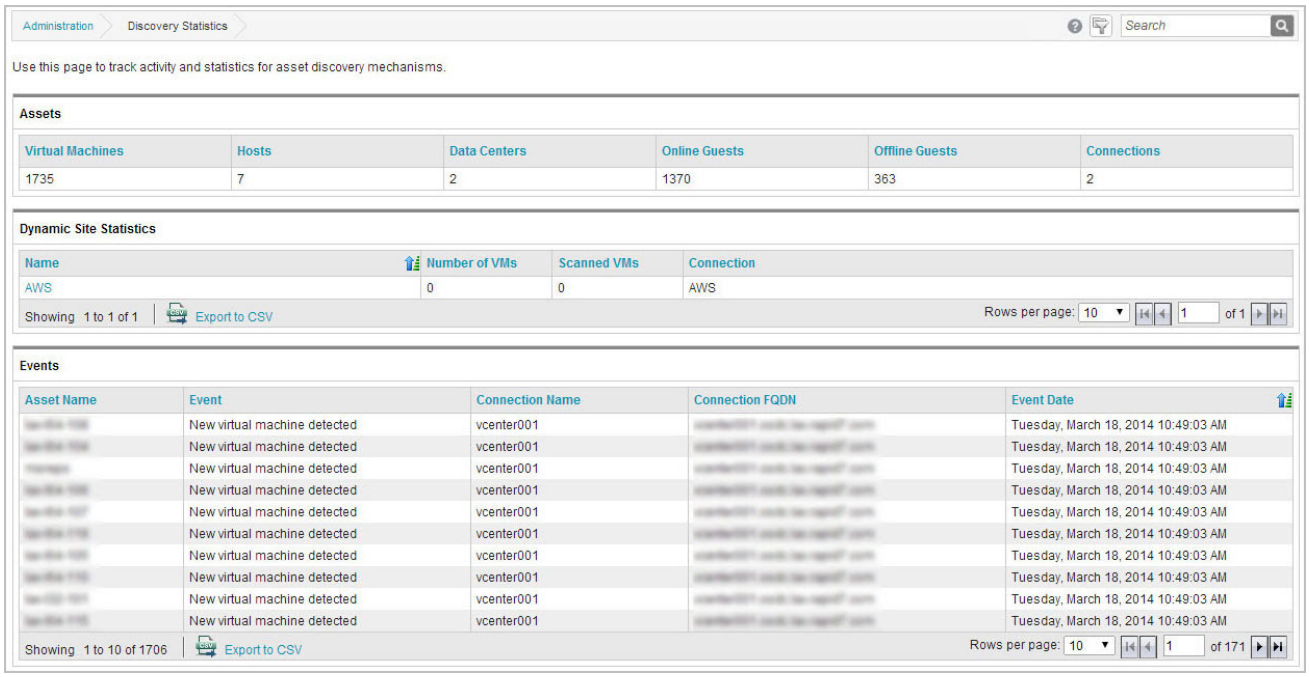
- *Assets* lists the number of currently discovered virtual machines, hosts, data centers, and discovery connections. It also indicates how many virtual machines are online and offline.
- *Dynamic Site Statistics* lists each dynamic site, the number of assets it contains, the number of scanned assets, and the connection through which discovery is initiated for the site's assets.
- *Events* lists every relevant change in the target discovery environment, such as virtual machines being powered on or off, renamed, or being added to or deleted from hosts.

Dynamic Discovery is not meant to enumerate the host types of virtual assets. The application categorizes each asset it discovers as a host type and uses this categorization as a filter in searches for creating dynamic asset groups. See *Performing filtered asset searches* on page 324. Possible host types include *Virtual machine* and *Hypervisor*. The only way to determine the host type of an asset is by performing a credentialed scan. So, any asset that you discover through Dynamic Discovery and do not scan with credentials will have an *Unknown* host type, as displayed on the scan results page for that asset. Dynamic discovery only finds virtual assets, so dynamic sites will only contain virtual assets.

Note: Listings in the *Events* table reflect discovery over the preceding 30 days.

To monitor Dynamic Discovery, take the following steps:

1. Go to the *Discovery Statistics* page in the Security Console Web interface.
2. Click the **Administration** tab.
3. In the *Discovery Options* area of the *Administration* page, click the **View** link for *Events*.



Viewing discovery statistics

Configuring a dynamic site

To create a dynamic site you must meet the following prerequisites:

- You must have a live Dynamic Discovery connection.
- You must initiate Dynamic Discovery. See *Initiating Dynamic Discovery* on page 183.

  If you attempt to create a dynamic site based on a number of discovered assets that exceeds the maximum number of scan targets in your license, you will see an error message instructing you to change your filter criteria to reduce the number of discovered assets. See *Using filters to refine Dynamic Discovery* on page 186.

Note: When you create a dynamic site, all assets that meet the site's filter criteria will not be correlated to assets that are part of existing sites. An asset that is listed in two sites is essentially regarded as two assets from a license perspective.

After creating and initiating a discovery connection, you can continue configuring a site.

If you have created and initiated a discovery connection outside of a site configuration, click the **Create Dynamic Site** button on the *Discovery* page. The Security Console displays the *Site Configuration*. Continue configuring the site.

Topics for site configuration

- *Selecting a Scan Engine or engine pool for a site* on page 75
- *Selecting a scan template* on page 88
- *Scheduling scans* on page 145
- *Setting up scan alerts* on page 143
- *Configuring scan credentials* on page 93
- *Giving users access to a site* on page 63

Managing assets in a dynamic site

As long as the connection for an initiated Dynamic Discovery is active, asset membership in a dynamic site is subject to change whenever changes occur in the target environment.

You can also change asset membership by changing the discovery connection or filters. See *Using filters to refine Dynamic Discovery* on page 186.

To view and change asset membership:

1. Click that **Edit** icon of the site you want to edit in the *Sites* table on the *Home* page.
2. Select the **Assets** tab.
3. The *Connection* option for specifying assets is already selected. Do not change it.
4. Click **Select Connection**.
5. Select a different connection from the drop-down list if desired.
6. Click the **Filters** button to change asset membership if desired. *Using filters to refine Dynamic Discovery* on page 186.
7. Click **Save** in the *Site Configuration*.

Whenever a change occurs in the target discovery environment, such as new virtual machines being added or removed, that change is reflected in the dynamic site asset list. This keeps your visibility into your target environment current.

Another benefit is that if the number of discovered assets in the dynamic site list exceeds the number of maximum scan targets in your license, you will see a warning to that effect before running a scan. This ensures that you do not run a scan and exclude certain assets. If you run a scan without adjusting the asset count, the scan will target assets that were previously discovered. You can adjust the asset count by refining the discovery filters for your site.

If you change the discovery connection or discovery filter criteria for a dynamic site that has been scanned, asset membership will be affected in the following ways: All assets that have not been scanned and no longer meet new discovery filter criteria, will be deleted from the site list. All assets that have been scanned and have scan data associated with them will remain on the site list whether or not they meet new filter discovery criteria. All newly discovered assets that meet new filter criteria will be added to the dynamic site list.

Integrating NSX network virtualization with scans

- *Activities in an NSX-integrated site* on page 203
- *Requirements for the vAsset Scan feature* on page 204
- *Deployment steps for the vAsset Scan feature* on page 204

Virtual environments are extremely fluid, which makes it difficult to manage them from a security perspective. Assets go online and offline continuously. Administrators re-purpose them with different operating systems or applications, as business needs change. Keeping track of virtual assets is a challenge, and enforcing security policies on them is an even greater challenge.

The vAsset Scan feature addresses this challenge by integrating Nexpose scanning with the VMware NSX network virtualization platform. The integration gives a Scan Engine direct access to an NSX network of virtual assets by registering the Scan Engine as a security service within that network. This approach provides several benefits:

- The integration automatically creates a Nexpose site, eliminating manual site configuration.
- The integration eliminates the need for scan credentials. As an authorized security service in the NSX network, the Scan Engine does not require additional authentication to collect extensive data from assets.
- Security management controls in NSX use scan results to automatically apply security policies to assets, saving time for IT or security teams. For example, if a scan flags a vulnerability that violates a particular policy, NSX can quarantine the affected asset until appropriate remediation steps are performed.

Note: The vAsset Scan feature is a different feature and license option from vAsset Discovery, which is related to the creation of dynamic sites that can later be scanned. For more information about that feature, see *Managing dynamic discovery of assets* on page 157.

Activities in an NSX-integrated site

When you create a site through this NSX integration process, you cannot do the following actions in the Site Configuration:

- Edit assets, which are dynamically added as part of the integration process.
- Change the Scan Engine, which is automatically configured as part of the integration process.
- Change the assigned scan template, which is Full Audit.
- Add scan credentials, which are unnecessary because the integration provides Nexpose with the depth of access to target assets that credentials would otherwise provide.

Requirements for the vAsset Scan feature

To use the vAsset Scan feature, you need the following components:

- a Nexpose installation with the vAsset Scan feature enabled in the license
- VMware ESXi 5.5 hosts
- VMware vCenter Server 5.5
- VMware NSX 6.0 or 6.1
- VMware Endpoint deployed
- VMware Endpoint Drivers (Thin Agent for VMs)

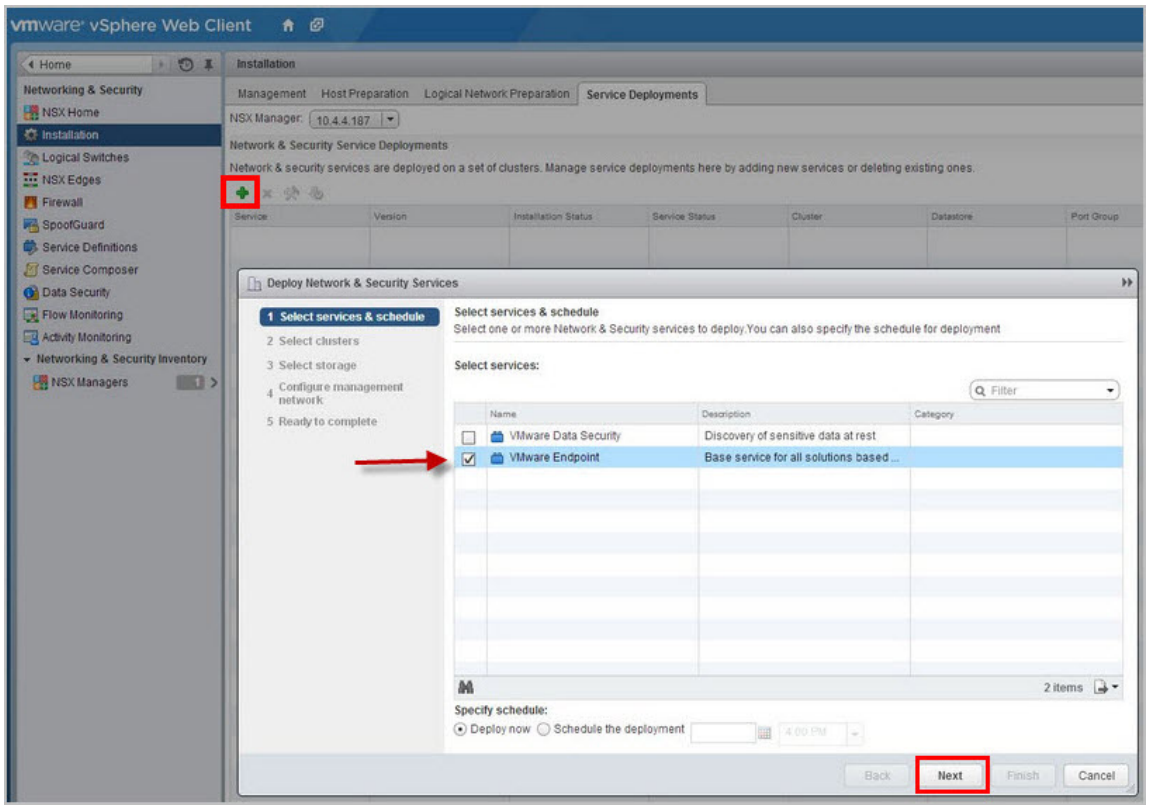
Deployment steps for the vAsset Scan feature

Deploying the vScan feature involves the following sequence of steps:

1. *Deploy the VMware endpoint* on page 205
2. *Deploy the Virtual Appliance (NexposeVA) to vCenter* on page 206
3. *Prepare the application to integrate with VMware NSX* on page 208
4. *Register Nexpose with NSX Manager* on page 211
5. *Deploy the Scan Engine from NSX* on page 213
6. *Create a security group* on page 215
7. *Create a security policy* on page 216
8. *Power on a Windows Virtual Machine* on page 218
9. *Scan the security group* on page 218

Deploy the VMware endpoint

1. Log onto the VMware vSphere Web Client.
2. From the *Home* menu, select **Network & Security**.
3. From the *Network & Security* menu, select **Installation.**
4. In the *Installation* pane, select the **Service Deployments** tab. Click the green plus sign () and then select the check box for **VMware Endpoint**. Then click the **Next** button to configure the deployment.



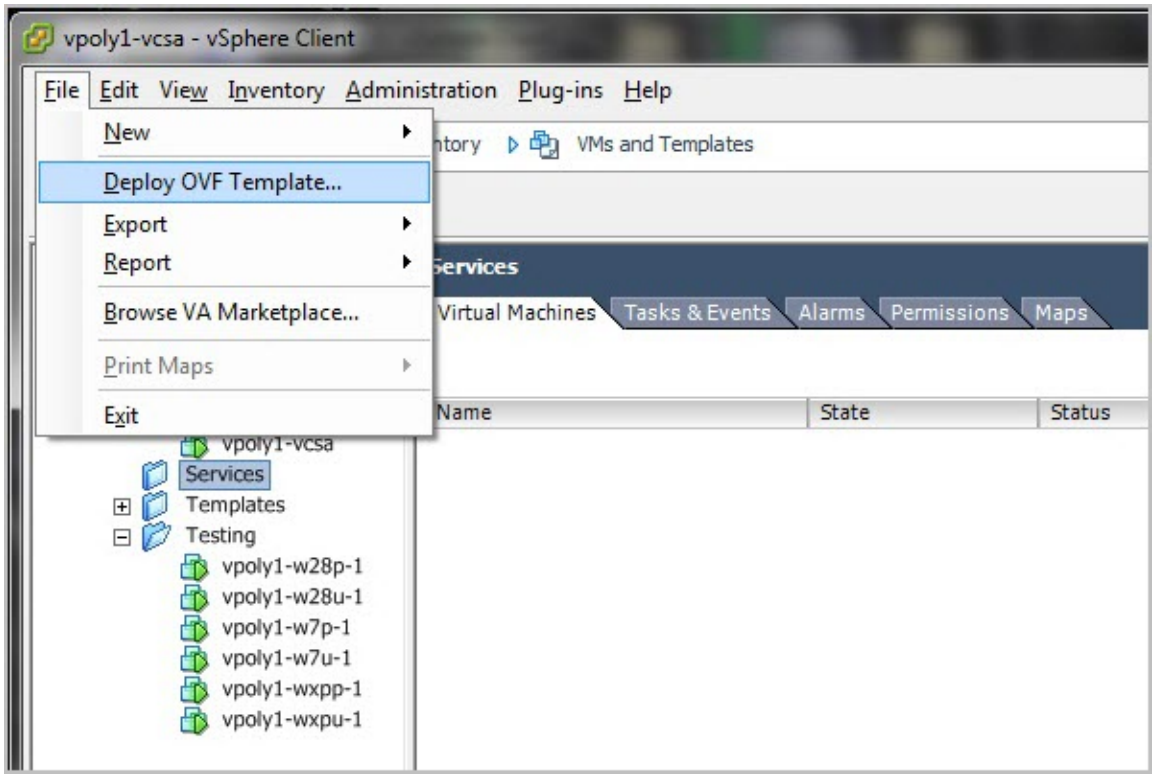
The vSphere Web Client-Select Services & Schedule pane

1. In the *Select clusters* pane, select a datacenter and cluster to deploy the VMware Endpoint on. Then click **Next**.
2. In the *Select storage* pane, select a data store for the VMware Endpoint. Then click **Next**.
3. In the *Configure management network* pane, select a network and IP assignment for the VMware Endpoint. Then click **Next**.
4. In the *Ready to complete* pane, click **Finish**.

Deploy the Virtual Appliance (NexposeVA) to vCenter

If you have an existing Nexpose installation running on a Linux operating system, you can skip this step and go directly to the topic *Prepare the application to integrate with VMware NSX* on page 208.

1. Download the NexposeVA.ova file from the Rapid7 Community at https://community.rapid7.com/docs/DOC-2595.
2. Log onto the VMware vSphere Client.
3. From the *File* menu, select **Deploy OVF Template...**
4. In the *Source* pane, click **Browse...** and locate and select the NexposeVA.ova file. Then, click **Next**.



The vSphere Client-Source > OVF Template details pane

5. In the *Name and Location* pane, enter a name and select an inventory location for the Virtual Appliance. Then, click **Next**.
6. In the *Host/Cluster* pane, select a datacenter and cluster in which to deploy the Virtual Appliance. Then, click **Next**.
7. In the *Storage* pane, select a data store for the Virtual Appliance. Then, click **Next**.
8. In the *Disk Format* pane, select a disk format for the Virtual Appliance. The format will depend on the datastore to which you are deploying. Then, click **Next**.
9. In the *Network Mapping* pane, select a network in which to deploy Virtual Appliance. Then, click **Next**.
10. If you are not using DHCP to auto-configure network settings for your Virtual Appliance deployment, go to the *Properties* pane and enter a default gateway address, a DNS server address, network interface address, and a netmask address. Then, click **Next**. OR If you are using DHCP, omit this step.
11. In the *Ready to Complete* pane, select the check box for **Power on after deployment**. Then, click **Finish**.

Note: If you configure a static IP address at this time, you will have to edit the OVF properties to make changes in the future.

Prepare the application to integrate with VMware NSX

Nexpose requires a copy of the Virtual Appliance Scan Engine to integrate with VMware NSX.

Download the Virtual Appliance Scan Engine from the Rapid7 Community at https://community.rapid7.com/docs/DOC-2595. Then take either of the following two sets of steps, depending on whether you are using Linux or Windows.

Linux

1. Log on to a shell session where Nexpose is installed on a Linux-based operating system. If you are using the Virtual Appliance, the default user name and password are both *nexpose*.
2. As a security best practice, change the credentials immediately after logging on.
3. Run the following script as root, or use sudo:

```
OVF_DEST=/opt/rapid7/nexpose/nsc/webapps/console/nse/ovf
 NEXPOSEVASE_SRC='http://download2.rapid7.com/download/NeXpose-
v4/NexposeVASE.ova'

 mkdir -p $OVF_DEST
 wget -P /tmp $NEXPOSEVASE_SRC

 tar -xvf /tmp/NexposeVASE.ova -C /tmp
 mv /tmp/NexposeVASE_OVF10.ovf $OVF_DEST/NexposeVASE.ovf
 mv /tmp/system.vmdk $OVF_DEST/system.vmdk
 chmod 644 $OVF_DEST/*
 rm -f /tmp/NexposeVASE*

 # TEMPORARY FIX - Hard-code private IP address in OVF file
 sed -i 's/ <Property ovf:key="ip1" ovf:userConfigurable="true"
ovf:type="string">/ <Property ovf:key="ip1" ovf:userConfigurable="true"
ovf:type="string" ovf:value="169.254.1.100">/g' ${OVF_DEST}
/NexposeVASE.ovf
 sed -i 's/ <Property ovf:key="netmask1" ovf:userConfigurable="true"
ovf:type="string">/ <Property ovf:key="netmask1"
ovf:userConfigurable="true" ovf:type="string"
ovf:value="255.255.255.0">/g' ${OVF_DEST}/NexposeVASE.ovf
```

The OVF_DEST in the script assumes Nexpose was installed in the default location of /opt/rapid7/nexpose. If you are not using the NexposeVA, modify your Nexpose installation path accordingly.

Windows

If you are in a Windows environment, take the following steps:

1. Log on to the Windows computer that has the Nexpose Security Console installed.
2. Download the Nexpose Virtual Appliance Scan Engine (NexposeVASE) at http://download2.rapid7.com/download/NeXpose-v4/NexposeVASE.ova.
3. If you don't have 7-Zip installed, download it at http://www.7-zip.org/download.html and install it.
4. Extract the NexposeVASE.ova file with 7-Zip.
5. Rename NexposeVASE_OVF10.ovf to *NexposeVASE.ovf*.
6. Delete the NexposeVASE_OVF10.mf file.
7. Create *nse/ovf folders* in C:\Program Files\[nexpose_installation_directory]\nsc\webapps\console.
8. Move the NexposeVASE.ovf and system.vmdk file to C:\Program Files\[nexpose_installation_directory]\webapps\console\nse\ovf.
9. Open the NexposeVASE.ovf file in a text editing application.
10. In the file, add a *ovf:value property* to the *ip1 key* and set the value to *169.254.1.100*

```
<Property ovf:key="ip1" ovf:userConfigurable="true" ovf:type="string"
ovf:value="169.254.1.100">
```

11. Add a ovf:value property to the netmask1 key and set the value to "255.255.255.0"

```
<Property ovf:key="netmask1" ovf:userConfigurable="true"
ovf:type="string" ovf:value="255.255.255.0">
```

12. Save and close the file.
13. Verify that Nexpose is licensed for the Virtual Scanning feature:
    a. Click the **Administration** tab in the Nexpose Security Console.
    b. On the *Administration* page, under Global and Console Settings, select the Administer link for Console.
    c. In the Security Console Configuration panel, select Licensing.
    d. On the Licensing page, look at the list of license-supported features and that Virtual Scanning is marked with a green check mark.
14. Verify the NexposeVASE.ovf file is accessible from the Security Console by typing the following URL in your browser: https://[Security_Console_IP_address]:3780/nse/ovf/NexposeVASE.ovf.

Register Nexpose with NSX Manager

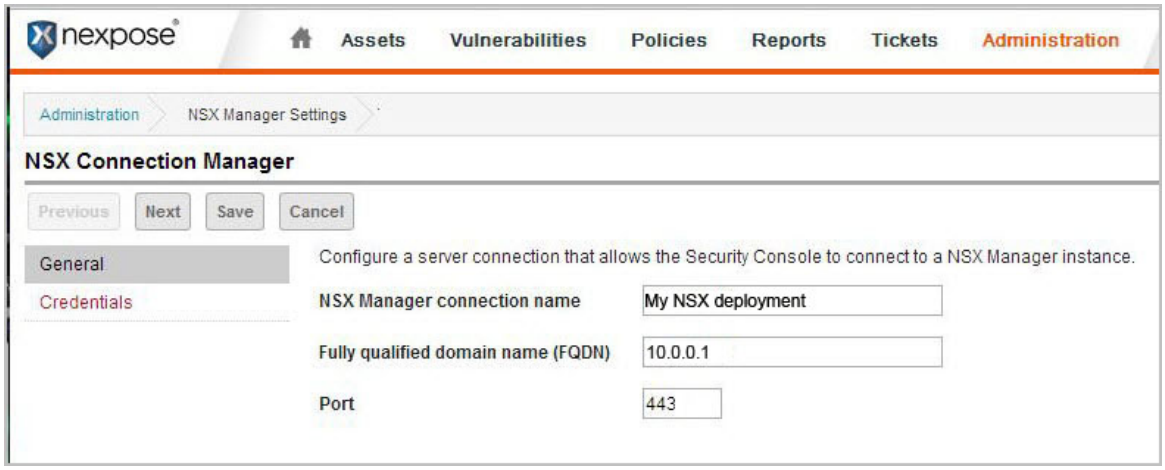
Nexpose must be registered with VMware NSX before it can be deployed into the virtual environment.

1. Log onto the Nexpose Security Console.
   Example: *https://[IP_address_of_Virtual_Appliance]:3780*
   The default user name is *nxadmin*, and the default password is *nxpassword*.

2. As a security best practice, change the default credentials immediately after logging on. To do so, click the **Administration** tab. On the *Administration* page, click the **manage** link next to *Users*. On the *Users* page, edit the default account with new, unique credentials, and click **Save**.

3. On the *Administration* page, click the **Create** link next to *NSX Manager* to create a connection between Nexpose and NSX Manager.

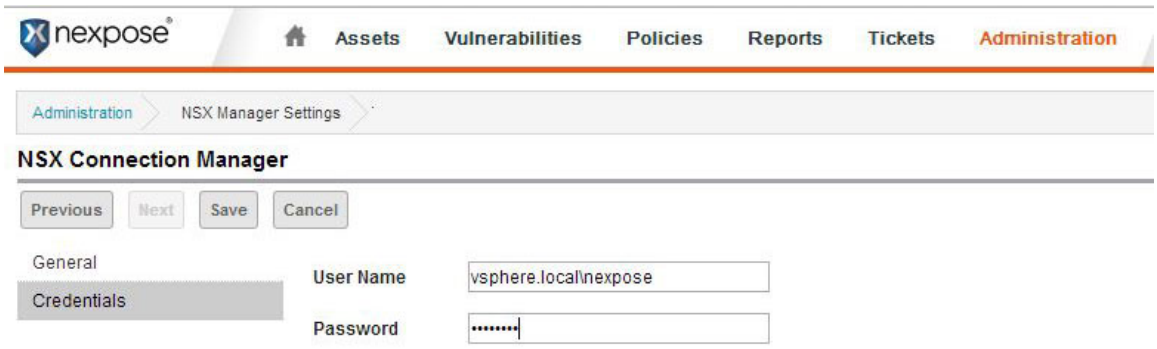
4. On the *General* page of the *NSX Connection Manager* panel, enter a connection name, the fully qualified domain name for the NSX Manager server, and a port number. The default port for NSX Manager is 443.



The Nexpose NSX Connection Manager panel-General page

5. On the *Credentials* page of the *NSX Connection Manager* panel, enter credentials for Nexpose to use when connecting with NSX Manager.

Note: These credentials must be created on NSX in advance, and the user must have the NSX Enterprise Administrator role.

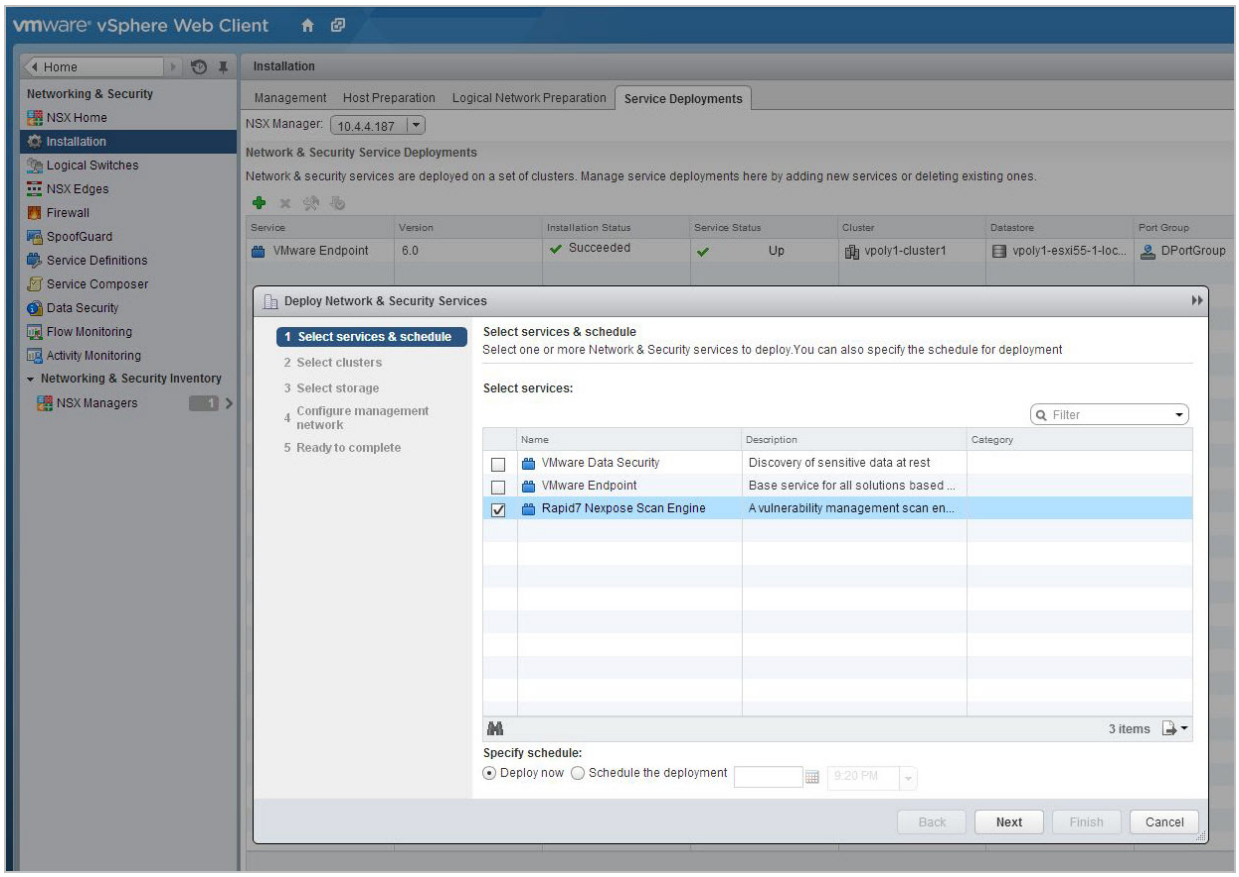


The Nexpose NSX Connection Manager panel-Credentials page

Deploy the Scan Engine from NSX

This deployment authorizes the Scan Engine to run as a security service in NSX. It also automatically creates a site in Nexpose.

1. Log onto the VMware vSphere Web Client.
2. From the *Home* menu, select **Network & Security**.
3. From the *Network & Security* menu, select **Installation**.
4. From the *Installation* menu, select **Service Deployments**.
5. In the *Installation* pane, click the green plus sign (+) and then select the check box for **Rapid7 Nexpose Scan Engine**. Then click the **Next** button to configure the deployment.

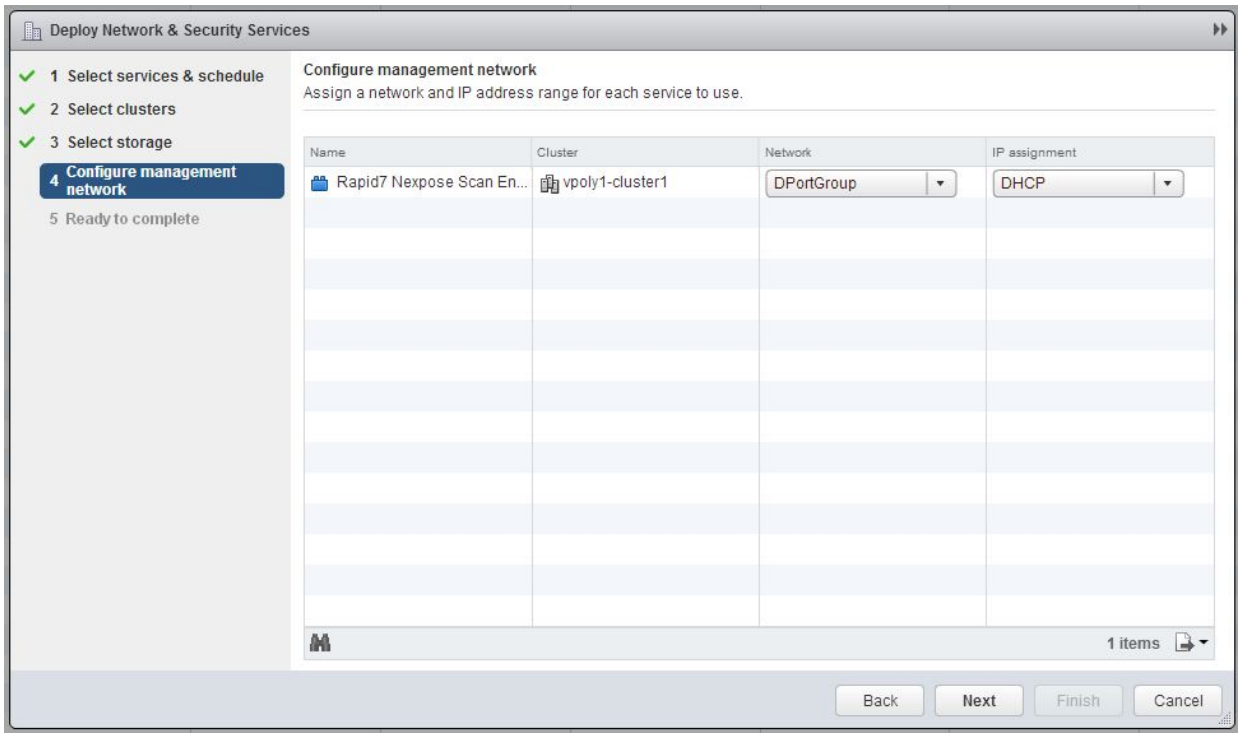


Configuring Scan Engine settings in NSX

6. Select the cluster in which to deploy the Rapid7 Nexpose Scan Engine.

Note: One Scan Engine will be deployed to each host in the selected cluster.

7. Configure the deployment according to your environment settings. Then click **Finish**.



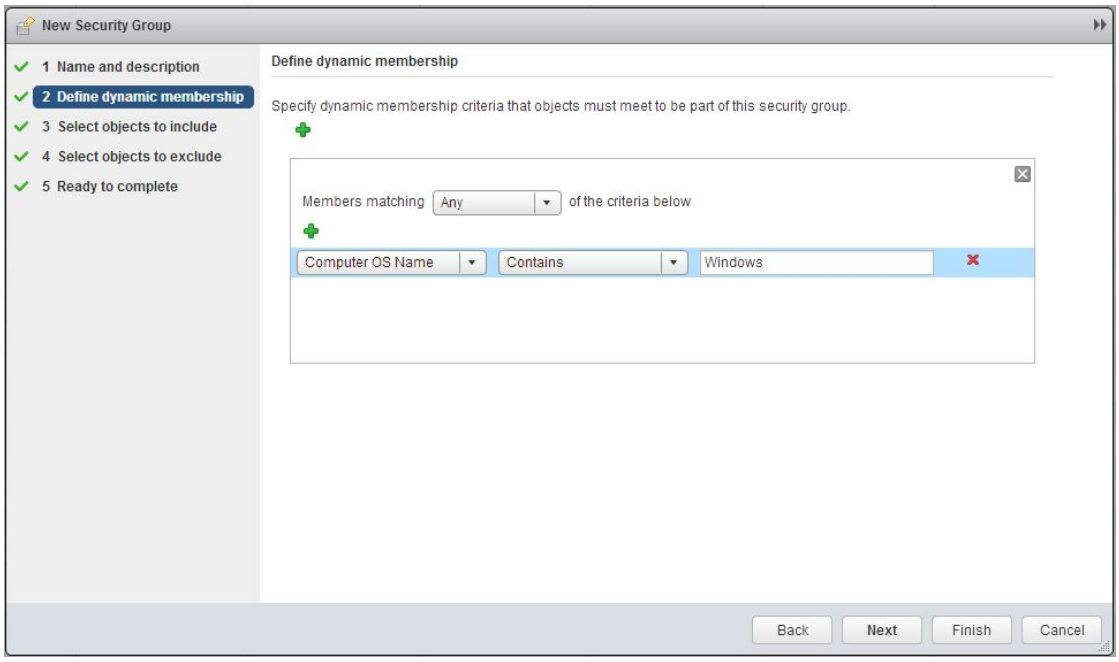
Configuring Scan Engine settings in NSX

Note: The Service Status will display *Warning* while the Scan Engine is initializing.

Create a security group

This procedure involves creating a group of virtual machines for Nexpose to scan. You will apply a security policy to this group in the following procedure.

1. From the *Home* menu in vSphere Web Client, select **Network & Security**.
2. From the *Network & Security* menu in vSphere Web Client, select **Service Composer**.
3. In the *Service Composer* pane, click **New Security Group**.
4. Create a security group. Use either dynamic criteria selection or enter individual virtual machine names.

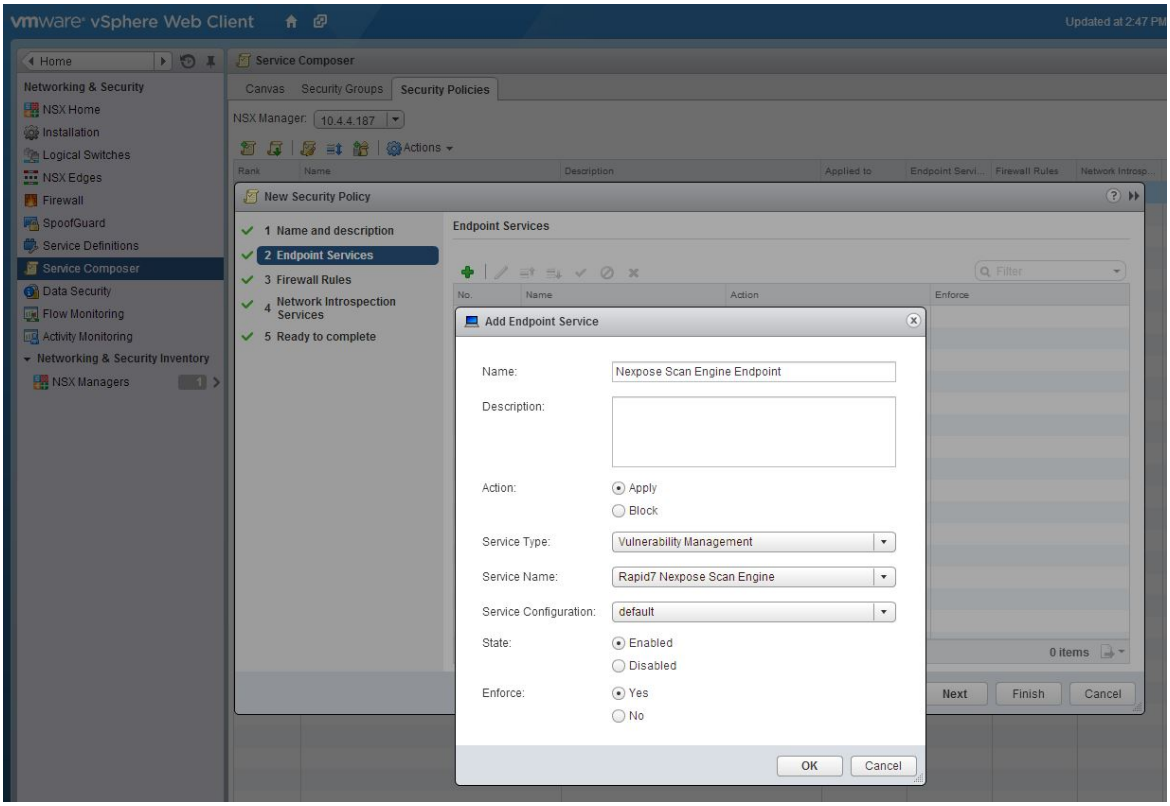


Creating a security group in NSX

Create a security policy

This new policy applies the Scan Engine as an endpoint service for the security group.

1. After you create a security group click, select it and click **Apply Policy**. Then, click the **New Security Policy...** link.
2. Create a new security policy for the *Rapid7 Nexpose Scan Engine* endpoint service, selecting the following settings:
   - **Action:** *Apply*
   - **Service Type:** *Vulnerability Management*
   - **Service Name:** *Rapid7 Nexpose Scan Engine*
   - **Service Configuration:** *default*
   - **State:** *Enabled*
   - **Enforced:** *Yes*
3. Click **OK**.



Creating a security policy in NSX

Power on a Windows Virtual Machine

This machine will serve as a scan target to verify that the integration is operating correctly.

1. Power on a Windows Virtual Machine that has VMware Tools version 9.4.0 or later installed.

Scan the security group

The rules of the policy will be enforced within the security group based on scan results.

1. Log onto the Nexpose Security Console.
2. In the *Site Listing* table, find the site that was auto-created when you deployed the Scan Engine from NSX.
3. Click the **Scan** icon to start the scan.

For information about monitoring the scan see *Running a manual scan* on page 222.

Importing AppSpider scan data

If you use Rapid7 AppSpider to scan your Web applications, you can import AppSpider data with Nexpose scan data and reports. This allows you to view security information about your Web assets side-by-side with your other network assets for more comprehensive assessment and prioritization.

The process involves importing an AppSpider-generated file of scan results, *VulnerabilitiesSummary.xml*, into a Nexpose site. Afterward, you view and report on that data as you would with data from a Nexpose scan.

If you import the XML file on a recurring basis, you will build a cumulative scan history in Nexpose about the referenced assets. This allows you to track trends related to those assets as you would with any assets scanned in Nexpose.

Note: This import process works with AppSpider versions 6.4.122 or later.

To import AppSpider data, take the following steps:

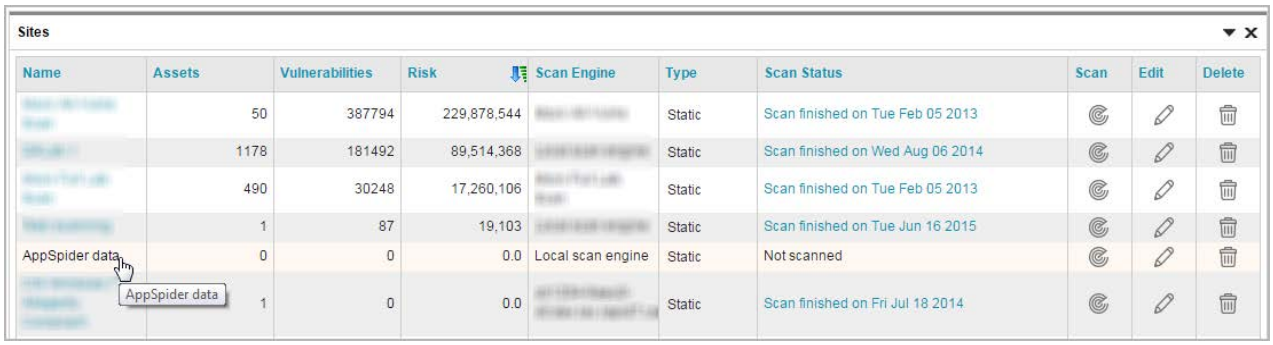
1. Create a site if you want a dedicated site to include AppSpider data exclusively. See *Creating and editing sites* on page 60.

   Since you are creating the site to contain AppSpider scan results, you do not need to set up scan credentials. You will need to include at least one asset, which is a requirement for creating a site. However, it will not be necessary to scan this asset.

   If you want to include AppSpider results in an existing site with assets scanned by Nexpose, skip this step.

2. Download the VulnerabilitiesSummary.xml file, generated by AppSpider, to the computer that you are using to access the Nexpose Web interface.

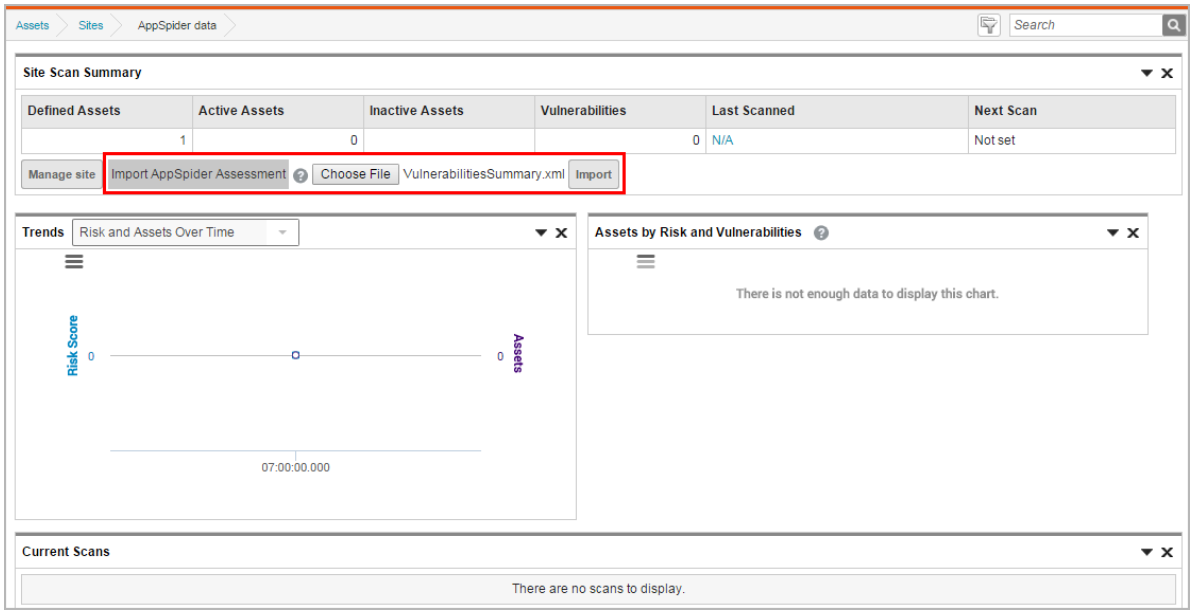
3. In the *Sites* table, select the name of the site that you want to use for AppSpider.



Selecting the site for importing AppSpider data

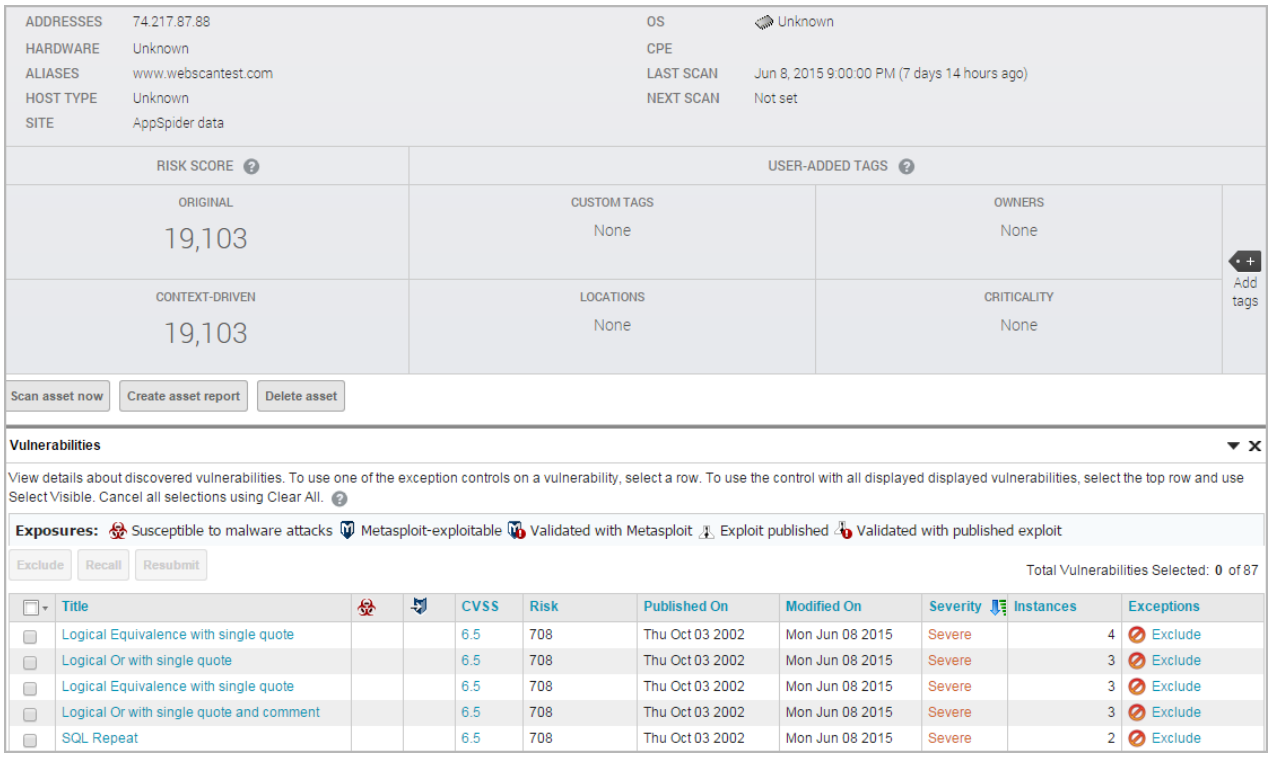
4. In the *Site Summary* table for that site, click the hypertext link labeled **Import AppSpider Assessment**.
5. Click the button that appears, labeled **Choose File**. Find the VulnerabilitiesSummary.xml on your local computer and click **Open** in Windows Explorer.

   The file name appears, followed by an **Import** button.
6. Click **Import**.



Importing the VulnerabilitiesSummary.xml file

The imported data appears in the *Assets* table on your site page. You can work with imported assets as you would with any scanned by Nexpose: View detailed information about them, tag them, and include them in asset groups, and reports.

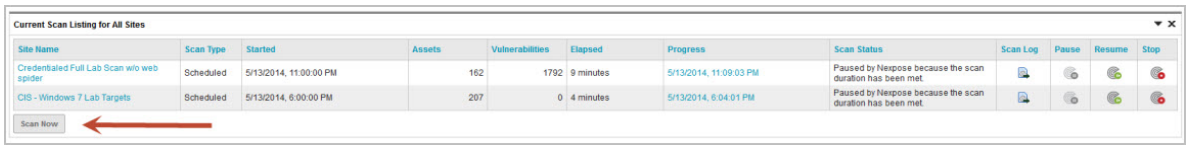


An asset scanned by AppSpider

Note: Although you can include imported assets in dynamic assets groups, the data about these imported assets is not subject to change with Nexpose scans. Data about imported assets only changes with subsequent imports of AppSpider data.

Running a manual scan

To start a scan manually, right away, click the **Scan** icon for a given site in the *Site Listing* pane of the *Home* page.



Starting a manual scan

Or, you can click the **Scan** button on the *Sites* page or on the page for a specific site.

The Security Console displays the *Start New Scan* dialog box, which lists all the assets that you specified in the site configuration to scan, or to exclude from the scan.

Note: You can start as many manual scans as you require. However, if you have manually started a scan of all assets in a site, or if a full site scan has been automatically started by the scheduler, the application will not permit you to run another full site scan.

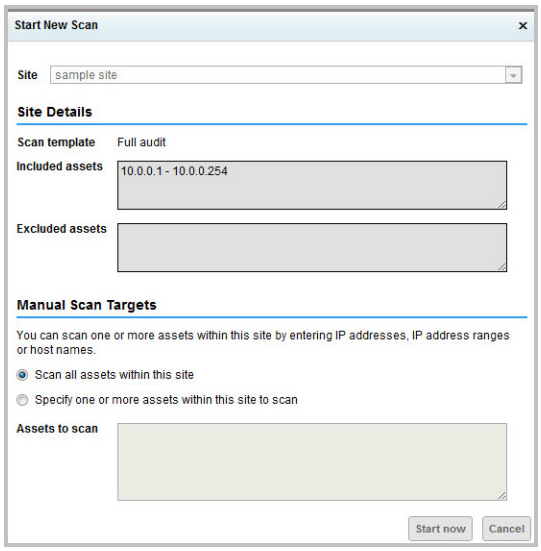
In the *Manual Scan Targets* area, select either the option to scan all assets within the scope of a site, or to specify certain target assets. Specifying the latter is useful if you want to scan a particular asset as soon as possible, for example, to check for critical vulnerabilities or verify a patch installation.

Note: You can only manually scan assets that were specified as addresses or in a range.

If you select the option to scan specific assets, enter their IP addresses or host names in the text box. Refer to the lists of included and excluded assets for the IP addresses and host names. You can copy and paste the addresses.

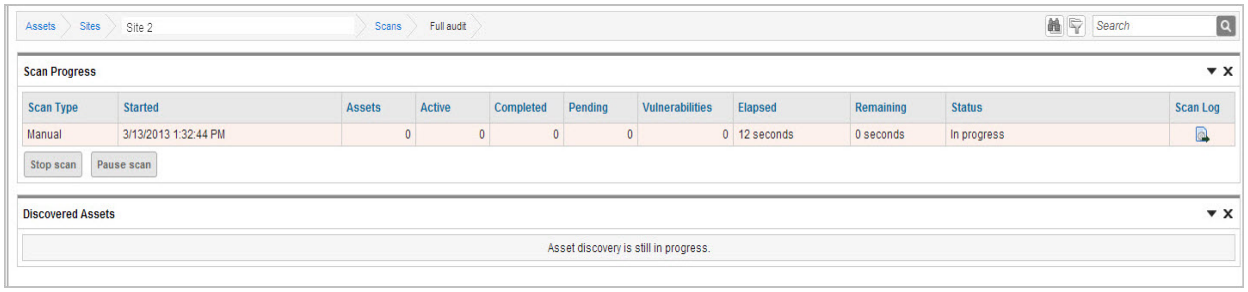
Note: If you are scanning Amazon Web Services (AWS) instances, and if your Security Console and Scan Engine are located outside the AWS network, you do not have the option to manually specify assets to scan. See *Inside or outside the AWS network?* on page 165.

Click the **Start Now** button to begin the scan immediately.



The Start New Scan window

When the scan starts, the Security Console displays a status page for the scan, which will display more information as the scan continues.



The status page for a newly started scan

Monitoring the progress and status of a scan

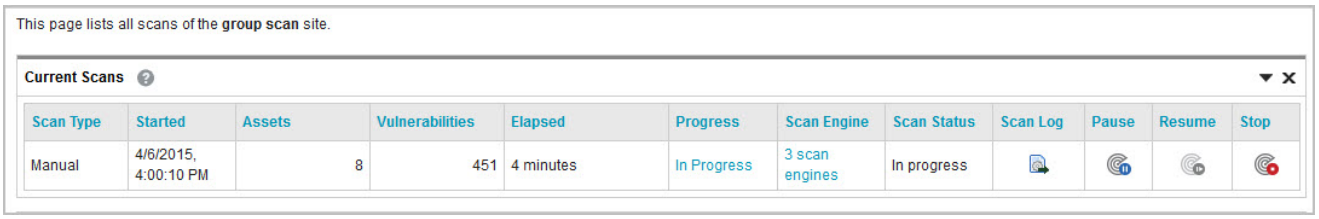
Viewing scan progress

When a scan starts, you can keep track of how long it has been running and the estimated time remaining for it to complete. You can even see how long it takes for the scan to complete on an individual asset. These metrics can be useful to help you anticipate whether a scan is likely to complete within an allotted window.

You also can view the assets and vulnerabilities that the in-progress scan is discovering if you are scanning with any of the following configurations:

- distributed Scan Engines (if the Security Console is configured to retrieve incremental scan results)
- the local Scan Engine (which is bundled with the Security Console)

If your scan includes asset groups and more than one Scan Engine is used, the table will list a count of Scan Engines used.


This page lists all scans of the **group scan** site.

Current Scans

Scan Type	Started	Assets	Vulnerabilities	Elapsed	Progress	Scan Engine	Scan Status	Scan Log	Pause	Resume	Stop
Manual	4/6/2015, 4:00:10 PM	8	451	4 minutes	In Progress	3 scan engines	In progress				

Scan progress table with multiple Scan Engines

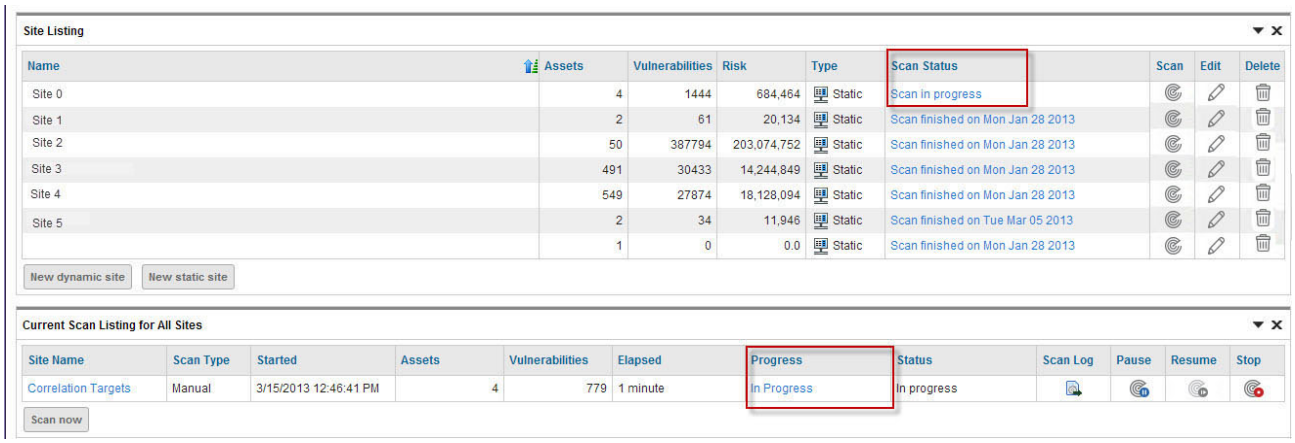
Viewing these discovery results can be helpful in monitoring the security of critical assets or determining if, for example, an asset has a zero-day vulnerability.

To view the progress of a scan:

1. Locate the *Site Listing* table on the *Home* page.
2. In the table, locate the site that is being scanned.
3. In the *Status* column, click the **Scan in progress** link.

OR

1. On the *Home* page, locate the *Current Scan Listing for All Sites* table.
2. In the table, locate the site that is being scanned.
3. In the *Progress* column, click the **In Progress** link.



The progress links for scans that are currently running

You will also find progress links in the *Site Listing* table on the *Sites* page or the *Current Scan Listing* table on the page for the site that is being scanned.

When you click the progress link in any of these locations, the Security Console displays a progress page for the scan.

At the top of the page, the *Scan Progress* table shows the scan's current status, start date and time, elapsed time, estimated remaining time to complete, and total discovered vulnerabilities. It lists the number of assets that have been discovered, as well as the following asset information:

- *Active* assets are those that are currently being scanned for vulnerabilities.
- *Completed* assets are those that have been scanned for vulnerabilities.
- *Pending* assets are those that have been discovered, but not yet scanned for vulnerabilities.

These values appear below a progress bar that indicates the percentage of completed assets. The bar is helpful for tracking progress at a glance and estimating how long the remainder of the scan will take.

Note: Remember to use bread crumb links to go back and forth between the *Home*, *Sites*, and specific site and scan pages.

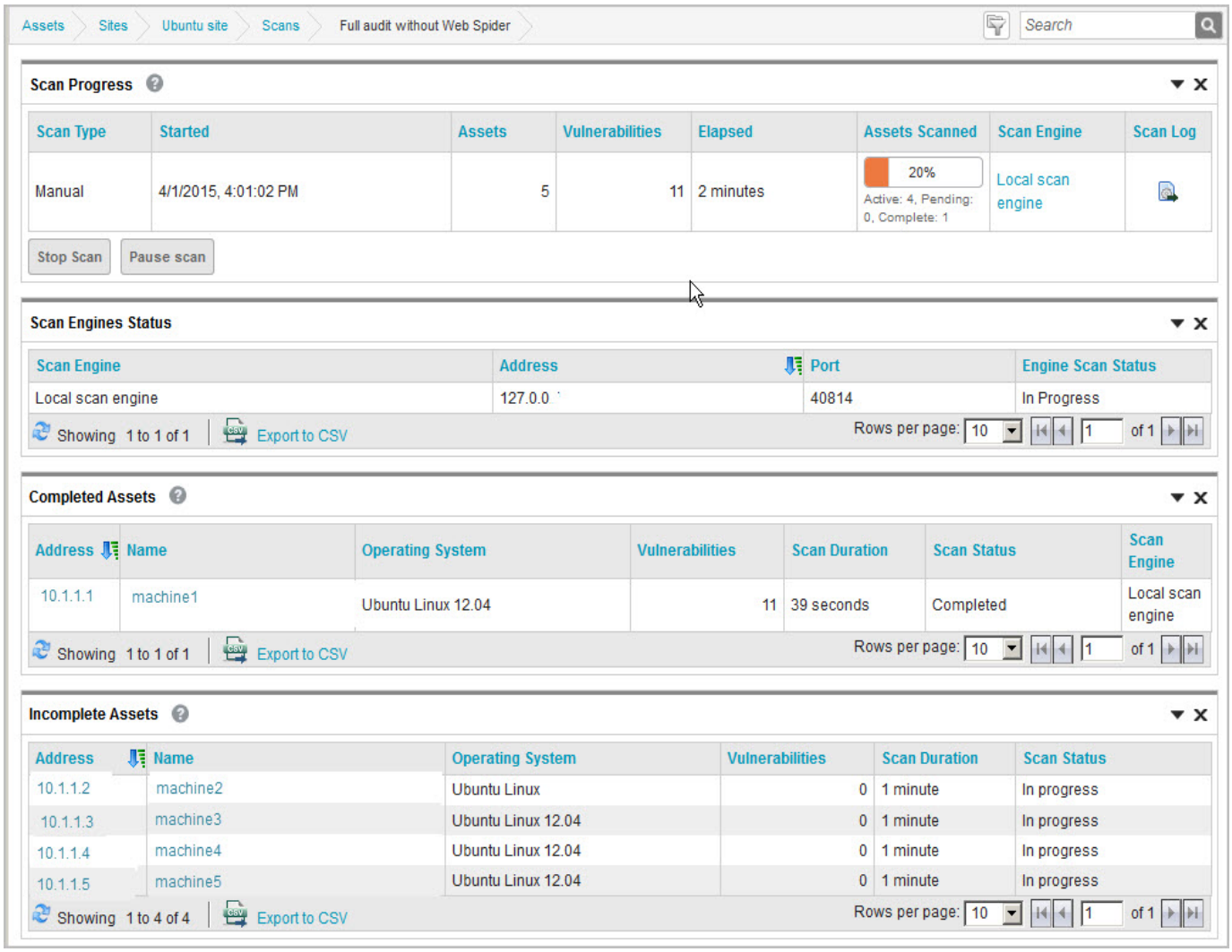
You can click the icon for the scan log to view detailed information about scan events. For more information, see *Viewing the scan log* on page 231.

The *Completed Assets* table lists assets for which scanning completed successfully, failed due to an error, or was stopped by a user.

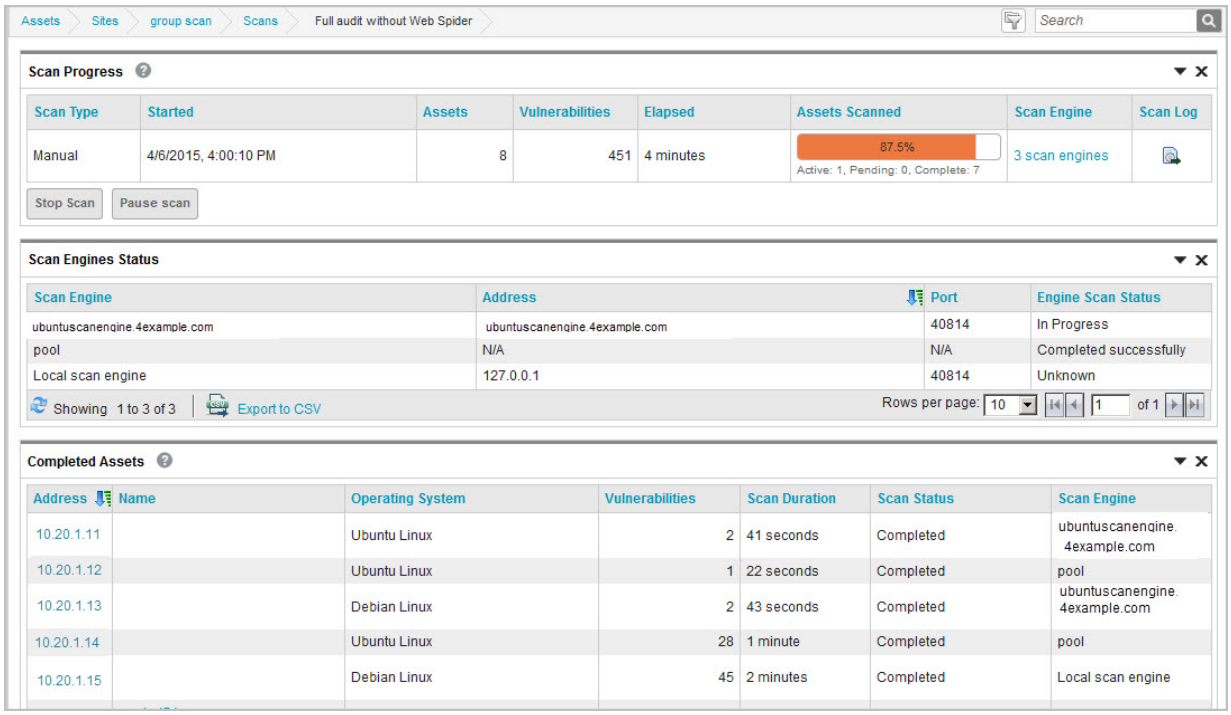
The *Incomplete Assets* table lists assets for which the scan is pending, in progress, or has been paused by a user. Additionally, any assets that could not be completely scanned because they went offline during the scan are marked *Incomplete* when the entire scan job completes.

These table list every asset's fingerprinted operating system (if available), the number of vulnerabilities discovered on it, and its scan duration and status. You can click the address or name link for any asset to view more details about, such as all the specific vulnerabilities discovered on it.

The table refreshes throughout the scan with every change in status. You can disable the automatic refresh by clicking the icon at the bottom of the table. This may be desirable with scans of large environments because the constant refresh can be a distraction.



A scan progress page with a single Scan Engine used



A scan progress page with multiple Scan Engines used

Understanding different Scan Engine statuses

The scan progress page also reports the status of the Scan Engine used for the site.

If you are scanning an asset group that is configured to use the Scan Engine most recently used for each asset, you may see statuses reported for more than one Scan Engine. For more information, see *Determining how to scan each asset when scanning asset groups* on page 76 .

The *Status* column reports the status of the Scan Engine. These statuses correspond to the scan states. See *Understanding different scan states* on page 227. An additional possible Scan Engine status is:

- *Unknown*: The Scan Engine could not be contacted. You can check whether the Scan Engine is running and reachable.

Understanding different scan states

It is helpful to know the meaning of the various scan states listed in the *Status* column of the *Scan Progress* table. While some of these states are fairly routine, others may point to problems that you can troubleshoot to ensure better performance and results for future scans. It is also helpful

to know how certain states affect scan data integration or the ability to resume a scan. In the *Status* column, a scan may appear to be in any one of the following states:

In progress: A scan is gathering information on a target asset. The Security Console is importing data from the Scan Engine and performing data integration operations such as correlating assets or applying vulnerability exceptions. In certain instances, if a scan's status remains *In progress* for an unusually long period of time, it may indicate a problem. See *Determining if scans with normal states are having problems* on page 229.

Completed successfully: The Scan Engine has finished scanning the targets in the site, and the Security Console has finished processing the scan results. If a scan has this state but there are no scan results displayed, see *Determining if scans with normal states are having problems* on page 229 to diagnose this issue.

Stopped: A user has manually stopped the scan before the Security Console could finish importing data from the Scan Engine. The data that the Security Console had imported before the stop is integrated into the scan database, whether or not the scan has completed for an individual asset. You cannot resume a stopped scan. You will need to run a new scan.

Paused: One of the following events occurred:

- A scan was manually paused by a user.
- A scan has exceeded its scheduled duration window. If it is a recurring scan, it will resume where it paused instead of restarting at its next start date/time.
- A scan has exceeded the Security Console's memory threshold before the Security Console could finish importing of data from the Scan Engine

In all cases, the Security Console processes results for targets that have a status of *Completed Successfully* at the time the scan is paused. You can resume a paused scan manually.

Note: When you resume a paused scan, the application will scan any assets in that site that did not have a status of *Completed Successfully* at the time you paused the scan. Since it does not retain the partial data for the assets that did not reach the completed state, it begins gathering information from those assets over again on restart.

Failed: A scan has been disrupted due to an unexpected event. It cannot be resumed. An explanatory message will appear with the *Failed* status. You can use this information to troubleshoot the issue with Technical Support. One cause of failure can be the Security Console or Scan Engine going out of service. In this case, the Security Console cannot recover the data from the scan that preceded the disruption.

Another cause could be a communication issue between the Security Console and Scan Engine. The Security Console typically can recover scan data that preceded the disruption. You can determine if this has occurred by one of the following methods:

- Check the connection between your Security Console and Scan Engine with a ICMP (ping) request.
- Click the *Administration* tab and then go to the *Scan Engines* page. Click on the **Refresh** icon for the Scan Engine associated with the failed scan. If there is a communication issue, you will see an error message.
- Open the nsc.log file located in the \nsc directory of the Security Console and look for error-level messages for the Scan Engine associated with the failure.

Aborted: A scan has been interrupted due to crash or other unexpected events. The data that the Security Console had imported before the scan was aborted is integrated into the scan database. You cannot resume an aborted scan. You will need to run a new scan.

Determining if scans with normal states are having problems

If a scan has an *In progress* status for an unusually long time, this may indicate that the Security Console cannot determine the actual state of the scan due to a communication failure with the Scan Engine. To test whether this is the case, try to stop the scan. If a communication failure has occurred, the Security Console will display a message indicating that no scan with a given ID exists.

If a scan has a *Completed successfully* status, but no data is visible for that scan, this may indicate that the Scan Engine has stopped associating with the scan job. To test whether this is the case, try starting the scan again manually. If this issue has occurred, the Security Console will display a message that a scan is already running with a given ID.

In either of these cases, contact Technical Support.

Pausing, resuming, and stopping a scan

If you are a user with appropriate site permissions, you can pause, resume or stop manual scans and scans that have been started automatically by the application scheduler.

Note: Remember to use bread crumb links to go back and forth between the *Home*, site, and scan pages.

You can pause, resume, or stop scans in several areas:

- the *Home* page
- the *Sites* page
- the page for the site that is being scanned
- the page for the actual scan

To pause a scan, click the **Pause** icon for the scan on the *Home*, *Sites*, or specific site page; or click the **Pause Scan** button on the specific scan page.

A message displays asking you to confirm that you want to pause the scan. Click **OK**.

To resume a paused scan, click the **Resume** icon for the scan on the *Home*, *Sites*, or specific site page; or click the **Resume Scan** button on the specific scan page. The console displays a message, asking you to confirm that you want to resume the scan. Click **OK**.

To stop a scan, click the **Stop** icon for the scan on the *Home*, *Sites*, or specific site page; or click the **Stop Scan** button on the specific scan page. The console displays a message, asking you to confirm that you want to stop the scan. Click **OK**.

The stop operation may take 30 seconds or more to complete pending any in-progress scan activity.

Viewing scan results

The Security Console lists scan results by ascending or descending order for any category depending on your sorting preference. In the *Asset Listing* table, click the desired category column heading, such as *Address* or *Vulnerabilities*, to sort results by that category.

Two columns in the *Asset Listing* table show the numbers of known exposures for each asset. The column with the ™ icon enumerates the number of vulnerability exploits known to exist for each asset. The number may include exploits available in Metasploit and/or the Exploit Database. The column with the icon enumerates the number of malware kits that can be used to exploit the vulnerabilities detected on each asset.

Click the link for an asset name or address to view scan-related, and other information about that asset. Remember that the application scans sites, not asset groups, but asset groups can include assets that also are included in sites.

To view the results of a scan, click the link for a site's name on the *Home* page. Click the site name link to view assets in the site, along with pertinent information about the scan results. On this page, you also can view information about any asset within the site by clicking the link for its name or address.

Viewing the scan log

To troubleshoot problems related to scans or to monitor certain scan events, you can download and view the log for any scan that is in progress or complete.

Understanding scan log file names

Scan log files have a .log extension and can be opened in any text editing program. A scan log's file name consists of three fields separated by hyphens: the respective site name, the scan's start date, and scan's start time in military format. Example: localsite-20111122-1514.log.

If the site name includes spaces or characters not supported by the name format, these characters are converted to hexadecimal equivalents. For example, the site name *my site* would be rendered as *my_20site* in the scan log file name.

The following characters are supported by the scan log file format:

- numerals
- letters
- hyphens (-)
- underscores (_)

The file name format supports a maximum of 64 characters for the site name field. If a site name contains more than 64 characters, the file name only includes the first 64 characters.

You can change the log file name after you download it. Or, if your browser is configured to prompt you to specify the name and location of download files, you can change the file name as you save it to your hard drive.

Finding the scan log

You can find and download scan logs wherever you find information about scans in the Web interface. You can only download scan logs for sites to which you have access, subject to your permissions.

- On the *Home* page, in the *Site Listing* table, click any link in the *Scan Status* column for in-progress or most recent scan of any site. Doing so opens the summary page for that scan. In the *Scan Progress* table, find the *Scan Log* column.
- On any site page, click the **View scan history** button in the *Site Summary* table. Doing so opens the *Scans* page for that site. In the *Scan History* table, find the *Scan Log* column.
- The *Scan History* page lists all scans that have been run in your deployment. On any page of the Web interface, click the **Administration** tab. On the *Administration* page, click the **view** link for *Scan History*. In the *Scan History* table, find the *Scan Log* column.

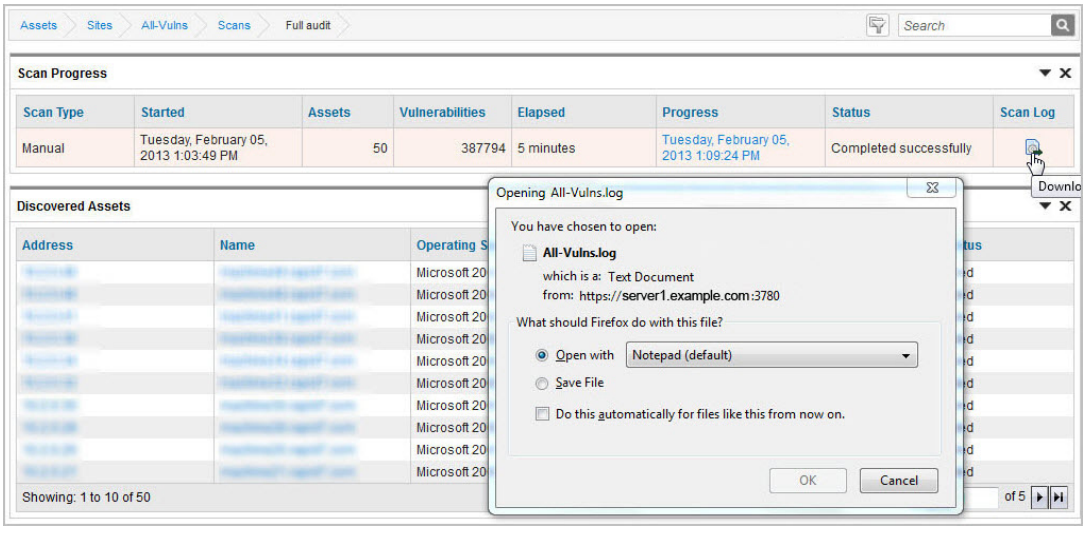
Downloading the scan log

To download a scan log click the **Download** icon for a scan log.

A pop-up window displays the option to open the file or save it to your hard drive. You may select either option.

If you do not see an option to open the file, change your browser configuration to include a default program for opening a .log file. Any text editing program, such as Notepad or gedit, can open a .log file. Consult the documentation for your browser to find out how to select a default program.

To ensure that you have a permanent copy of the scan log, choose the option to save it. This is recommended in case the scan information is ever deleted from the scan database.



Downloading a scan log

Tracking scan events in logs

While the Web interface provides useful information about scan progress, you can use scan logs to learn more details about the scan and track individual scan events. This is especially helpful if, for example, certain phases of the scan are taking a long time. You may want to verify that the prolonged scan is running normally and isn't "hanging". You may also want to use certain log information to troubleshoot the scan.

This section provides common scan log entries and explains their meaning. Each entry is preceded with a time and date stamp; a severity level (DEBUG, INFO, WARN, ERROR); and information that identifies the scan thread and site.

The beginning and completion of a scan phase

2013-06-26T15:02:59 [INFO] [Thread: Scan default:1] [Site: Chicago_servers] Nmap phase started.
The Nmap (Network Mapper) phase of a scan includes asset discovery and port-scanning of those assets. Also, if enabled in the scan template, this phase includes IP stack fingerprinting.

2013-06-26T15:25:32 [INFO] [Thread: Scan default:1] [Site: Chicago_servers] Nmap phase complete.
The Nmap phase has completed, which means the scan will proceed to vulnerability or policy checks.

Information about scan threads

2013-06-26T15:02:59 [INFO] [Thread: Scan default:1] [Site: Chicago_servers] Nmap will scan 1024 IP addresses at a time.
This entry states the maximum number of IP addresses each individual Nmap process will scan before that Nmap process exits and a new Nmap process is spawned. These are the work units assigned to each Nmap process. Only 1 Nmap process exists per scan.

2013-06-26T15:04:12 [INFO] [Thread: Scan default:1] [Site: Chicago_servers] Nmap scan of 1024 IP addresses starting.
This entry states the number of IP addresses that the current Nmap process for this scan is scanning. At a maximum, this number can be equal to the maximum listed in the preceding entry. If this number is less than the maximum in the preceding entry, that means the number of IP addresses remaining to be scanned in the site is less than the maximum. Therefore, the process reflected in this entry is the last process used in the scan.

Information about scan tasks within a scan phase

2013-06-26T15:04:13 [INFO] [Thread: Scan default:1:nmap:stdin] [Site: Chicago_servers] Nmap task Ping Scan started.
A specific task in the Nmap scan phase has started. Some common tasks include the following:

- *Ping Scan:* Asset discovery
- *SYN Stealth Scan:* TCP port scan using the SYN Stealth Scan method (as configured in the scan template)
- *Connect Scan:*TCP port scan using the Connect Scan method (as configured in the scan template)
- *UDP Scan:* UDP port scan

2013-06-26T15:04:44 [INFO] [Thread: Scan default:1:nmap:stdin] [Site: Chicago_servers] Nmap task Ping Scan is an estimated 25.06% complete with an estimated 93 second(s) remaining.
This is a sample progress entry for an Nmap task.

Discovery and port scan status

2013-06-26T15:06:04 [INFO] [Thread: Scan default:1:nmap:stdin] [Site: Chicago_servers] [10.0.0.1] DEAD (reason=no-response)
The scan reports the targeted IP address as *DEAD* because the host did not respond to pings.

2013-06-26T15:06:04 [INFO] [Thread: Scan default:1:nmap:stdin] [Site: Chicago_servers] [10.0.0.2] DEAD (reason=host-unreach)
The scan reports the targeted IP address as *DEAD* because it received an *ICMP host unreachable* response. Other ICMP responses include *network unreachable*, *protocol unreachable*, *administratively prohibited*. See the RFC4443 and RFC 792 specifications for more information.

2013-06-26T15:07:45 [INFO] [Thread: Scan default:1:nmap:stdin] [Site: Chicago_servers] [10.0.0.3:3389/TCP] OPEN (reason=syn-ack:TTL=124)
2013-06-26T15:07:45 [INFO] [Thread: Scan default:1:nmap:stdin] [Site: Chicago_servers] [10.0.0.4:137/UDP] OPEN (reason=udp-response:TTL=124)
The preceding two entries provide status of a scanned port and the reason for that status. *SYN-ACK* reflects a SYN-ACK response to a SYN request. Regarding TTL references, if two open ports have different TTLs, it could mean that a man-in-the-middle device between the Scan Engine and the scan target is affecting the scan.

2013-06-26T15:07:45 [INFO] [Thread: Scan default:1:nmap:stdin] [Site: Chicago_servers] [10.0.0.5] ALIVE (reason=echo-reply:latency=85ms:variance=13ms:timeout=138ms)
This entry provides information on the reason that the scan reported the host as *ALIVE*, as well

as the quality of the network the host is on; the latency between the Scan Engine and the host; the variance in that latency; and the timeout Nmap selected when waiting for responses from the target. This type of entry is typically used by Technical Support to troubleshoot unexpected scan behavior. For example, a host is reported *ALIVE*, but does not reply to ping requests. This entry indicates that the scan found the host through a TCP response.

The following list indicates the most common reasons for discovery and port scan results as reported by the scan:

- *conn-refused:* The target refused the connection request.
- *reset:* The scan received an RST (reset) response to a TCP packet.
- *syn-ack:* The scan received a SYN|ACK response to a TCP SYN packet.
- *udp-response:* The scan received a UDP response to a UDP probe.
- *perm-denied:* The Scan Engine operating system denied a request sent by the scan. This can occur in a full-connect TCP scan. For example, the firewall on the Scan Engine host is enabled and prevents Nmap from sending the request.
- *net-unreach:* This is an ICMP response indicating that the target asset's network was unreachable. See the RFC4443 and RFC 792 specifications for more information.
- *host-unreach:* This is an ICMP response indicating that the target asset was unreachable. See the RFC4443 and RFC 792 specifications for more information.
- *port-unreach:* This is an ICMP response indicating that the target port was unreachable. See the RFC4443 and RFC 792 specifications for more information.
- *admin-prohibited:* This is an ICMP response indicating that the target asset would not allow ICMP echo requests to be accepted. See the RFC4443 and RFC 792 specifications for more information.
- *echo-reply:* This is an ICMP echo response to an echo request. It occurs during the asset discovery phase.
- *arp-response:* The scan received an ARP response. This occurs during the asset discovery phase on the local network segment.
- *no-response:* The scan received no response, as in the case of a filtered port or dead host.
- *localhost-response:* The scan received a response from the local host. In other words, the local host has a Scan Engine installed, and it is scanning itself.
- *user-set:* As specified by the user in the scan template configuration, host discovery was disabled. In this case, the scan does not verify that target hosts are alive; it "assumes" that the targets are alive.

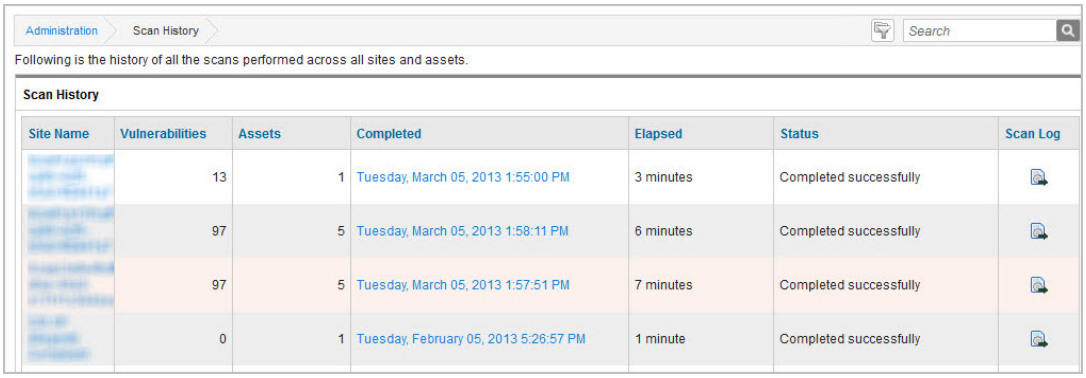
Viewing history for all scans

You can quickly browse the scan history for your entire deployment by seeing the *Scan History* page.

On any page of the Web interface, click the **Administration** tab. On the *Administration* page, click the **view** link for *Scan History*.

The interface displays the *Scan History* page, which lists all scans, plus the total number of scanned assets, discovered vulnerabilities, and other information pertaining to each scan. You can click the date link in the *Completed* column to view details about any scan.

You can download the log for any scan as discussed in the preceding topic.



Viewing scan history

Assess

After you discover all the assets and vulnerabilities in your environment, it is important to parse this information to determine what the major security threats are, such as high-risk assets, vulnerabilities, potential malware exposures, or policy violations.

Assess gives you guidance on viewing and sorting your scan results to determine your security priorities. It includes the following sections:

Locating and working with assets on page 240: There are several ways to drill down through scan results to find specific assets. For example, you can find all assets that run a particular operating system or that belong to a certain site. This section covers these different paths. It also discusses how to sort asset data by different security metrics and how to look at the detailed information about each asset.

Working with vulnerabilities on page 265: Depending on your environment, your scans may discover thousands of vulnerabilities. This section shows you how to sort vulnerabilities based on various security metrics, affected assets, and other criteria, so that you can find the threats that require immediate attention. The section also covers how to exclude vulnerabilities from reports and risk score calculations.

Working with Policy Manager results on page 297: If you work for a U.S. government agency or a vendor that transacts business with the government, you may be running scans to verify that your assets comply with United States Government Configuration Baseline (USGCB) or Federal Desktop Core Configuration (FDCC) policies. Or you may be testing assets for compliance with customized policies based on USGCB or FDCC policies. This section shows you how to track your overall compliance, view scan results for policies and the specific rules that make up those policies, and override rule results.

Locating and working with assets

By viewing and sorting asset information based on scans, you can perform quick assessments of your environment and any security issues affecting it.

Tip: While it is easy to view information about scanned assets, it is a best practice to create asset groups to control which users can see which asset information in your organization. See *Using asset groups to your advantage* on page 315.

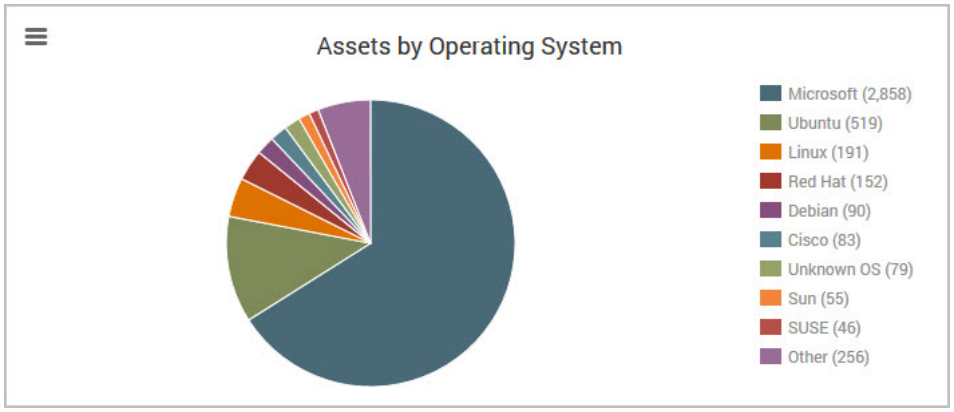
You can view all discovered assets that you have access to by simply clicking the **Assets** tab and viewing the *Assets* table on the *Assets* page.

Viewing asset counts and statistics

The number of all discovered assets to which you have access appears at the top of the page, as well as the number of sites, asset groups, and tagged assets to which you have access.

Note: If you are using a Dynamic Discovery connection, such as mobile, AWS, VMware, or DHCP, the total asset count includes assets that have been discovered as well as those that have been assessed.

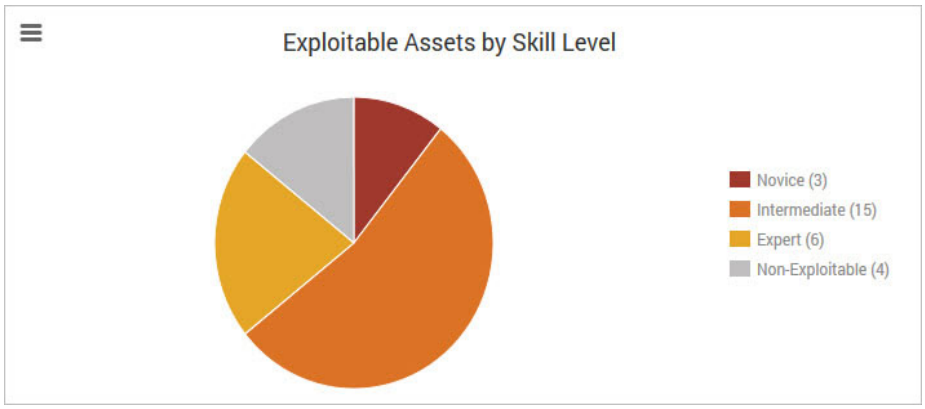
Also near the top of the page are pie charts displaying aggregated information about the assets in the *Assets* table below. With these charts, you can see an overview of your vulnerability status as well as interact with that data to help prioritize your remediations.



Assets by Operating System

The *Assets by Operating System* chart shows how many assets are running each operating system. You can mouse over each section for a count and percentage of each operating system.

You can also click on a section to drill down to a more detailed breakdown of that category. For more information on this functionality, see *Locating assets by operating systems* on page 246.

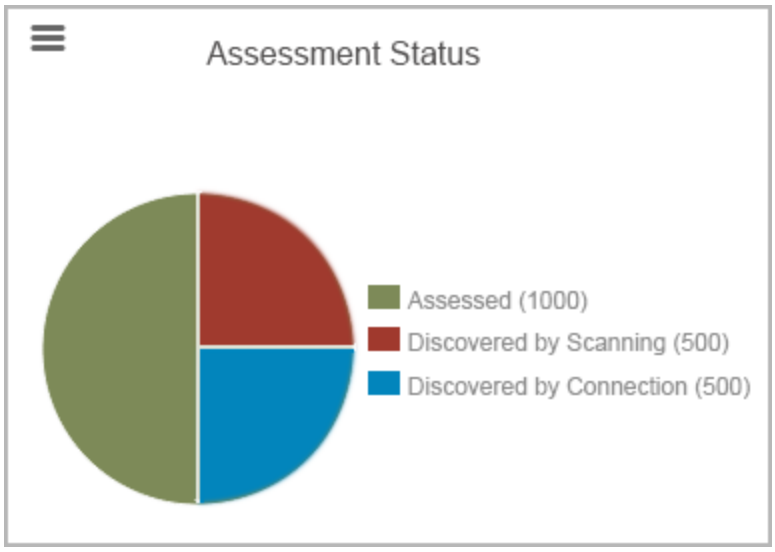


Exploitable Assets by Skill Level

On the *Exploitable Assets by Skill Level* chart, your assets with exploitable vulnerabilities are classified according to skill level required for exploits. Novice-level assets are the easiest to exploit, and therefore the ones you want to address most urgently. Assets are not counted more than once, but are categorized according to the most exploitable vulnerability on the asset. For example, if an asset has a Novice-level vulnerability, two Intermediate-level vulnerabilities, and one Expert-level vulnerability, that asset will fall into the Novice category. Assets without any known exploits appear in the Non-Exploitable slice.

Note: A similar pie chart appears on the *Vulnerabilities* page, but that one classifies the individual vulnerabilities rather than the assets. For more information, see *Working with vulnerabilities* on page 265.

A third pie chart shows the numbers of assets that have been *assessed* for vulnerabilities and policy compliance as well as those that have been discovered and not yet assessed, either by scan or Dynamic Discovery connection.



Assessment status

Comparing scanned and discovered assets

If you use Dynamic Discovery (see *Managing dynamic discovery of assets* on page 157), the *Assets* page displays two separate asset tables.

One lists assets that have been *scanned*.

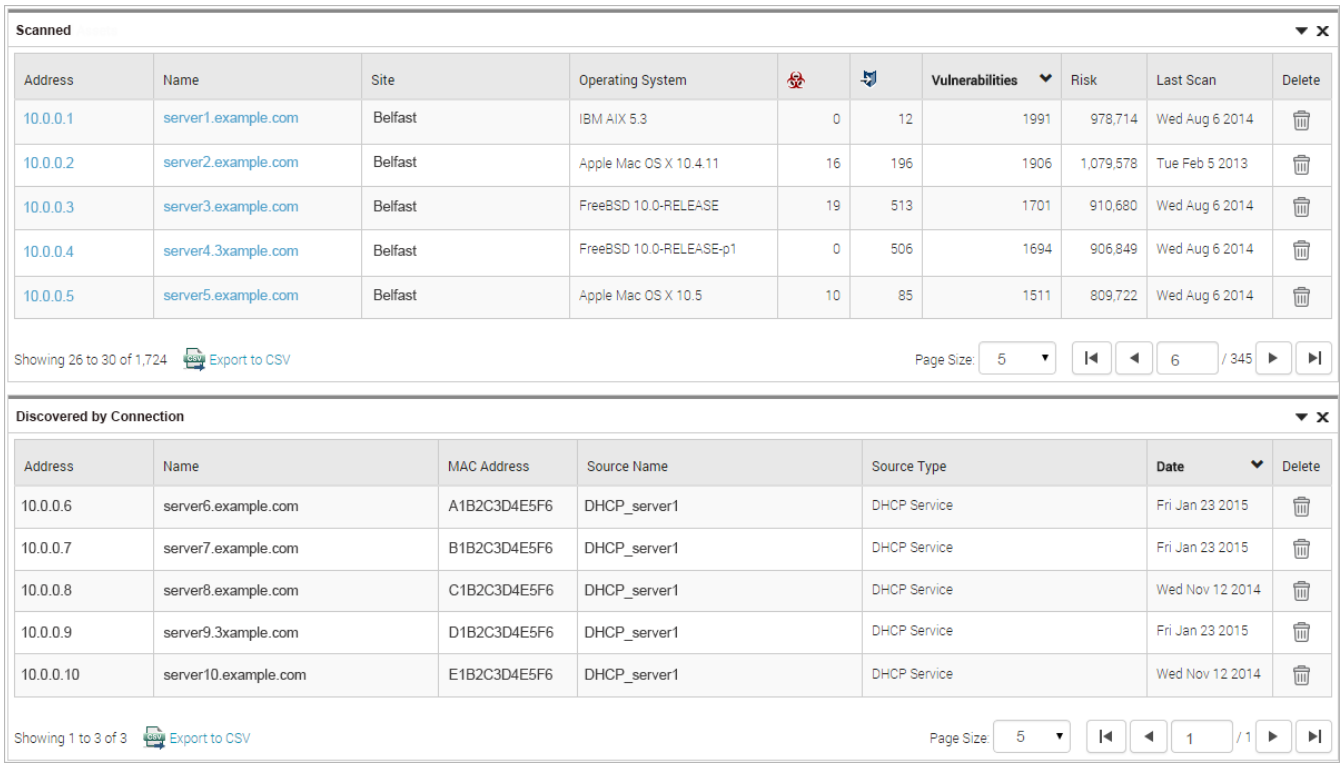
The other table lists assets that have been *discovered* through a Dynamic Discovery connection. These latter assets have yet to be scanned for vulnerabilities or policy compliance. After any of these latter assets are scanned for the first time, they are removed from the *Discovered by Connection* table and displayed in the *Scanned* table.

Note: IP addresses are not listed for mobile devices. Instead the column displays the value *Mobile device* for each of these assets.

If you have created at least one discovery connection but you have not initiated a connection to actually discover assets, the *Discovered by Connection* appears with no assets listed.

Viewing assets that have been discovered but not yet assessed is a good way to expose areas in your environment that may have unknown security issues.

Note: The *Discovered by Connection* table does not list assets that have been scanned with a discovery scan. Those assets appear in the *Scanned* table.



Scanned

Address	Name	Site	Operating System			Vulnerabilities	Risk	Last Scan	Delete
10.0.0.1	server1.example.com	Belfast	IBM AIX 5.3	0	12	1991	978,714	Wed Aug 6 2014	
10.0.0.2	server2.example.com	Belfast	Apple Mac OS X 10.4.11	16	196	1906	1,079,578	Tue Feb 5 2013	
10.0.0.3	server3.example.com	Belfast	FreeBSD 10.0-RELEASE	19	513	1701	910,680	Wed Aug 6 2014	
10.0.0.4	server4.3xample.com	Belfast	FreeBSD 10.0-RELEASE-p1	0	506	1694	906,849	Wed Aug 6 2014	
10.0.0.5	server5.example.com	Belfast	Apple Mac OS X 10.5	10	85	1511	809,722	Wed Aug 6 2014	

Showing 26 to 30 of 1,724 Export to CSV Page Size: 5 6 / 345

Discovered by Connection

Address	Name	MAC Address	Source Name	Source Type	Date	Delete
10.0.0.6	server6.example.com	A1B2C3D4E5F6	DHCP_server1	DHCP Service	Fri Jan 23 2015	
10.0.0.7	server7.example.com	B1B2C3D4E5F6	DHCP_server1	DHCP Service	Fri Jan 23 2015	
10.0.0.8	server8.example.com	C1B2C3D4E5F6	DHCP_server1	DHCP Service	Wed Nov 12 2014	
10.0.0.9	server9.3xample.com	D1B2C3D4E5F6	DHCP_server1	DHCP Service	Fri Jan 23 2015	
10.0.0.10	server10.example.com	E1B2C3D4E5F6	DHCP_server1	DHCP Service	Wed Nov 12 2014	

Showing 1 to 3 of 3 Export to CSV Page Size: 5 1 / 1

The assets tables

You can sort assets in the *Assets* table by clicking a row heading for any of the columns. For example, click the top row of the *Risk* column to sort numerically by the total risk score for all vulnerabilities discovered on each asset.

You can generate a comma-separated values (CSV) file of the asset kit list to share with others in your organization. Click the **Export to CSV** . Depending on your browser settings, you will see a pop-up window with options to save the file or open it in a compatible program.

You can control the number of assets that appear in each table by selecting a value in the *Rows per page* dropdown list in the bottom, right frame of the table. Use the navigation options in that area to view more asset records.

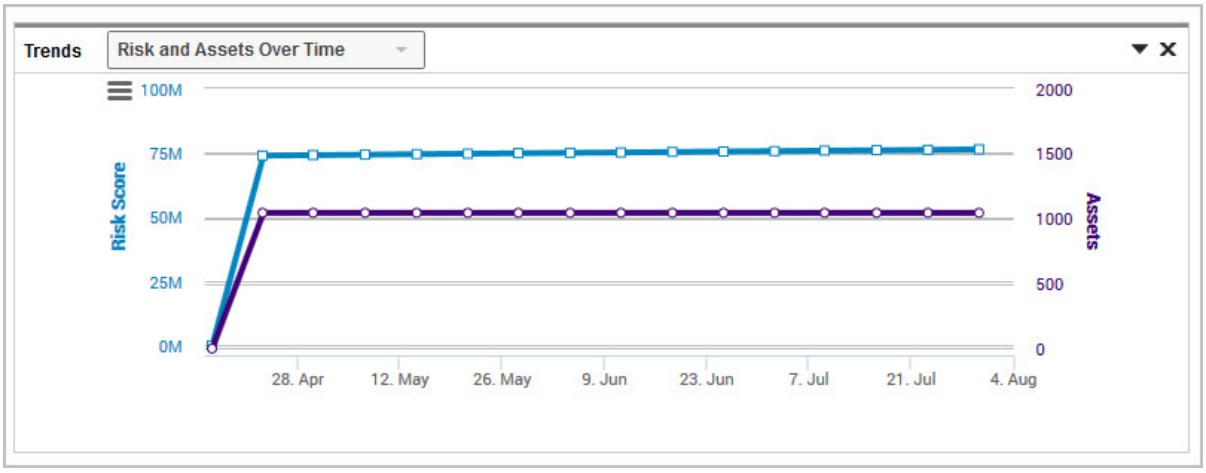
Locating assets by sites

To view assets by sites to which they have been assigned, click the hyperlinked number of sites displayed at the top of the *Assets page*. The Security Console displays the *Sites* page. From this page you can create a new site.

Charts and graphs at the top of the *Sites* page provide a statistical overview of sites, including risks and vulnerabilities.

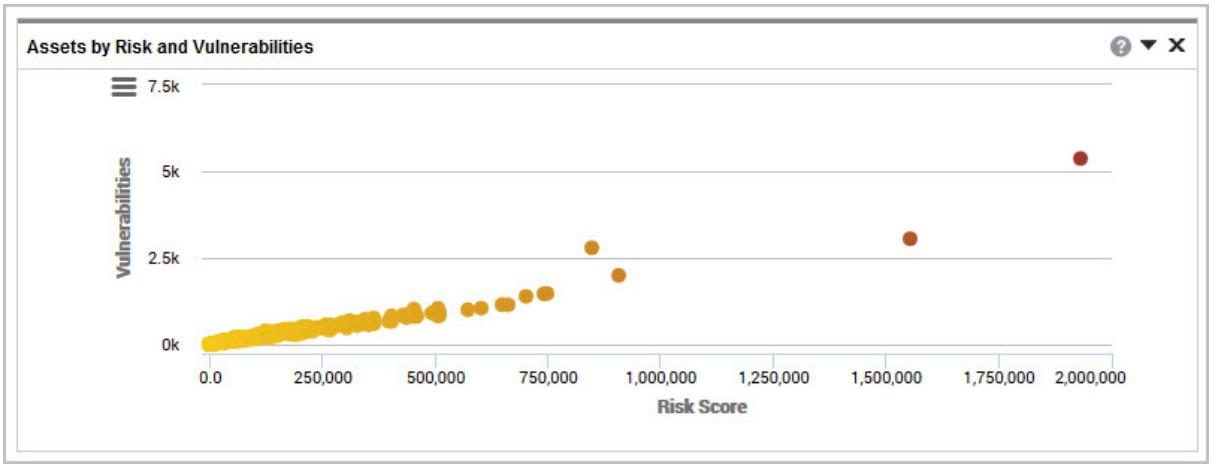
If a scan is in progress for any site, a column labeled *Scan Status* appears in the table. To view information about that scan, click the **Scan in progress** link. If no scans are in progress, a column labeled *Last Scan* appears in the table. Click the date link in the *Last Scan* column for any site to view information about the most recently completed scan for that site.

Click the link for any site in the *Site Listing* pane to view its assets. The Security Console displays a page for that site, including recent scan information, statistical charts and graphs.



Site Summary trend chart

The *Site Summary* page displays trending chart as well as a scatter plot. The default selection for the trend chart matches the *Home* page – risk and assets over time. You can also use the drop down menu to choose to view **Vulnerabilities over time** for this site. This vulnerabilities chart will populate with data starting from the time that you installed the August 6, 2014 product update. If you recently installed the update, the chart will show limited data now, but additional data will be gathered and displayed over time.



Assets by Risk and Vulnerabilities

The scatter plot chart permits you to easily spot outliers so you can spot assets that have above average risk. Assets with the highest amount of risk and vulnerabilities will appear outside of the cluster. The position and colors also indicate the risk associated with the asset by the asset's risk score - the further to the right and redder the color, the higher the risk. You can take action by selecting an asset directly from the chart, which will transfer you to the asset level view.

If a site has more 7,000 assets, a bubble chart view first appears which allows you to select a group of assets to then refine your view by selecting a bubble and showing the scatter plot for that bubble.

The *Assets* table shows the name and IP address of every scanned asset. If your site includes IPv4 and IPv6 addresses, the *Address* column groups these addresses separately. You can change the order of appearance for these address groups by clicking the sorting icon in the *Address* column.

Note: IP addresses are not listed for mobile devices. Instead the column displays the value *Mobile device* for each of these assets.

In the *Assets* table, you can view important security-related information about each asset to help you prioritize remediation projects: the number of available exploits, the number of vulnerabilities, and the risk score.

You will see an exploit count of 0 for assets that were scanned prior to the January 29, 2010, release, which includes the Exploit Exposure feature. This does not necessarily mean that these assets do not have any available exploits. It means that they were scanned before the feature was available. For more information, see *Using Exploit Exposure* on page 681.

From the details page of an asset, you can manage site assets and create site-level reports. You also can start a scan for that asset.

To view information about an asset listed in the *Assets* table, click the link for that asset. See *Viewing the details about an asset* on page 248.

Locating assets by asset groups

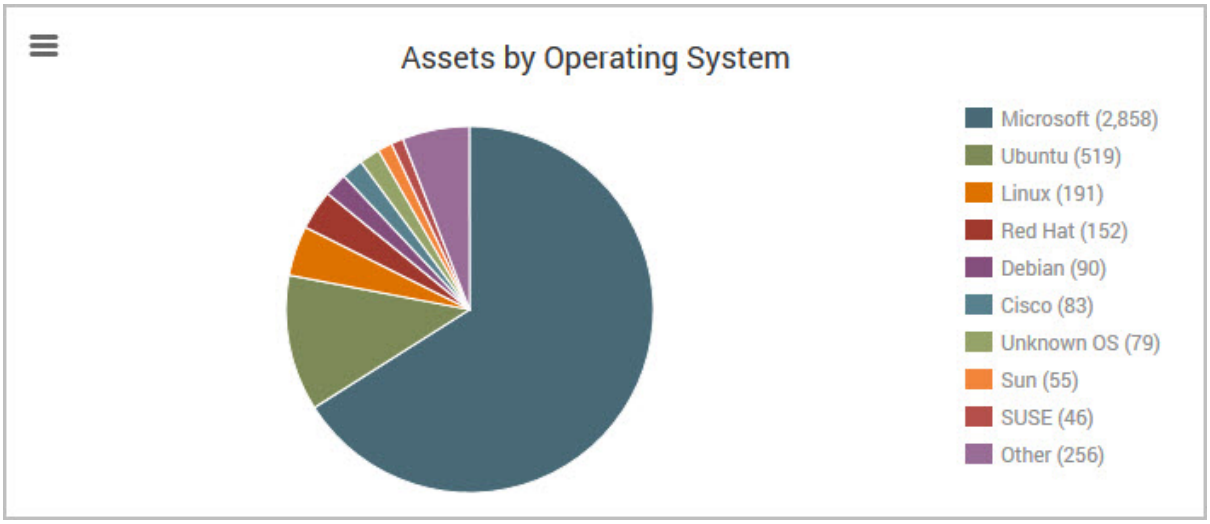
To view assets by asset groups in which they are included, click the hyperlinked number of asset groups displayed at the top of the *Assets page*. The Security Console displays the *Asset Groups* page.

Charts and graphs at the top of the *Asset Groups* page provide a statistical overview of asset groups, including risks and vulnerabilities. From this page you can create a new asset group. See *Using asset groups to your advantage* on page 315.

Click the link for any group in the *Scanned* table to view its assets. The Security Console displays a page for that asset group, including statistical charts and graphs and a list of assets. In the *Assets* pane, you can view the scan, risk, and vulnerability information about any asset. You can click a link for the site to which the asset belongs to view information about the site. You also can click the link for any asset address to view information about it. See *Viewing the details about an asset* on page 248.

Locating assets by operating systems

To view assets by the operating systems running on them, see the *Assets by Operating System* chart or table on the *Assets* page.



Assets by Operating System

The *Assets by Operating System* pie chart offers drill down functionality, meaning you can select an operating system to view a further breakdown of the category selected. For example, if Microsoft is selected for the OS you will then see a listing of all Windows OS versions present, such as Windows Server 2008, Windows Server 2012, and so on. Continuing to click on wedges further breaks down the systems to specific editions and service packs, if applicable. A large number of unknowns in your chart indicates that those assets were not fingerprinted successfully and should be investigated.

Note: If your assets have more than 10 types of operating systems, the chart shows the nine most frequently found operating systems, and an **Other** category. Click the **Other** wedge to see the remaining operating systems.

The *Assets by Operating System* table lists all the operating systems running in your network and the number of instances of each operating system. Click the link for an operating system to view the assets that are running it.The Security Console displays a page that lists all the assets running that operating system. You can view scan, risk, and vulnerability information about any asset. You can click a link for the site to which the asset belongs to view information about the site. You also can click the link for any asset address to view information about it. See *Viewing the details about an asset* on page 248.

Locating assets by software

To view assets by the software running on them, see the *Software Listing* table on the *Assets* page. The table lists any software that the application found running in your network, the number of instances of program, and the type of program.

The application only lists software for which it has credentials to scan. An exception to this would be when it discovers a vulnerability that permits root/admin access.

Click the link for a program to view the assets that are running it.

The Security Console displays a page that lists all the assets running that program. You can view scan, risk, and vulnerability information about any asset. You can click a link for the site to which the asset belongs to view information about the site. You also can click the link for any asset address or name to view information about it. See *Viewing the details about an asset* on page 248.

Locating assets by services

To view assets by the services they are running, see the *Service Listing* table on the *Assets* page. The table lists all the services running in your network and the number of the number of instances of each service. Click the link for a service to view the assets that are running it. See *Viewing the details about an asset* on page 248.

Viewing the details about an asset

Regardless of how you locate an asset, you can find out more information about it by clicking its name or IP address.

The Security Console displays a page for each asset determined to be unique. Upon discovering a live asset, Nexpose uses correlation heuristics to identify whether the asset is unique within the site. Factors considered include:

- MAC address(es)
- host name(s)
- IP address
- virtual machine ID (if applicable)

On the page for a discovered asset, you can view or add business context tags associated with that asset. For more information and instructions, see *Applying RealContext with tags* on page 254.

The asset *Trend* chart gives you the ability to view risk or vulnerabilities over time for this specific asset. Use the drop-down list to switch the view to risk or vulnerabilities.

You can view the *Vulnerability Listing* table for any reported vulnerabilities and any vulnerabilities excluded from reports. The table lists any exploits or malware kits associated with vulnerabilities to help you prioritize remediation based on these exposures.

Additionally, the table displays a special icon for any vulnerability that has been validated with an exploit. If a vulnerability has been validated with an exploit via a Metasploit module, the column displays the  icon. If a vulnerability has been validated with an exploit published in the Exploit Database, the column displays the  icon. For more information, see *Working with validated vulnerabilities* on page 276.

You can also view information about software, services, policy listings, databases, files, and directories on that asset as discovered by the application. You can view any users or groups associated with the asset.

The *Addresses* field in the *Asset Properties* pane displays all addresses (separated by commas) that have been discovered for the asset. This may include addresses that have not been scanned. For example: A given asset may have an IPv4 address and an IPv6 address. When configuring scan targets for your site, you may have only been aware of the IPv4 address, so you included only that address to be scanned in the site configuration. Viewing the discovered IPv6 address on the asset page allows you to include it for future scans, increasing your security coverage.

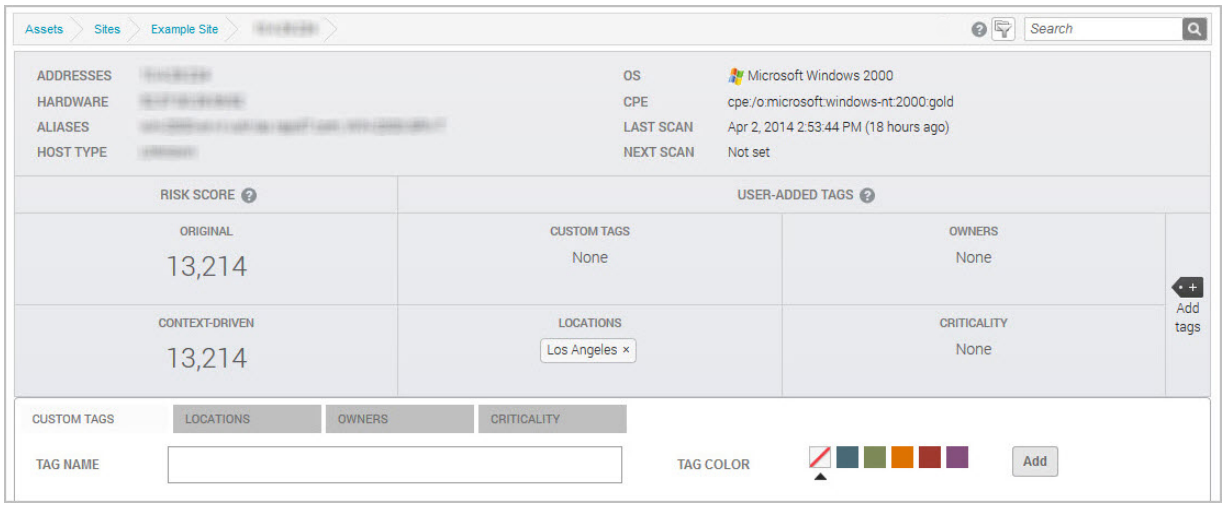
You can view any asset *fingerprints*. Fingerprinting is a set of methods by which the application identifies as many details about the asset as possible. By inspecting properties such as the specific bit settings in reserved areas of a buffer, the timing of a response, or a unique acknowledgement interchange, it can identify indicators about the asset's hardware and operating system.

In the *Asset Properties* table, you can run a scan or create a report for the asset.

In the *Vulnerability Listing* table, you can open a ticket for tracking the remediation of the vulnerabilities. See *Using tickets* on page 569. For more information about the *Vulnerabilities Listing* table and how you can use it, see *Viewing active vulnerabilities* on page 265 and *Working with vulnerability exceptions* on page 279. The table lists different security metrics, such as CVSS rating, risk score, vulnerability publication date, and severity rating. You can sort vulnerabilities according to any of these metrics by clicking the column headings. Doing so allows you to order vulnerabilities according to these different metrics and get a quick view of your security posture and priorities.

If you have scanned the asset with Policy Manager Checks, you can view the results of those checks in the *Policy Listing* table. If you click the name of any listed policy, you can view more information about it, such as other assets that were tested against that policy or the results of compliance checks for individual rules that make up the policy. For more information, see *Working with Policy Manager results* on page 297.

If you have scanned the asset with standard policy checks, such as for Oracle or Lotus Domino, you can review the results of those checks in the *Standard Policy Listing* table.



The page for a specific asset

Deleting assets

You may want to delete assets for one of several reasons:

- Assets may no longer be active in your network.
- Assets may have dynamic IP addresses that are constantly changing. If a scan on a particular date "rediscovered" these assets, you may want to delete assets scanned on that date.
- Network misconfigurations result in higher asset counts. If results from a scan on a particular date reflect misconfigurations, you may want to delete assets scanned on that date.

If any of the preceding situations apply to your environment, a best practice is to create a dynamic asset group based on a scan date. See *Working with asset groups* on page 315. Then you can locate the assets in that group using the steps described in *Locating and working with assets* on page 240. Using the bulk asset deletion feature described in this topic, you can delete multiple inactive assets in one step.

If you delete an asset from a site, it will no longer be included in the site or any asset groups in which it was previously included. If you delete an asset from an asset group, it will also be deleted from the site that contained it, as well as any other asset groups in which it was previously included. The deleted asset will no longer appear in the Web interface or reports other than historical reports, such as trend reports. If the asset is rediscovered in a future scan it will be regarded in the Web interface and future reports as a new asset.

Note: *Deleting* an asset from an asset group is different from *removing* an asset from an asset group. The latter is performed in asset group management. See *Working with asset groups* on page 315.

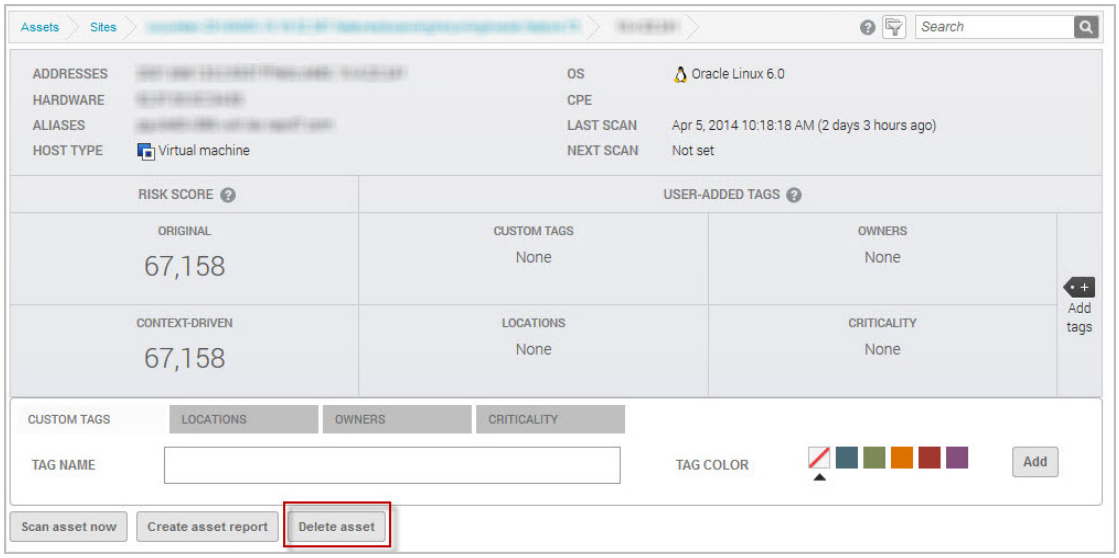
You can only delete assets in sites or asset groups to which you have access.

To delete individual assets that you locate by using the *site* or *asset group* drill-down described in *Locating and working with assets* on page 240, take the following steps:

1. After locating assets you want to delete, select the row for each asset in the *Assets* table.
2. Click **Delete Assets**.

To delete individual assets that you are viewing by using the drill-down described in *Viewing the details about an asset* on page 248, take the following steps:

1. After locating assets you want to delete, click the row for the asset in the *Assets* table to go to the Asset Details page.
2. Click **Delete Assets**.



Deleting an individual asset from the asset details page.

To delete all the displayed assets that you locate by using the *site* or *asset group* drill-down, take the following steps:

1. After locating assets you want to delete, click the top row in the *Assets* table.
2. Click **Select Visible** in the pop-up that appears. This step selects all of the assets *currently displayed* in the table.
3. Click **Delete Assets**.

   To cancel your selection, click the top row in the *Assets* table. Then click **Clear All** in the pop-up that appears.

Note: This procedure deletes only the assets displayed in the table, not all the assets in the site or asset group. For example, if a site contains 100 assets, but your table is configured to display 25, you can only select those 25 at one time. You will need repeat this procedure or increase the number of assets that the table displays to select all assets. The *Total Assets Selected* field on the right side of the table indicates how many assets are contained in the site or asset group.



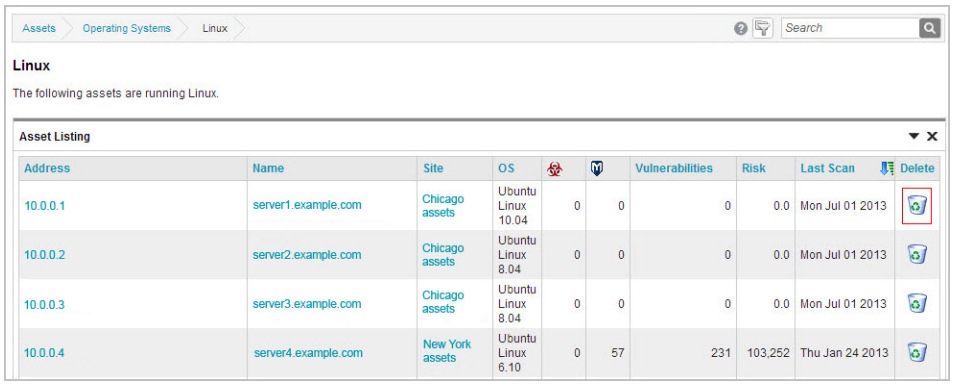
Deleting multiple assets in one step

To delete assets that you locate by using the *Asset, Operating System*, *Software*, or *Service* listing table as described in the preceding section, take the following step.

1. After locating assets you want to delete, click the **Delete** icon for each asset.

This action deletes an asset and all of its related data (including vulnerabilities) from any site or asset group to which it belongs, as well as from any reports in which it is included.

Note: Bulk asset deletion is not currently available for *Assets* tables that you locate using *operating system*, *software*, *service*, or *all-assets* drill-downs.



Deleting assets located via the operating system drill-down

Removing vs. deleting assets at the site level

If you are globally linking matching assets across all sites (see *Linking assets across sites* on page 672), you also have the option to *remove* an asset from a site, which breaks the link between the site and the asset. Unlike a deleted asset, the removed asset is still available in other sites in which is it was already present. However, if the asset is only in one site, it will be deleted from the entire workspace.



The option to remove assets from a site

Applying RealContext with tags

When tracking assets in your organization, you may want to identify, group, and report on them according to how they impact your business.

For example, you have a server with sensitive financial data and a number of workstations in your accounting office located in Cleveland, Ohio. The accounting department recently added three new staff members. Their workstations have just come online and will require a number of security patches right away. You want to assign the security-related maintenance of these accounting assets to different IT administrators: A SQL and Linux expert is responsible for the server, and a Windows administrator handles the workstations. You want to make these administrators aware that these assets have high priority.

These assets are of significant importance to your organization. If they were attacked, your business operations could be disrupted or even halted. The loss or corruption of their data could be catastrophic.

The scan data distinguishes these assets by their IP addresses, vulnerability counts, risk scores, and installed operating systems and services. It does not isolate them according to the unique business conditions described in the preceding scenario.

Using a feature called *RealContext*, you can apply *tags* to these assets to do just that. Your can tag all of these accounting assets with a *Cleveland* location and a *Very High* criticality level. You can tag your accounting server with a label, *Financials*, and assign it an owner named *Chris*, who is a Linux administrator with SQL expertise. You can assign your Windows workstations to a Windows administrator owner named *Brett*. And you can tag the new workstations with the label *First-quarter hires*. Then, you can create dynamic asset groups based on these tags and send reports on the tagged assets to Chris and Brett, so that they know that the workstation assets should be prioritized for remediation. For information on using tag-related search filters to create dynamic asset groups, see *Performing filtered asset searches* on page 324.

You also can use tags as filters for report scope. See *Creating a basic report* on page 356.

Types of tags

You can use several built-in tags:

- You can tag and track assets according to their geographic or physical *Locations*, such as data centers.
- You can associate assets with *Owners*, such as members of your IT or security team, who are in charge of administering them.
- You can apply levels of *Criticality* to assets to indicate their importance to your business or the negative impact resulting from an attack on them. A criticality level can be *Very Low*, *Low*, *Medium*, *High*, or *Very High*. Additionally, you can apply numeric values to criticality levels and use the numbers as multipliers that impact risk score. For more information, see *Adjusting risk with criticality* on page 665.

You can also create custom tags that allow you to isolate and track assets according to any context that might be meaningful to you. For example, you could tag certain assets *PCI*, *Web site back-end*, or *consultant laptops*.

Tagging assets, sites, and asset groups

You can tag an asset individually on the details page for that asset. You also can tag a site or an asset group, which would apply the tag to all member assets. The tagging workflow is identical, regardless of where you tag an asset:

1. If you are creating or editing a site: Go to the *General* page of the *Site Configuration* panel, and select **Add tags**.

   If you are creating or editing a static asset group: Go to the *General* page of the *Asset Group Configuration* panel, and select **Add tags**.

   If you are creating or editing a dynamic asset group: In the *Configuration* panel for the asset group, select **Add tags**.

   If you have just run a filtered asset search: To tag all of the search results, select **Add tags**, which appears above the search results table on the *Filtered Asset Search* page.

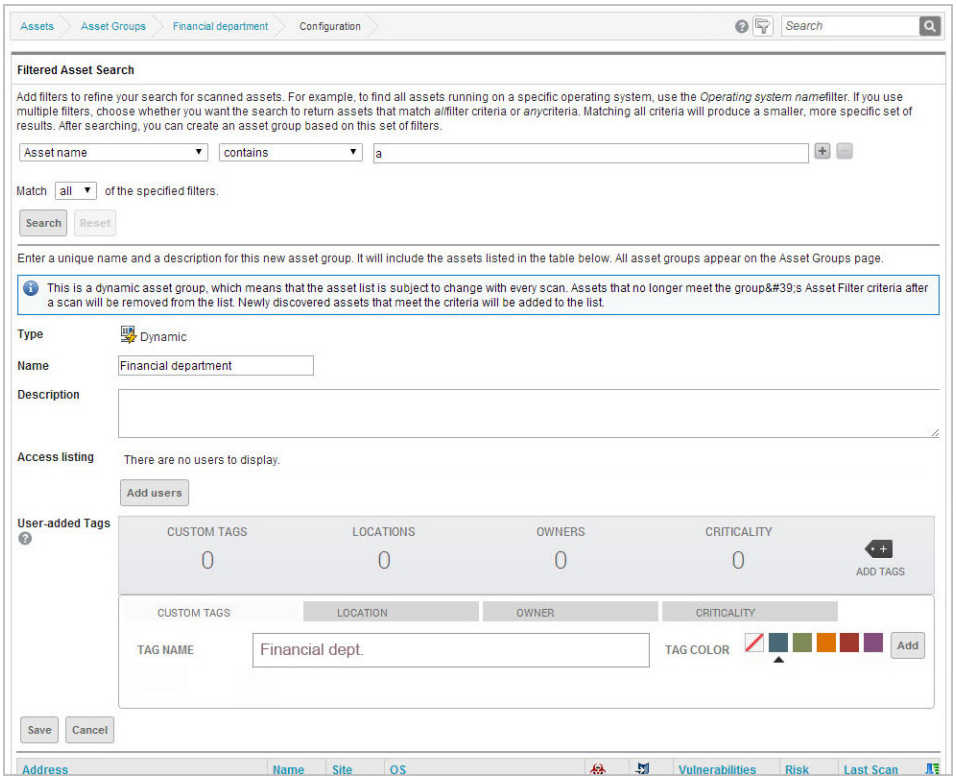
   The section for configuring tags expands.

2. Select a tag type.
3. If you select *Custom Tag*, *Location*, or *Owner*, type a new tag name to create a new tag. To add multiple names, type one name, press ENTER, type the next, press ENTER, and repeat as often as desired.

   OR

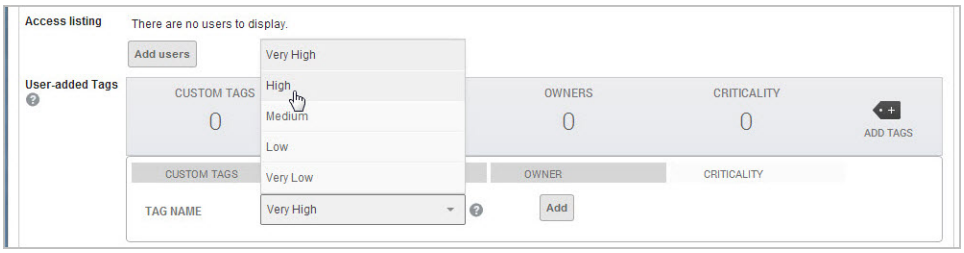
   To apply an previously created tag, start typing the name of the tag until the rest of the name fills in the text box.

   If you are creating a new custom tag, select a color in which the tag name will appear. All built-in tags have preset colors.



Creating a custom tag

If you select *Criticality*, select a criticality level from the drop-down list.



Applying a criticality level

4. Click **Add**.

   The tag name appears in a *User-added tags* panel.

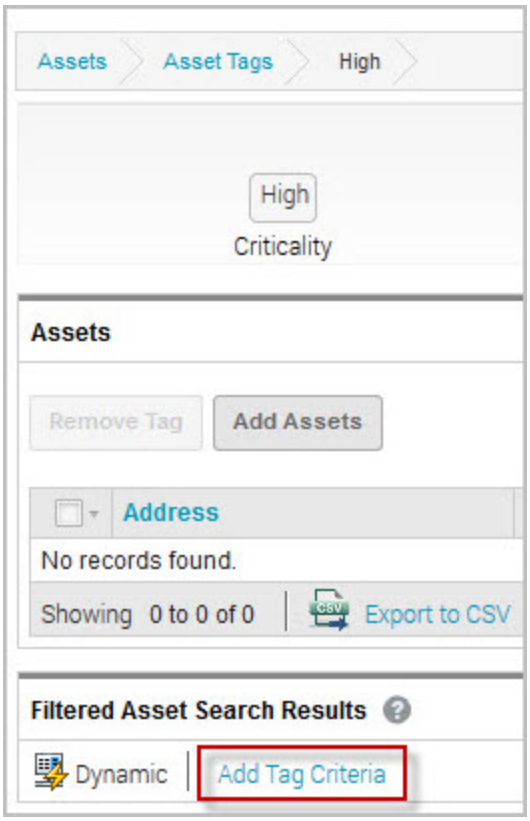
5. If you are creating or editing a site or asset group, click **Save** to save the configuration changes.

Applying business context with dynamic asset filters

Another way to apply tags is by specifying criteria for which tags can be dynamically applied. This allows you to apply business context based on filters without having to create new sites or groups. It also allows you to add new criteria for which assets should have the tags as you think of them, rather than at the time you first tag assets. For example, you may have searched for all your assets meeting certain Payment Card Industry (PCI) criteria and applied the *High* criticality level. Later, you decide you also want to filter for the Windows operating system. You can apply the additional filter on the page for the *High* criticality level itself.

To apply business context with dynamic asset filters:

1. Click the name of any tag to go to the details page for that tag.
2. Click **Add Tag Criteria**.
3. Select the search filters. The available filters are the same as those available in the asset search filters. See *Performing filtered asset searches* on page 324. There are some restrictions on which filters you can use with criticality tags. See *Filter restrictions for criticality tags* on page 259.
4. Select **Search**.
5. Select **Save**.



You can add criteria for when a tag will be dynamically applied

To view existing business context for a tag:

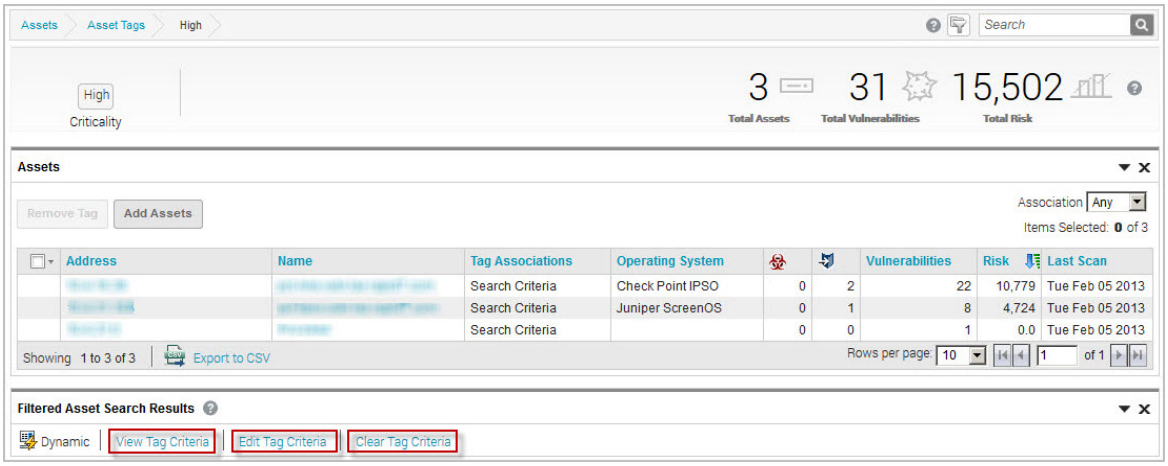
- On the details page for that tag, select **View Tag Criteria**.

To edit, add new, or remove dynamic asset filters for a tag:

1. Click the name of any tag to go to the details page for that tag.
2. Click **Edit Tag Criteria**.
3. Edit or add the search filters. The available filters are the same as those available in the asset search filters. See *Performing filtered asset searches* on page 324. There are some restrictions on which filters you can use with criticality tags. See *Filter restrictions for criticality tags* on page 259.
4. Select **Search**.
5. Select **Save**.

To remove all criteria for a tag:

- On the details page for that tag, select **Clear Tag Criteria**.



You can take different actions to view or modify rules for tags

Filter restrictions for criticality tags

Certain filters are restricted for criticality tags, in order to prevent circular references. These restrictions apply to criticality tags applied through tag criteria, and to those added through dynamic asset groups. See *Performing filtered asset searches* on page 324.

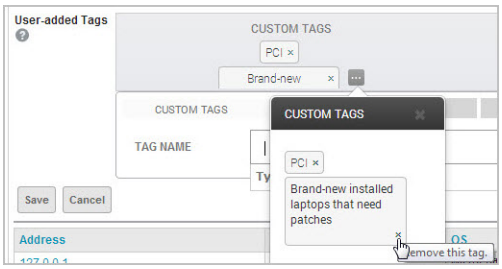
The following filters cannot be used with criticality tags:

- Asset risk score
- User-added criticality level
- User-added custom tag
- User-added tag (location)
- User-added tag (owner)

Removing and deleting tags

If a tag no longer accurately reflects the business context of an asset, you can remove it from that asset. To do so, click the **x** button next to the tag name. If the tag name is longer than one line, mouse over the ampersand below the name to expand it and then click the **x** button. Removing a tag is not the same as deleting it.

If you tag a site or an asset group, all of the member assets will "inherit" that tag. You cannot remove an inherited tag at the individual asset level. Instead, you will need to edit the site or asset group in which the tag was applied and remove it there.



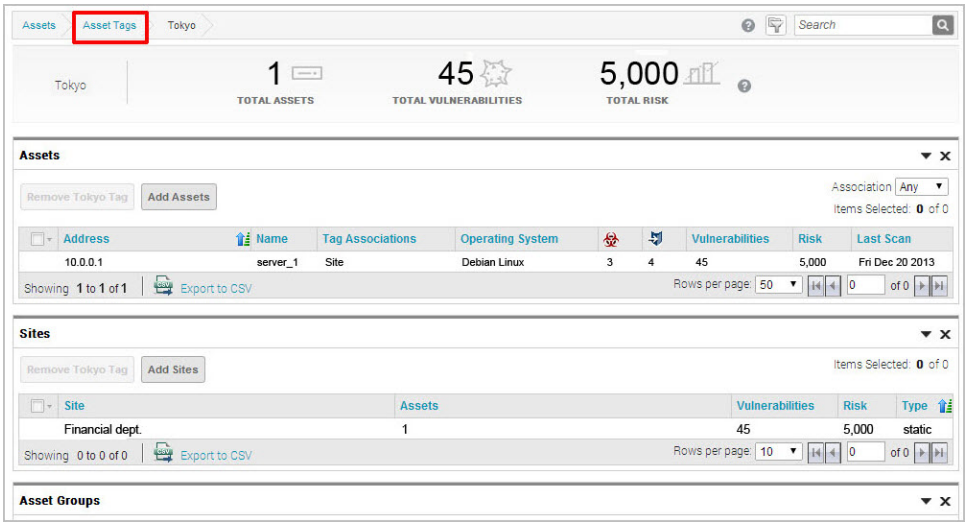
Expanding a tag name and then removing it

If a tag no longer has any business relevance at all, you can delete it completely.

Note: You cannot delete a criticality tag.

To delete a tag, go to the *Tags* page:

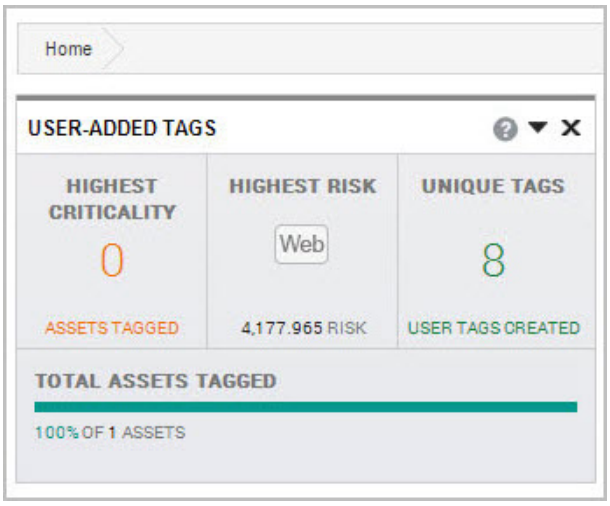
Click the name of any tag to go to the details page for that tag. Then click the *Asset Tags* breadcrumb.



Viewing the details page of a tag

OR

Click the number of unique tags displayed in the *User-Added Tags* pane on the *Home* page, even if the number is 0.



The User-added Tags pane on the Home page

Go to the *Asset Tag Listing* table of the *Tags* page. Select the check box for any tag you want to delete. To select all displayed tags, select the check box in the top row. Then, click **Delete**.

Tip: If you want to see which assets are associated with the tag before deleting it, click the tag name to view its details page. This could be helpful in case you want to apply a different tag to those assets.

Changing the criticality of an asset

Over time, the criticality of an asset may change. For example, a laptop may initially be used by a temporary worker and not contain sensitive data, which would indicate low criticality. That laptop may later be used by a senior executive and contain sensitive data, which would merit a higher criticality level.

Your options for changing an asset's criticality level depend on where the original criticality level was initially applied and where you are changing it:

- If you apply a criticality level to a site and then change the criticality of a member asset, you can only increase the criticality level. For example, if you apply a criticality level of *Medium* to a site and then change the criticality level of an individual member asset, you can only change the level to *High* or *Very High*.
- If you apply a criticality level to an asset group, and if any asset has had a criticality level applied elsewhere (in sites, other asset groups, or individually), the asset will retain the highest-applied criticality level. For example, an asset named *Server_1* belongs to a site named *Boston* with a criticality level of *Medium*. A criticality level of *Very High* is later applied to Server_1 individually. If you apply a *High* criticality level to a new asset group that includes Server_1, it will retain the *Very High* criticality level.
- If you apply a criticality level to an asset group, and if any asset has had a criticality level applied elsewhere (in sites, other asset groups, or individually), the asset will retain the highest-applied criticality level. For example, an asset named *Server_1* belongs to a site named *Boston* with a criticality level of *Medium*. A criticality level of *Very High* is later applied to Server_1 individually. If you apply a *High* criticality level to a new asset group that includes Server_1, it will retain the *Very High* criticality level.
- If you apply a criticality level to an individual asset, you can later change the criticality to any desired level.

Creating tags without applying them

You can create tags without immediately applying them to assets. This could be helpful if, for example, you want to establish a convention for how tag names are written.

1. Click the number of unique tags displayed in the *User-Added Tags* pane on the *Home* page, even if the number is 0.

   The Security Console displays the *Asset Tags* page, which lists all tags and displays useful information about assets to which they are applied.

2. Click **Add tags** and add any tags as described in *Tagging assets, sites, and asset groups* on page 255.

Avoiding "circular references" when tagging asset groups

You may apply the same tag to an asset as well as an asset group that contains it. For example, you might want to create a group based on assets tagged with a certain location or owner. This may occasionally lead to a circular reference loop in which tags refer to themselves instead of the assets or groups to which they were originally applied. This could prevent you from getting useful context from the tags.

The following example shows how a circular reference can occur with with location and custom tags:

1. A first user tags a number of assets with the location *Cleveland*.
2. The user creates a dynamic asset group called *Midwest office* with search results based on assets tagged *Cleveland*.
3. The user applies a custom tag named *Accounting* to the *Midwest office* asset group because all the assets in the group are used by the accounting team.
4. A second user, who is not aware of the *Midwest office* dynamic asset group or the *Cleveland* tag, creates a new dynamic asset group named *Financial* with search results based on the *Accounting* tag.
5. That user tags the *Financial* group with *Cleveland*, expecting that all assets in the group will inherit the tag. But because the assets were tagged *Cleveland* by the first user, the *Cleveland* tag now refers to itself in a potentially infinite loop.

The following example shows how a circular reference can occur with criticality:

1. You create a dynamic asset group *Priorities* for all assets that have an original risk score of less than 1,000. One of these assets is named *Server_1*.
2. You tag this group with a *Very High* criticality level, so that every asset in the group inherits the tag.
3. Your Security Console has been configured to double the risk score of assets with a *Very High* criticality level. See *Adjusting risk with criticality* on page 665.
4. *Server_1* has its risk score doubled, which causes it to no longer meet the filter criteria of *Priorities*. Therefore, it is removed from *Priorities*.
5. Since *Server_1* no longer inherits the *Very High* criticality level applied to *Priorities*, it reverts to its original risk score, which is lower than 1,000.
6. *Server_1* now once again meets the criteria for membership in *Priorities*, so it once again inherits the *Very High* criticality level applied to the asset group. This, again, causes its risk score to double, so that it no longer meets the criteria for membership in *Priorities*. This is a circular reference loop.

The best way to prevent circular references is to look at the *Tags* page to see what tags have been created. Then go to the details page for a tag that you are considering using and to see which assets, sites, and asset groups it is applied to. This is especially helpful if you have multiple Security Console users and high numbers of tags and asset groups. To access to the details page for a tag, simply click the tag name.

Working with vulnerabilities

Analyzing the vulnerabilities discovered in scans is a critical step in improving your security posture. By examining the frequency, affected assets, risk level, exploitability and other characteristics of a vulnerability, you can prioritize its remediation and manage your security resources effectively.

Every vulnerability discovered in the scanning process is added to vulnerability database. This extensive, full-text, searchable database also stores information on patches, downloadable fixes, and reference content about security weaknesses. The application keeps the database current through a subscription service that maintains and updates vulnerability definitions and links. It contacts this service for new information every six hours.

The database has been certified to be compatible with the MITRE Corporation's Common Vulnerabilities and Exposures (CVE) index, which standardizes the names of vulnerabilities across diverse security products and vendors. The index rates vulnerabilities according to MITRE's Common Vulnerabilities Scoring System (CVSS) Version 2.

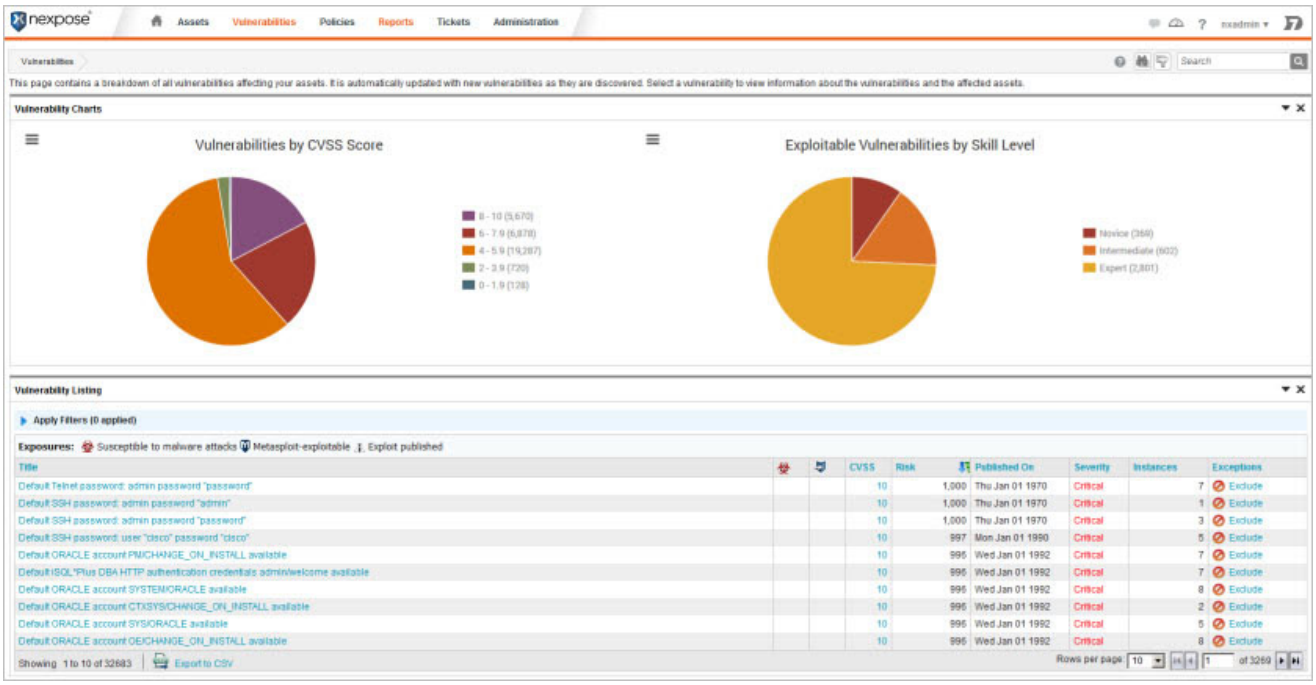
An application algorithm computes the CVSS score based on ease of exploit, remote execution capability, credentialed access requirement, and other criteria. The score, which ranges from 1.0 to 10.0, is used in Payment Card Industry (PCI) compliance testing. For more information about CVSS scoring, go to the FIRST Web site (http://www.first.org/cvss/cvss-guide.html).

Viewing active vulnerabilities

Viewing vulnerabilities and their risk scores helps you to prioritize remediation projects. You also can find out which vulnerabilities have exploits available, enabling you to verify those vulnerabilities. See *Using Exploit Exposure* on page 681.

Click the **Vulnerabilities** tab that appears on every page of the console interface.

The Security Console displays the *Vulnerabilities* page, which lists all the vulnerabilities for assets that the currently logged-on user is authorized to see, depending on that user's permissions. Since Global Administrators have access to all assets in your organization, they will see all the vulnerabilities in the database.



The Vulnerabilities page

The charts on the *Vulnerabilities* page display your vulnerabilities by CVSS score and exploitable skill levels. The *CVSS Score chart* displays how many of your vulnerabilities fall into each of the CVSS score ranges. This score is based on access complexity, required authentication, and impact on data. The score ranges from 1 to 10, with 10 being the worst, so you should prioritize the vulnerabilities with the higher numbers.

The *Exploitable Vulnerabilities by Skill Level* chart shows you your vulnerabilities categorized by the level of skill required to exploit them. The most easily exploitable vulnerabilities present the greatest threat, since there will be more people who possess the necessary skills, so you should prioritize remediating the Novice-level ones and work your way up to Expert.

You can change the sorting criteria by clicking any of the column headings in the *Vulnerability Listing* table.

The *Title* column lists the name of each vulnerability.

Two columns indicate whether each vulnerability exposes your assets to malware attacks or exploits. Sorting entries according to either of these criteria helps you to determine at a glance which vulnerabilities may require immediate attention because they increase the likelihood of compromise.

For each discovered vulnerability that has at least one malware kit (also known as an *exploit kit*) associated with it, the console displays a malware exposure icon . If you click the icon, the

console displays the *Threat Listing* pop-up window that lists all the malware kits that attackers can use to write and deploy malicious code for attacking your environment through the vulnerability. You can generate a comma-separated values (CSV) file of the malware kit list to share with others in your organization. Click the **Export to CSV** icon . Depending on your browser settings, you will see a pop-up window with options to save the file or open it in a compatible program.

You can also click the **Exploits** tab in the pop-up window to view published exploits for the vulnerability.

In the context of the application a *published* exploit is one that has been developed in Metasploit or listed in the Exploit Database (www.exploit-db.com).

For each discovered vulnerability with an associated exploit the console displays a exploit icon. If you click this icon the console displays the *Threat Listing* pop-up window that lists descriptions about all available exploits, their required skill levels, and their online sources. The Exploit Database is an archive of exploits and vulnerable software. If a Metasploit exploit is available, the console displays the ™ icon and a link to a Metasploit module that provides detailed exploit information and resources.

There are three levels of exploit skill: *Novice*, *Intermediate*, and *Expert*. These map to Metasploit's seven-level exploit ranking. For more information, see the Metasploit Framework page (http://www.metasploit.com/redmine/projects/framework/wiki/Exploit_Ranking).

- *Novice* maps to *Great* through *Excellent*.
- *Intermediate* maps to *Normal* through *Good*.
- *Expert* maps to *Manual* through *Low* through *Average*.

You can generate a comma-separated values (CSV) file of the exploit list and related data to share with others in your organization. Click the **Export to CSV** icon . Depending on your browser settings, you will see a pop-up window with options to save the file or open it in a compatible program.

You can also click the **Malware** tab in the pop-up window to view any malware kits that attackers can use to write and deploy malicious code for attacking your environment through the vulnerability.

The *CVSS Score* column lists the score for each vulnerability.

The *Published On* column lists the date when information about each vulnerability became available.

The *Risk* column lists the risk score that the application calculates, indicating the potential danger that each vulnerability poses to an attacker exploits it. The application provides two risk scoring models, which you can configure. See *Selecting a model for calculating risk scores* in the *administrator's guide*. The risk model you select controls the scores that appear in the *Risk* column. To learn more about risk scores and how they are calculated, see the PCI, CVSS, and risk scoring FAQs, which you can access in the *Support* page.

The application assigns each vulnerability a severity level, which is listed in the *Severity* column. The three severity levels–Critical, Severe, and Moderate–reflect how much risk a given vulnerability poses to your network security. The application uses various factors to rate severity, including CVSS scores, vulnerability age and prevalence, and whether exploits are available. See the PCI, CVSS, and risk scoring FAQs, which you can access in the *Support* page.

Note: The severity ranking in the *Severity* column is not related to the severity score in PCI reports.

1 to 3 = Moderate

4 to 7 = Severe

8 to 10 = Critical

The *Instances* column lists the total number of instances of that vulnerability in your site. If you click the link for the vulnerability name, you can view which specific assets are affected by the vulnerability. See *Viewing vulnerability details* on page 274.

You can click the icon in the *Exclude* column for any listed vulnerability to exclude that vulnerability from a report.

An administrative change to your network, such as new credentials, may change the level of access that an asset permits during its next scan. If the application previously discovered certain vulnerabilities because an asset permitted greater access, that vulnerability data will no longer be available due to diminished access. This may result in a lower number of reported vulnerabilities, even if no remediation has occurred. Using baseline comparison reports to list differences between scans may yield incorrect results or provide more information than necessary because of these changes. Make sure that your assets permit the highest level of access required for the scans you are running to prevent these problems.

The *Vulnerability Categories* and *Vulnerability Check Types* tables list all categories and check types that the Application *can* scan for. Your scan template configuration settings determine which categories or check types the application *will* scan for. To determine if your environment has a vulnerability belonging to one of the listed checks or types, click the appropriate link. The

Security Console displays a page listing all pertinent vulnerabilities. Click the link for any vulnerability to see its detail page, which lists any affected assets.

Filtering your view of vulnerabilities

Your scans may discover hundreds, or even thousands, of vulnerabilities, depending on the size of your scan environment. A high number of vulnerabilities displayed in the *Vulnerability Listing* table may make it difficult to assess and prioritize security issues. By filtering your view of vulnerabilities, you can reduce the sheer number of those displayed, and restrict the view to vulnerabilities that affect certain assets. For example, a Security Manager may only want to see vulnerabilities that affect assets in sites or asset groups that he or she manages. Or you can restrict the view to vulnerabilities that pose a greater threat to your organization, such as those with higher risk scores or CVSS rankings.

Working with filters and operators in vulnerability displays

Filtering your view of vulnerabilities involves selecting one or more filters, which are criteria for displaying specific vulnerabilities. For each filter you then select an operator, which controls how the filter is applied.

Site name is a filter for vulnerabilities that affect assets in specific sites. It works with the following operators:

- The *is* operator displays a drop-down list of site names. Click a name to display vulnerabilities that affect assets in that site. Using the SHIFT key, you can select multiple names.
- The *is not* operator displays a drop-down list of site names. Click a name to filter out vulnerabilities that affect assets in that site, so that they are not displayed. Using the SHIFT key, you can select multiple names.

Asset group name is a filter for vulnerabilities that affect assets in specific asset groups. It works with the following operators:

- The *is* operator displays a drop-down list of asset group names. Click a name to display vulnerabilities that affect assets in that asset group. Using the SHIFT key, you can select multiple names.
- The *is not* operator displays a drop-down list of asset group names. Click a name to filter out vulnerabilities that affect assets in that asset group, so that they are not displayed. Using the SHIFT key, you can select multiple names.

CVE ID is a filter for vulnerabilities based on the CVE ID. The CVE identifiers (IDs) are unique, common identifiers for publicly known information security vulnerabilities. For more information, see https://cve.mitre.org/cve/identifiers/index.html. The filter applies a search string to the CVE IDs, so that the search returns vulnerabilities that meet the specified criteria. It works with the following operators:

- *is* returns all vulnerabilities whose names match the search string exactly.
- *is not* returns all vulnerabilities whose names do not match the search string.
- *contains* returns all vulnerabilities whose names contain the search string anywhere in the name.
- *does not contain* returns all vulnerabilities whose names do not contain the search string.

After you select an operator, you type a search string for the CVE ID in the blank field.

CVSS score is a filter for vulnerabilities with specific CVSS rankings. It works with the following operators:

- The *is* operator displays all vulnerabilities that have a specified CVSS score.
- The *is not* operator displays all vulnerabilities that do not have a specified CVSS score.
- The *is in the range of* operator displays all vulnerabilities that fall within the range of two specified CVSS scores and include the high and low scores in the range.
- The *is higher than* operator displays all vulnerabilities that have a CVSS score higher than a specified score.
- The *is lower than* operator displays all vulnerabilities that have a CVSS score lower than a specified score.

After you select an operator, enter a score in the blank field. If you select the range operator, you would enter a low score and a high score to create the range. Acceptable values include any numeral from 0.0 to 10. You can only enter one digit to the right of the decimal. If you enter more than one digit, the score is automatically rounded up. For example, if you enter a score of 2.25, the score is automatically rounded up to 2.3.

Risk score is a filter for vulnerabilities with certain risk scores. It works with the following operators:

- The *is* operator displays all vulnerabilities that have a specified risk score.
- The *is not* operator displays all vulnerabilities that do not have a specified risk score.
- The *is in the range of* operator displays all vulnerabilities that fall within the range of two specified risk scores and include the high and low scores in the range.
- The *is higher than* operator displays all vulnerabilities that have a risk score higher than a specified score.
- The *is lower than* operator displays all vulnerabilities that have a risk score lower than a specified score.

After you select an operator, enter a score in the blank field. If you select the range operator, you would type a low score and a high score to create the range. Keep in mind your currently selected risk strategy when searching for assets based on risk scores. For example, if the currently selected strategy is Real Risk, you will not find assets with scores higher than 1,000. Learn about different risk score strategies. Refer to the risk scores in your vulnerability and asset tables for guidance.

Vulnerability category is a filter that lets you search for vulnerabilities based on the categories that have been flagged on them during scans. Lists of vulnerability categories can be found in the scan template configuration or the report configuration.

The filter applies a search string to vulnerability categories, so that the search returns a list of vulnerabilities that either are or are not in categories that match that search string. It works with the following operators:

- *contains* returns all vulnerabilities whose category contains the search string. You can use an asterisk (*) as a wildcard character.
- *does not contain* returns all vulnerabilities that do not have a vulnerability whose category contains the search string. You can use an asterisk (*) as a wildcard character.
- *is* returns all vulnerabilities whose category matches the search string exactly.
- *is not* returns all vulnerabilities that do not have a vulnerability whose category matches the exact search string.
- *starts with* returns all vulnerabilities whose categories begin with the same characters as the search string.
- *ends with* returns all vulnerabilities whose categories end with the same characters as the search string.

After you select an operator, you type a search string for the vulnerability category in the blank field.

Vulnerability title is a filter that lets you search vulnerabilities based on their titles.The filter applies a search string to vulnerability titles, so that the search returns a list of assets that either have or do not have the specified string in their titles. It works with the following operators:

- *contains* returns all vulnerabilities whose name contains the search string. You can use an asterisk (*) as a wildcard character.
- *does not contain* returns all vulnerabilities whose name does not contain the search string. You can use an asterisk (*) as a wildcard character.
- *is* returns all vulnerabilities whose name matches the search string exactly.
- *is not* returns all vulnerabilties whose names do not match the exact search string.
- *starts with* returns all vulnerabilities whose names begin with the same characters as the search string.
- *ends with* returns all vulnerabilities whose names end with the same characters as the search string.

After you select an operator, you type a search string for the vulnerability name in the blank field.

Note: You can only use each filter once. For example, you cannot select the *Site name* filter twice. If you want to specify more than one site name or asset name in the display criteria, use the **SHIFT** key to select multiple names when configuring the filter.

Applying vulnerability display filters

To apply vulnerability display filters, take the following steps:

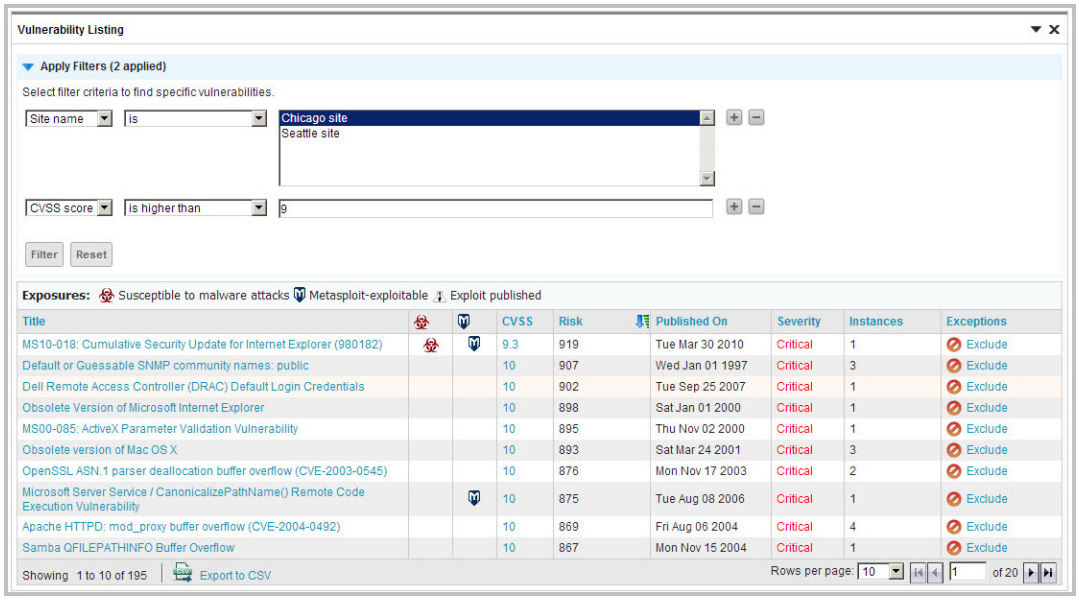
1. Click the **Vulnerabilities** tab of the Security Console Web interface.

   The Security Console displays the *Vulnerabilities* page.

2. In the *Vulnerability Listing* table, expand the section to **Apply Filters**.
3. Select a filter from the drop-down list.
4. Select an operator for the filter.
5. Enter or select a value based on the operator.
6. Use the + button to add filters. Repeat the steps for selecting the filter, operator, and value. Use the - button to remove filters.
7. Click **Filter**.

The Security Console displays vulnerabilities that meet *all* filter criteria in the table.

Currently, filters do not change the number of displayed instances for each vulnerability.

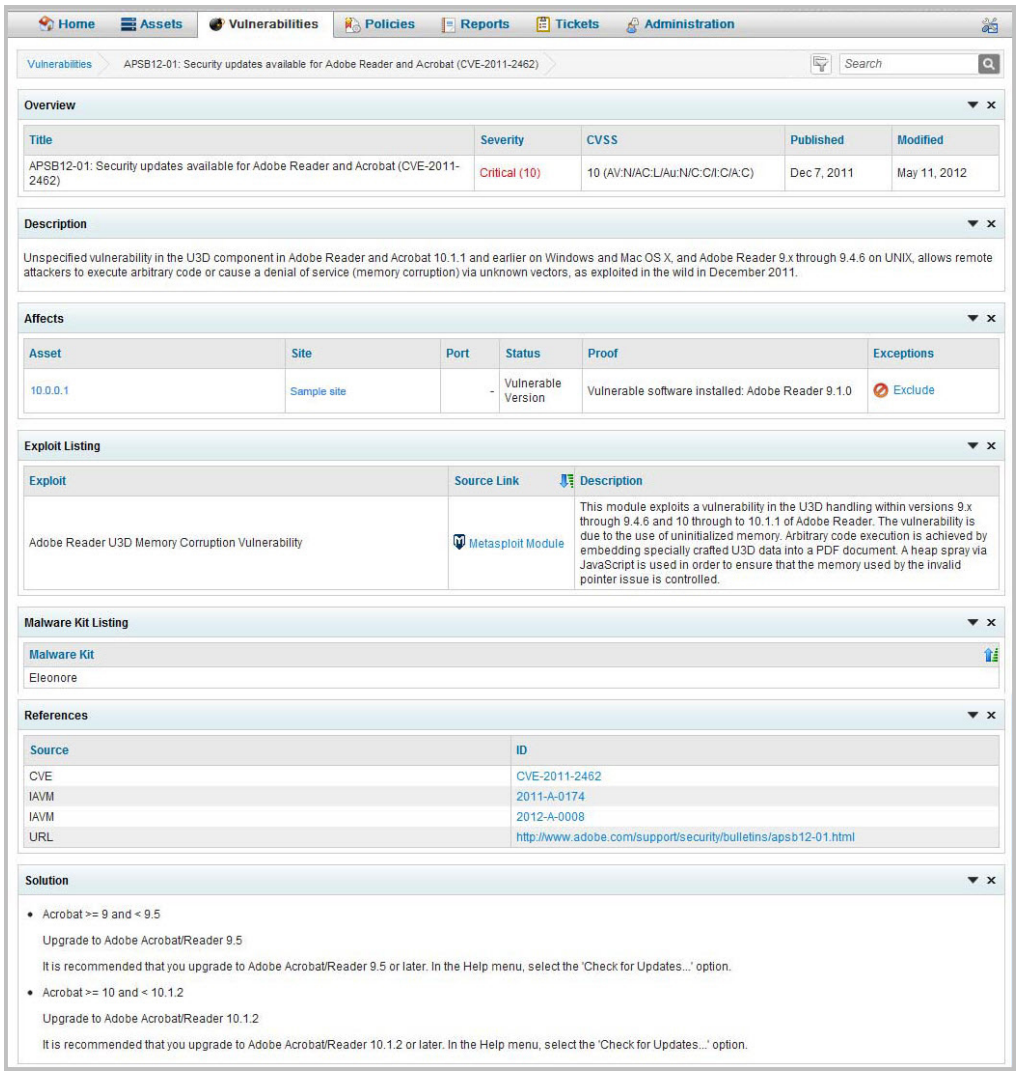


Filtering the display of vulnerabilities

Tip: You can export the filtered view of vulnerabilities as a comma-separated values (CSV) file to share with members of your security team. To do so, click the **Export to CSV** link at the bottom of the *Vulnerability Listing* table.

Viewing vulnerability details

Click the link for any vulnerability listed on the *Vulnerabilities* page to view information about it. The Security Console displays a page for that vulnerability.



The page for a specific vulnerability

At the top of the page is a description of the vulnerability, its severity level and CVSS rating, the date that information about the vulnerability was made publicly available, and the most recent date that Rapid7 modified information about the vulnerability, such as its remediation steps.

Below these items is a table listing each affected asset, port, and the site on which a scan reported the vulnerability. You can click on the link for the device name or address to view all of its vulnerabilities. On the device page, you can create a ticket for remediation. See *Using tickets* on page 569. You also can click the site link to view information about the site.

The *Port* column in the *Affected Assets* table lists the port that the application used to contact the affected service or software during the scan. The *Status* column lists a *Vulnerable* status for an asset if the application confirmed the vulnerability. It lists a *Vulnerable Version* status if the

application only detected that the asset is running a version of a particular program that is known to have the vulnerability.

The *Proof* column lists the method that the application used to detect the vulnerability on each asset. It uses exploitation methods typically associated with hackers, inspecting registry keys, banners, software version numbers, and other indicators of susceptibility.

The *Exploits* table lists descriptions of available exploits and their online sources. The Exploit Database is an archive of exploits and vulnerable software. If a Metasploit exploit is available, the console displays the ™ icon and a link to a Metasploit module that provides detailed exploit information and resources.

The *Malware* table lists any malware kit that attackers can use to write and deploy malicious code for attacking your environment through the vulnerability.

The *References* table, which appears below the *Affected Assets* pane, lists links to Web sites that provide comprehensive information about the vulnerability. At the very bottom of the page is the *Solution* pane, which lists remediation steps and links for downloading patches and fixes.

If you wish to query the database for a specific vulnerability, and you know its name, type all or part of the name in the **Search** box that appears on every page of the console interface, and click the magnifying glass icon. The console displays a page of search results organized by different categories, including vulnerabilities.

Working with validated vulnerabilities

There are many ways to sort and prioritize vulnerabilities for remediation. One way is to give higher priority to vulnerabilities that have been *validated*, or proven definitively to exist. The application uses a number of methods to flag vulnerabilities during scans, such as fingerprinting software versions known to be vulnerable. These methods provide varying degrees of certainty that a vulnerability exists. You can increase your certainty that a vulnerability exists by exploiting it, which involves deploying code that penetrates your network or gains access to a computer through that specific vulnerability.

As discussed in the topic *Viewing active vulnerabilities* on page 265, any vulnerability that has a published exploit associated with it is marked with a Metasploit or Exploit Database icon. You can integrate Rapid7 Metasploit as a tool for validating vulnerabilities discovered in scans and then have Nexpose indicate that these vulnerabilities have been validated on specific assets.

Note: Metasploit is the only exploit application that the vulnerability validation feature supports. See a tutorial for performing vulnerability validation with Metasploit.

To work in Nexposewith vulnerabilities that have been validated with Metasploit, take the following steps:

1. After performing exploits in Metasploit, click the **Assets** tab of the NexposeSecurity Console Web interface.
2. Locate an asset that you would like to see validated vulnerabilities for. See *Locating and working with assets* on page 240.
3. Double-click the asset's name or IP address.

   The Security Console displays the details page for the asset.

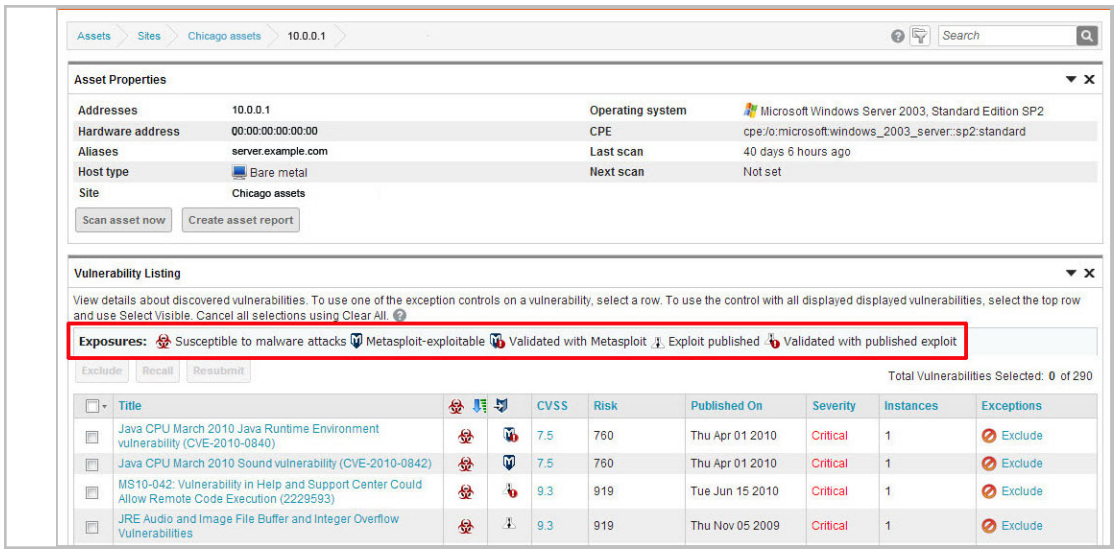
View the *Exploits* column ( ) in the *Vulnerability Listing* table.

4. If a vulnerability has been validated with an exploit via a Metasploit module, the column displays the icon.

   If a vulnerability has been validated with an exploit published in the Exploit Database, the column displays the icon.

5. To sort the vulnerabilities according to whether they have been validated, click the title row in the *Exploits* column.

   As seen in the following screen shot, the descending sort order for this column is 1) vulnerabilities that *have been* validated with a Metasploit exploit, 2) vulnerabilities that *can be* validated with a Metasploit exploit, 3) vulnerabilities that *have been* validated with an Exploit database exploit, 4) vulnerabilities that *can be* validated with an Exploit database exploit.



The asset details page with the Exposures legend highlighted

Working with vulnerability exceptions

All discovered vulnerabilities appear in the *Vulnerabilities Listing* table of the Security Console Web interface. Your organization can exclude certain vulnerabilities from appearing in reports or affecting risk scores.

Understanding cases for excluding vulnerabilities

There are several possible reasons for excluding vulnerabilities from reports.

Compensating controls: Network managers may mitigate the security risks of certain vulnerabilities, which, technically, could prevent their organization from being PCI compliant. It may be acceptable to exclude these vulnerabilities from the report under certain circumstances. For example, the application may discover a vulnerable service on an asset behind a firewall because it has authorized access through the firewall. While this vulnerability could result in the asset or site failing the audit, the merchant could argue that the firewall reduces any real risk under normal circumstances. Additionally, the network may have host- or network-based intrusion prevention systems in place, further reducing risk.

Acceptable use: Organizations may have legitimate uses for certain practices that the application would interpret as vulnerabilities. For example, anonymous FTP access may be a deliberate practice and not a vulnerability.

Acceptable risk: In certain situations, it may be preferable not to remediate a vulnerability if the vulnerability poses a low security risk and if remediation would be too expensive or require too much effort. For example, applying a specific patch for a vulnerability may prevent an application from functioning. Re-engineering the application to work on the patched system may require too much time, money, or other resources to be justified, especially if the vulnerability poses minimal risk.

False positives: According to PCI criteria, a merchant should be able to report a false positive, which can then be verified and accepted by a Qualified Security Assessor (QSA) or Approved Scanning Vendor (ASV) in a PCI audit. Below are scenarios in which it would be appropriate to exclude a false positive from an audit report. In all cases, a QSA or ASV would need to approve the exception.

Backporting may cause false positives. For example, an Apache update installed on an older Red Hat server may produce vulnerabilities that should be excluded as false positives.

If an exploit reports false positives on one or more assets, it would be appropriate to exclude these results.

Note: In order to comply with federal regulations, such as the Sarbanes-Oxley Act (SOX), it is often critically important to document the details of a vulnerability exception, such as the personnel involved in requesting and approving the exception, relevant dates, and information about the exception.

Understanding vulnerability exception permissions

Your ability to work with vulnerability exceptions depends on your permissions. If you do not now know what your permissions are, consult your Global administrator.

Three permissions are associated with the vulnerability exception workflow:

- Submit Vulnerability Exceptions: A user with this permission can submit requests to exclude vulnerabilities from reports.
- Review Vulnerability Exceptions: A user with this permission can approve or reject requests to exclude vulnerabilities from reports.
- Delete Vulnerability Exceptions: A user with this permission can delete vulnerability exceptions and exception requests. This permission is significant in that it is the only way to overturn a vulnerability request approval. In that sense, a user with this permission can wield a check and balance against users who have permission to review requests.

Understanding vulnerability exception status and work flow

Every vulnerability has an exception status, including vulnerabilities that have never been considered for exception. The range of actions you can take with respect to exceptions depends on the exception status, as well as your permissions, as indicated in the following table:

If the vulnerability has the following exception status...	...and you have the following permission...	...you can take the following action:
never been submitted for an exception	Submit Exception Request	submit an exception request
previously approved and later deleted or expired	Submit Exception Request	submit an exception request
under review (submitted, but not approved or rejected)	Review Vulnerability Exceptions	approve or reject the request
excluded for another instance, asset, or site	Submit Exception Request	submit an exception request
under review (and submitted by you)		recall the exception
under review (submitted, but not approved or rejected)	Delete Vulnerability Exceptions	delete the request
approved	Review Vulnerability Exceptions	view and change the details of the approval, but not overturn the approval
rejected	Submit Exception Request	submit another exception request
approved or rejected	Delete Vulnerability Exceptions	delete the exception, thus overturning the approval

Understanding different options for exception scope

A vulnerability may be discovered once or multiple times on a certain asset. The vulnerability may also be discovered on hundreds of assets. Before you submit a request for a vulnerability exception, review how many instances of the vulnerability have been discovered and how many assets are affected. It's also important to understand the circumstances surrounding each affected asset. You can control the scope of the exception by using one of the following options when submitting a request:

- You can create an exception for *all instances* of a vulnerability on all affected assets. For example, you may have many instances of a vulnerability related to an open SSH port. However, if in all instances a compensating control is in place, such as a firewall, you may want to exclude that vulnerability globally.
- You can create an exception for *all instances of a vulnerability in a site*. As with global exceptions, a typical reason for a site-specific exclusion is a compensating control, such as all of a site's assets being located behind a firewall.
- You can create an exception for *all instances of a vulnerability on a single asset*. For example one of the assets affected by a particular vulnerability may be located in a DMZ. Or perhaps it only runs for very limited periods of time for a specific purpose, making it less sensitive.
- You can create an exception for a *single instance of a vulnerability*. For example, a vulnerability may be discovered on each of several ports on a server. However, one of those ports is behind a firewall. You may want to exclude the vulnerability instance that affects that protected port.

Submitting or re-submitting a request for a global vulnerability exception

A global vulnerability exception means that the application will not report the vulnerability on any asset in your environment that has that vulnerability. Only a Global Administrator can submit requests for global exceptions.

Locate the vulnerability for which you want to request an exception. There are several ways to locate to a vulnerability. The following way is easiest for a global exception.

1. Click the **Vulnerabilities** tab of the Security Console Web interface.

   The console displays the *Vulnerabilities* page.

2. Locate the vulnerability in the *Vulnerability Listing* table.

Create and submit the exception request.

1. Look at the *Exceptions* column for the located vulnerability.

   This column displays one of several possible actions. If an exception request has not previously been submitted for that vulnerability, the column displays an **Exclude** icon. If it was submitted and then rejected, the column displays a **Resubmit** icon.

2. Click the icon.

Tip: If a vulnerability has an action icon other than **Exclude**, see *Understanding vulnerability exception permissions* on page 280.

   A *Vulnerability Exception* dialog box appears. If an exception request was previously submitted and then rejected, read the displayed reasons for the rejection and the user name of the reviewer. This is helpful for tracking previous decisions about the handling of this vulnerability.

3. Select *All instances* if it is not already displayed from the **Scope** drop-down list.

4. Select a reason for the exception from the drop-down list.

   For information about exception reasons, see *Understanding cases for excluding vulnerabilities* on page 279.

5. Enter additional comments.

   These are especially helpful for a reviewer to understand your reasons for the request.

   Note: If you select *Other* as a reason from the drop-down list, additional comments are required.

6. Click **Submit & Approve** to have the exception take effect.

7. (Optional) Click **Submit** to place the exception under review and have another individual in your organization review it.

   Note: Only a Global Administrator can submit and approve a vulnerability exception.

Verify the exception (if you submitted *and* approved it).

After you approve an exception, the vulnerability no longer appears in the list on the *Vulnerabilities* page.

1. Click the **Administration** tab.

   The console displays the *Administration* page.

2. Click the **Manage** link for *Vulnerability Exceptions*.

3. Locate the exception in the *Vulnerability Exception Listing* table.

Submitting or re-submitting an exception request for all instances of a vulnerability on a specific site

Note: If you enabled the option to link matching assets across all sites after the April 8, 2015, product update, you cannot use this Web interface feature to exclude vulnerabilities in sites *after* enabling the linking option. Site-level exceptions created in the Web interface before the option was enabled will continue to apply. See *Linking assets across sites* on page 672. You can use the API to exclude vulnerabilities at the site level. See the API guide.

Note: The vulnerability information in the page for a scan is specific to that particular scan instance. The ability to create an exception is available in more cumulative levels such as the site or vulnerability listing in order for the vulnerability to be excluded in future scans.

Locate the vulnerability for which you want to request an exception. There are several ways to locate to a vulnerability. The following ways are easiest for a site-specific exception:

1. If you want to find a specific vulnerability, click the **Vulnerabilities** tab of the Security Console Web interface.

   The Security Console displays the *Vulnerabilities* page.

2. Locate the vulnerability in the *Vulnerability Listing* table, and click the link for it.

3. Find an asset in a particular site for which you want to exclude vulnerability instances in the *Affects* table of the vulnerability details page.

   OR

1. If you want to see what vulnerabilities are affecting assets in different sites, click the **Assets** tab.

   The Security Console displays the *Assets* page.

2. Click the option to view assets by sites.

   The Security Console displays the *Sites* page.

3. Click a site in which you want to view vulnerabilities.

   The Security Console displays the page for the selected site.

4. Click an asset in the *Asset Listing* table.

   The Security Console displays the page for the selected asset.

5. Locate the vulnerability you want to exclude in the *Vulnerability Listing* table and click the link for it.

Create and submit an individual exception request.

1. Look at the *Exceptions* column for the located vulnerability. If an exception request has not previously been submitted for that vulnerability, the column displays an **Exclude** icon. If it was submitted and then rejected, the column displays a **Resubmit** icon.

2. Click the **Exclude** icon.

   Note: If a vulnerability has an action link other than **Exclude**, see *Understanding cases for excluding vulnerabilities* on page 279.

   A *Vulnerability Exception* dialog box appears. If an exception request was previously submitted and then rejected, read the displayed reasons for the rejection and the user name of the reviewer. This is helpful for tracking previous decisions about the handling of this vulnerability.

3. Select *All instances in this site* from the **Scope** drop-down list.

4. Select a reason for the exception from the drop-down list.

   For information about exception reasons, see *Understanding cases for excluding vulnerabilities* on page 279.

5. Enter additional comments.

These are especially helpful for a reviewer to understand your reasons for the request. If you select *Other* as a reason from the drop-down list, additional comments are required.

6. Click **Submit & Approve** to have the exception take effect.
7. Click **Submit** to place the exception under review and have another individual in your organization review it.

Create and submit multiple, simultaneous exception requests.

This procedure is useful if you want to exclude a large number of vulnerabilities because, for example, they all have the same compensating control.

1. After going to the *Vulnerability Listing* table as described in the preceding section, select the row for each vulnerability that you want to exclude.

   OR

2. To select all the vulnerabilities displayed in the table, click the check box in the top row. Then select the pop-up option **Select Visible**.
3. Click **Exclude** for vulnerabilities that have not been submitted for exception, or click **Resubmit** for vulnerabilities that have been rejected for exception.
4. Proceed with the vulnerability exception workflow as described in the preceding section.

   If you've selected multiple vulnerabilities but then want to cancel the selection, click the top row. Then select the pop-up option **Clear All**.

Note: If you select all listed vulnerabilities for exclusion, it will only apply to vulnerabilities that have not been excluded. For example, if the *Vulnerabilities Listing* table includes vulnerabilities that are under review or rejected, the global exclusion will not apply to them. The same applies for global resubmission: It will only apply to listed vulnerabilities that have been rejected for exclusion.



Selecting multiple vulnerabilities

Verify the exception (if you submitted *and* approved it). After you approve an exception, the vulnerability no longer appears in the list on the *Vulnerabilities* page.

1. Click the *Administration* tab.

   The console displays the *Administration* page.

2. Click the **Manage** link for *Vulnerability Exceptions*.

3. Locate the exception in the *Vulnerability Exception Listing* table.

Submitting or re-submitting an exception request for all instances of a vulnerability on a specific asset

Locate the vulnerability for which you want to request an exception. There are several ways to locate to a vulnerability. The following ways are easiest for an asset-specific exception.

1. If you want to find a specific vulnerability click the **Vulnerabilities** tab of the Security Console Web interface.

   The Security Console displays the *Vulnerabilities* page.

2. Locate the vulnerability in the *Vulnerability Listing* table, and click the link for it.

3. Click the link for the asset that includes the instances of the vulnerability that you want to have excluded in the *Affects* table of the vulnerability details page.

4. On the details page of the affected asset, locate the vulnerability in the *Vulnerability Listing* table and click the link for it.

   OR

1. If you want to see what vulnerabilities are affecting specific assets that you find using different grouping categories, click the **Assets** tab.

   The Security Console displays the *Assets* page.

2. Select one of the options to view assets according to different grouping categories: sites they belong to, asset groups they belong to, hosted operating systems, hosted software, or hosted services. Or click the link to view all assets.

3. Depending on the category you selected, click through displayed subcategories until you find the asset you are searching for. See *Locating and working with assets* on page 240.

   The Security Console displays the page for the selected asset.

4. Locate the vulnerability that you want to exclude in the *Vulnerability Listing* table and click the link for it.

Create and submit a single exception request.

Note: If a vulnerability has an action link other than **Exclude**, see *Understanding vulnerability exception status and work flow* on page 281.

1. Look at the *Exceptions* column for the located vulnerability. This column displays one of several possible actions. If an exception request has not previously been submitted for that vulnerability, the column displays an **Exclude** icon. If it was submitted and then rejected, the column displays a **Resubmit** icon.

2. Click the icon.

   A *Vulnerability Exception* dialog box appears. If an exception request was previously submitted and then rejected, read the displayed reasons for the rejection and the user name of the reviewer. This is helpful for tracking previous decisions about the handling of this vulnerability.

3. Select *All instances on this asset* from the **Scope** drop-down list.

Note: If you select *Other* as a reason from the drop-down list, additional comments are required.

4. Enter additional comments.

   These are especially helpful for a reviewer to understand your reasons for the request.

5. Click **Submit & Approve** to have the exception take effect.
6. (*Optional*) Click **Submit** to place the exception under review and have another individual in your organization review it.

Create and submit (or resubmit) multiple, simultaneous exception requests.

This procedure is useful if you want to exclude a large number of vulnerabilities because, for example, they all have the same compensating control.

1. After going to the *Vulnerability Listing* table as described in the preceding section, select the row for each vulnerability that you want to exclude.

   OR

   To select all the vulnerabilities displayed in the table, click the check box in the top row. Then select the pop-up option **Select Visible**.
2. Click **Exclude** for vulnerabilities that have not been submitted for exception, or click **Resubmit** for vulnerabilities that have been rejected for exception.
3. Proceed with the vulnerability exception workflow as described in the preceding section.

   If you've selected multiple vulnerabilities but then want to cancel the selection, click the top row. Then select the pop-up option **Clear All**.

Note: If you select all listed vulnerabilities for exclusion, it will only apply to vulnerabilities that have not been excluded. For example, if the *Vulnerabilities Listing* table includes vulnerabilities that are under review or rejected, the global exclusion will not apply to them. The same applies for global resubmission: It will only apply to listed vulnerabilities that have been rejected for exclusion.

Verify the exception (if you submitted *and* approved it). After you approve an exception, the vulnerability no longer appears in the list on the *Vulnerabilities* page.

1. Click the **Administration** tab.

   The Security Console displays the *Administration* page.
2. Click the **Manage** link for *Vulnerability Exceptions*.
3. Locate the exception in the *Vulnerability Exception Listing* table.

Submitting or re-submitting an exception request for a single instance of a vulnerability

When you create an exception for a single instance of a vulnerability, the application will not report the vulnerability against the asset if the device, port, and additional data match.

Locate the instance of the vulnerability for which you want to request an exception. There are several ways to locate to a vulnerability. The following way is easiest for a site-specific exception.

1. Click the **Vulnerabilities** tab of the security console Web interface.
2. Locate the vulnerability in the *Vulnerability Listing* table on the *Vulnerabilities* page, and click the link for it.
3. Locate the affected asset in the in the *Affects* table on the details page for the vulnerability.
4. (*Optional*) Click the **Assets** tab and use one of the displayed options to find a vulnerability on an asset. See *Locating and working with assets* on page 240.
5. Locate the vulnerability in the *Vulnerability Listing* table on the asset page, and click the link for it.

Create and submit a single exception request.

Note: If a vulnerability has an action link other than **Exclude**, see *Understanding vulnerability exception status and work flow* on page 281 .

1. Look at the *Exceptions* column for the located vulnerability. This column displays one of several possible actions. If an exception request has not previously been submitted for that vulnerability, the column displays an **Exclude** icon. If it was submitted and then rejected, the column displays a **Resubmit** icon.
2. Click the icon.

   A *Vulnerability Exception* dialog box appears. If an exception request was previously submitted and then rejected, you can view the reasons for the rejection and the user name of the reviewer in a note at the top of the box. Select a reason for requesting the exception from the drop-down list. For information about exception reasons, see *Understanding cases for excluding vulnerabilities* on page 279.
3. Select *Specific instance on this asset* from the **Scope** drop-down list.

   If you select *Other* as a reason from the drop-down list, additional comments are required.

4. Enter additional comments. These are especially helpful for a reviewer to understand your reasons for the request.
5. Click **Submit & Approve** to have the exception take effect.
6. (Optional) Click **Submit** to place the exception under review and have another individual in your organization review it.

Re-submit multiple, simultaneous exception requests.

This procedure is useful if you want to exclude a large number of vulnerabilities because, for example, they all have the same compensating control.

1. After going to the *Vulnerability Listing* table as described in the preceding section, select the row for each vulnerability that you want to exclude.

   OR

2. To select all the vulnerabilities displayed in the table, click the check box in the top row. Then select the pop-up option **Select Visible**.
3. Click **Exclude** for vulnerabilities that have not been submitted for exception, or click **Resubmit** for vulnerabilities that have been rejected for exception.
4. Proceed with the vulnerability exception workflow as described in the preceding section.

   If you've selected multiple vulnerabilities but then want to cancel the selection, click the top row. Then select the pop-up option **Clear All**.

Note: If you select all listed vulnerabilities for exclusion, it will only apply to vulnerabilities that have not been excluded. For example, if the *Vulnerabilities Listing* table includes vulnerabilities that are under review or rejected, the global exclusion will not apply to them. The same applies for global resubmission: It will only apply to listed vulnerabilities that have been rejected for exclusion.

Verify the exception (if you submitted *and* approved it). After you approve an exception, the vulnerability no longer appears in the list on the *Vulnerabilities* page.

1. Click the **Administration** tab.

   The console displays the *Administration* page.

2. Click the **Manage** link for *Vulnerability Exceptions*.
3. Locate the exception in the *Vulnerability Exception Listing* table.

Recalling an exception request that you submitted

You can recall, or cancel, a vulnerability exception request that you submitted if its status remains under review.

Locate the exception request, and verify that it is still under review. The location depends on the scope of the exception. For example, if the exception is for all instances of the vulnerability on a single asset, locate that asset in the *Affects* table on the details page for the vulnerability. If the link in the Exceptions column is **Under review**, you can recall it.

Recall a single request.

1. Click the **Under Review** link.
2. Click **Recall** in the *Vulnerability Exception* dialog box.

   The link in the *Exceptions* column changes to **Exclude**.

Recall multiple, simultaneous exception requests.

This procedure is useful if you want to recall a large number of requests because, for example, you've learned that since you submitted them it has become necessary to include them in a report.

1. After locating the exception request as described in the preceding section, select the row for each vulnerability that you want to exclude.

   OR

2. To select all the vulnerabilities displayed in the table, click the check box in the top row. Then select the pop-up option **Select Visible**.
3. Click **Recall**.
4. Proceed with the recall workflow as described in the preceding section.

   If you've selected multiple vulnerabilities but then want to cancel the selection, click the top row. Then select the pop-up option **Clear All**.

Note: If you select all listed vulnerabilities for recall, it will only apply to vulnerabilities that are under review. For example, if the *Vulnerabilities Listing* table includes vulnerabilities that have not been excluded, or have been rejected for exclusion, the global recall will not apply to them.

Reviewing an exception request

Upon reviewing a vulnerability exception request, you can either approve or reject it.

1. Locate the exception request.
2. Click the **Administration** tab of the security console Web interface.
3. On the *Administration* page, click the **Manage** link next to *Vulnerability Exceptions*.
4. Locate the request in the *Vulnerability Exception Listing* table.

   To select multiple requests for review, select each desired row.

   OR, to select all requests for review, select the top row.

   Selecting multiple requests is useful if you know, for example, that you want to accept or reject multiple requests for the same reason.

Review the request(s).

1. Click the **Under review** link in the *Review Status* column.
2. Read the comments by the user who submitted the request and decide whether to approve or reject the request.
3. Enter comments in the Reviewer's Comments text box. Doing so may be helpful for the submitter.

   If you want to select an expiration date for the review decision, click the calendar icon and select a date. For example, you may want the exception to be in effect only until a PCI audit is complete.

Note: You also can click the top row check box to select all requests and then approve or reject them in one step.

4. Click **Approve** or **Reject**, depending on your decision.

   The result of the review appears in the *Review Status* column.



Selecting multiple requests for review

Deleting a vulnerability exception or exception request

Deleting an exception is the only way to override an approved request.

Locate the exception or exception request.

1. Click the **Administration** tab of the security console Web interface.

   The console displays the *Administration* page.

2. Click the **Manage** link next to *Vulnerability Exceptions*.

3. Locate the request in the *Vulnerability Exception Listing* table.

   To select multiple requests for deletion, select each desired row.

   OR, to select all requests for deletion, select the top row.

Delete the request(s).

1. Click the **Delete** icon.

   The entry(ies) no longer appear in the *Vulnerability Exception Listing* table. The affected vulnerability(ies) appear in the appropriate vulnerability listing with an **Exclude** icon, which means that a user with appropriate permission can submit an exception request for it.

Viewing vulnerability exceptions in the Report Card report

When you generate a report based on the default Report Card template, each vulnerability exception appears on the vulnerability list with the reason for its exception.

How vulnerability exceptions appear in XML and CSV formats

Vulnerability exceptions can be important for the prioritization of remediation projects and for compliance audits. Report templates include a section dedicated to exceptions. See *Vulnerability Exceptions* on page 711. In XML and CSV reports, exception information is also available.

XML: The vulnerability test status attribute is set to one of the following values for vulnerabilities suppressed due to an exception:

```
exception-vulnerable-exploited - Exception suppressed exploited
vulnerability
```

```
exception-vulnerable-version - Exception suppressed version-checked
vulnerability
```

```
exception-vulnerable-potential - Exception suppressed potential
vulnerability
```

CSV: The vulnerability result-code column will be set to one of the following values for vulnerabilities suppressed due to an exception. Each code corresponds to results of a vulnerability check:

Each code corresponds to results of a vulnerability check:

- *ds* (skipped, disabled): A check was not performed because it was disabled in the scan template.
- *ee* (excluded, exploited): A check for an exploitable vulnerability was excluded.
- *ep* (excluded, potential): A check for a potential vulnerability was excluded.
- er (error during check): An error occurred during the vulnerability check.
- *ev* (excluded, version check): A check was excluded. It is for a vulnerability that can be identified because the version of the scanned service or application is associated with known vulnerabilities.
- *nt* (no tests): There were no checks to perform.
- *nv* (not vulnerable): The check was negative.
- *ov* (overridden, version check): A check for a vulnerability that would ordinarily be positive because the version of the target service or application is associated with known vulnerabilities was negative due to information from other checks.
- *sd* (skipped because of DoS settings): sd (skipped because of DOS settings)—If unsafe checks were not enabled in the scan template, the application skipped the check because of the risk of causing denial of service (DOS). See *Configuration steps for vulnerability check settings* on page 603.
- *sv* (skipped because of inapplicable version): the application did not perform a check because the version of the scanned item is not in the list of checks.
- *uk* (unknown): An internal issue prevented the application from reporting a scan result.
- *ve* (vulnerable, exploited): The check was positive. An exploit verified the vulnerability.
- *vp* (vulnerable, potential): The check for a potential vulnerability was positive.
- *vv* (vulnerable, version check): The check was positive. The version of the scanned service or software is associated with known vulnerabilities.

Working with Policy Manager results

If you work for a U.S. government agency, a vendor that transacts business with the government, or a company with strict configuration security policies, you may be running scans to verify that your assets comply with United States Government Configuration Baseline (USGCB) policies, Center for Internet Security (CIS) benchmarks, or Federal Desktop Core Configuration (FDCC). Or you may be testing assets for compliance with customized policies based on these standards.

After running Policy Manager scans, you can view information that answers the following questions:

- What is the overall rate of compliance for assets in my environment?
- Which policies are my assets compliant with?
- Which policies are my assets not compliant with?
- If my assets have failed compliance with a given policy, which specific policy rules are they not compliant with?
- Can I change the results of a specific rule compliance test?

Viewing the results of configuration assessment scans enables you to quickly determine the policy compliance status of your environment. You can also view test results of individual policies and rules to determine where specific remediation efforts are required so that you can make assets compliant.

Distinguishing between Policy Manager and standard policies

Note: You can only view policy test results for assets to which you have access. This is true for Policy Manager and standard policies.

This section specifically addresses Policy Manager results. The Policy Manager is a license-enabled feature that includes the following policy checks:

- USGCB 2.0 policies (only available with a license that enables USGCB scanning)
- USGCB 1.0 policies (only available with a license that enables USGCB scanning)
- Center for Internet Security (CIS) benchmarks (only available with a license that enables CIS scanning)
- FDCC policies (only available with a license that enables FDCC scanning)
- Custom policies that are based on USGCB or FDCC policies or CIS benchmarks (only available with a license that enables custom policy scanning)

You can view the results of Policy Manager checks on the *Policies* page or on a page for a specific asset that has been scanned with Policy Manager checks.

Standard policies are available with all licenses and include the following:

- Oracle policy
- Lotus Domino policy
- Windows Group policy
- AS/400 policy
- CIFS/SMB Account policy

You can view the results of standard policy checks on a page for a specific asset that has been scanned with one of these checks.

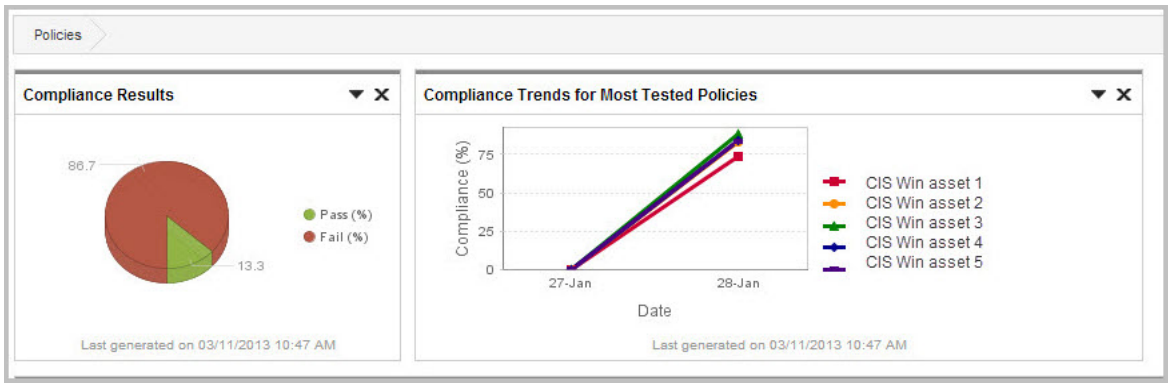
Standard policies are not covered in this section.

Getting an overview of Policy Manager results

If you want to get a quick overview of all the policies for which you've run Policy Manager checks, go to the *Policies* page by clicking the **Policies** tab on any page of the Web interface. The page lists tested policies for all assets to which you have access.

At the top of the page, a pie chart shows the ratio of passed and failed policy checks. A line graph shows compliance trends for the most tested policies over time. The y-axis shows the percentage

of assets that comply with each listed policy. You can use these statistics to gauge your overall compliance status and identify compliance issues.



Statistical graphics on the Policies pages

The *Policy Listing* table shows the number of assets that passed and failed compliance checks for each policy. It also includes the following columns:

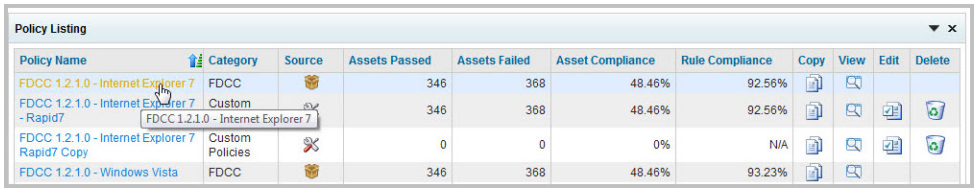
- Each policy is grouped in a category within the application, depending on its source, purpose, or other criteria. The category for any USGCB 2.0 or USGCB 1.0 policy is
- listed as USGCB. Another example of a category might be Custom, which would include custom policies based on built-in Policy Manager policies. Categories are listed under the *Category* heading.
- The *Asset Compliance* column shows the percentage of tested assets that comply with each policy.
- The table also includes a *Rule Compliance* column. Each policy consists of specific rules, and checks are run for each rule. The *Rule Compliance* column shows the percentage of rules with which assets comply for each policy. Any percentage below 100 indicates failure to comply with the policy
- The *Policy Listing* table also includes columns for copying, editing, and deleting policies. For more information about these options, see *Creating a custom policy* on page 631.

Viewing results for a Policy Manager policy

After assessing your overall compliance on the *Policies* page, you may want to view more specific information about a policy. For example, a particular policy shows less than 100 percent rule compliance (which indicates failure to comply with the policy) or less than 100 percent asset compliance . You may want to learn why assets failed to comply or which specific rule tests resulted in failure.

Tip: You can also view results of Policy Manager checks for a specific asset on the page for that asset. See *Viewing the details about an asset* on page 248.

On the *Policies* page, you can view details about a policy in the *Policy Listing* table by clicking the name of that policy.



Clicking a policy name to view information about it

The Security Console displays a page about the policy.

At the top of the page, a pie chart shows the ratio of assets that passed the policy check to those that failed. Two line graphs show the five most and least compliant assets.

An *Overview* table lists general information about how the policy is identified. The benchmark ID refers to an exhaustive collection of rules, some of which are included in the policy. The table also lists general asset and rule compliance statistics for the policy.

The *Tested Assets* table lists each asset that was tested against the policy and the results of each test, and general information about each asset. The *Asset Compliance* column lists each asset's percentage of compliance with all the rules that make up the policy. Assets with lower compliance percentages may require more remediation work than other assets.

You can click the link for any listed asset to view more details about it.

The *Policy Rule Compliance Listing* table lists every rule that is included in the policy, the number of assets that passed compliance tests, and the number of assets that failed. The table also includes an *Override* column. For information about overrides, see *Overriding rule test results* on page 303.

Understanding results for policies and rules

- A *Pass* result means that the asset complies with all the rules that make up the policy.
- A *Fail* result means that the asset does not comply with at least one of the rules that makes up the policy. The *Policy Compliance* column indicates the percentage of policy rules with which the asset does comply.
- A *Not Applicable* result means that the policy compliance test doesn't apply to the asset. For example, a check for compliance with Windows Vista configuration policies would not apply to a Windows XP asset.

Viewing information about policy rules

Every policy is made up of individual configuration rules. When performing a Policy Manager check, the application tests an asset for compliance with each of the rules of the policy. By viewing results for each rule test, you can isolate the configuration issues that are preventing your assets from being policy-compliant.

Viewing a rule's results for all tested assets

By viewing the test results for all assets against a rule, you can quickly determine which assets require remediation work in order to become compliant.

1. Click the **Policies** tab.

   The Security Console displays the *Policies* page.

2. In the *Policy Listing* table, click the name of a policy for which you want to view rule details.

   The Security Console displays the page for the policy.

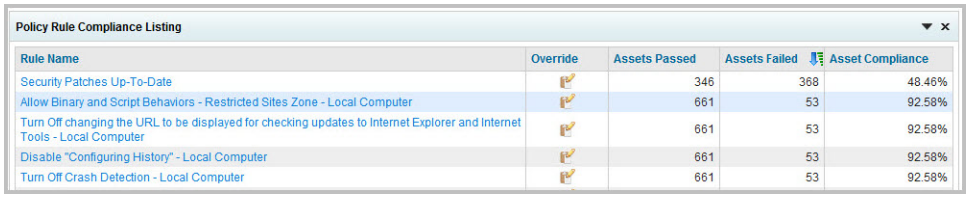
   Tip: Mouse over a rule name to view a description of the rule.

3. In the *Policy Rule Compliance Listing* table, click the link for any rule that you want to view details for.

   The Security Console displays the page for the rule.

The *Overview* table displays general information that identifies the rule, including its name and category, as well as the name and benchmark ID for the policy that the rule is a part of.

The *Tested Assets* table lists each asset that was tested for compliance with the rule and the result of the result of each test. The table also lists the date of the most recent scan for each rule test. This information can be useful if some remediation work has been done on the asset since the scan date, which might warrant overriding a *Fail* result or rescanning.



Policy Rule Compliance Listing

Rule Name	Override	Assets Passed	Assets Failed	Asset Compliance
Security Patches Up-To-Date		346	368	48.46%
Allow Binary and Script Behaviors - Restricted Sites Zone - Local Computer		661	53	92.58%
Turn Off changing the URL to be displayed for checking updates to Internet Explorer and Internet Tools - Local Computer		661	53	92.58%
Disable "Configuring History" - Local Computer		661	53	92.58%
Turn Off Crash Detection - Local Computer		661	53	92.58%

Policy Rule Compliance Listing table on a policy page

Viewing CCE data for a rule

Every rule has a Common Configuration Enumerator (CCE) identifier. CCE is a standard for identifying and correlating configuration data, allowing this data to be shared by multiple information sources and tools.

You may find it useful to analyze a policy rule's CCE data. The information may help you understand the rule better or to remediate the configuration issue that caused an asset to fail the test. Or, it may be simply useful to have the data available for reference.

1. Click the **Policies** tab.

   The Security Console displays the *Policies* page.

2. In the *Policy Listing* table, click the name of a policy for which you want to view rule details.

   The Security Console displays the page for the policy.

3. In the *Tested Assets* table, click the IP address or name of an asset that has been tested against the policy.

   The Security Console displays the page for the asset.

4. In the *Configuration Policy Rules* table, click the name of the rule for which you want to view CCE data.

   The Security Console displays the page for the rule.

   Note: The application applies any current CCE updates with its automatic content updates.

5. In the *Configuration Policy Rule CCE Data* table, view the rule's CCE identifier, description, affected platform, and most recent date that the rule was modified in the National Vulnerability Database.

   The Security Console displays the page for the rule.

6. Click the link for the rule's CCE identifier.

   The Security Console displays the CCE data page.

The page provides the following information:

- The *Overview* table displays the rule Common Configuration Enumerator (CCE) identifier, the specific platform to which the rule applies, and the most recent date that the rule was updated in the National Vulnerability Database. The application applies any current CCE updates with its automatic content updates.
- The *Parameters* table lists the parameters required to implement the rule on each tested asset.
- The *Technical Mechanisms* table lists the methods used to test compliance with the rule.
- The *References* table lists documentation sources to which the rule refers for detailed source information as well as values that indicate the specific information in the documentation source.
- The *Configuration Policy Rules* table lists the policy and the policy rule name for every imported policy in the application.

Overriding rule test results

You may want to override, or change, a test result for a particular rule on a particular asset for any of several reasons:

- You disagree with the result.
- You have remediated the configuration issue that produced a Fail result.
- The rule does not apply to the tested asset.

When overriding a result, you will be required to enter your reason for doing so.

Another user can also override your override. Yet another user can perform another override, and so on. For this reason, you can track all the overrides for a rule test back to the original result in the Security Console Web interface.

The most recent override for any rule is also identified in the XCCDF Results XML Report format. Overrides are not identified as such in the XCCDF Human Readable CSV Report format. The CSV format displays each current test result as of the most recent override. See *Working with report formats* on page 551.

All overrides and their reasons are incorporated, along with the policy check results, into the documentation that the U.S. government reviews in the certification process.

Understanding Policy Manager override permissions

Your ability to work with overrides depends on your permissions. If you do not know what your permissions are, consult your Global Administrator. These permissions apply specifically to Policy Manager policies.

Note: These permissions also include access to activities related to vulnerability exceptions. See *Managing users and authentication* in the administrator's guide.

Three permissions are associated with policy override workflow:

- *Submit Vulnerability Exceptions and Policy Overrides*: A user with this permission can submit requests to override policy test results.
- *Review Vulnerability Exceptions and Policy Overrides*: A user with this permission can approve or reject requests to override policy rule results.
- *Delete Vulnerability Exceptions and Policy Overrides*: A user with this permission can delete policy test result overrides and override requests.

Understanding override scope options

When overriding a rule result, you will have a number of options for the scope of the override:

Global: You can override a rule for all assets in all sites. This scope is useful if assets are failing a policy that includes a rule that isn't relevant to your organization. For example, an FDCC policy includes a rule for disabling remote desktop access. This rule does not make sense for your organization if your IT department administers all workstations via remote desktop access. This override will apply to all future scans, unless you override it again.

All assets in a specific site: This scope is useful if a policy includes a rule that isn't relevant to a division within your organization and that division is encompassed in a site. For example, your organization disables remote desktop administration except for the engineering department. If all of the engineering department's assets are contained within a site, you can override a Fail result for the remote desktop rule in that site. This override will apply to all future scans, unless you override it again.

All scan results for a single asset: This scope is useful if a policy includes a rule that isn't relevant for small number of assets. For example, your organization disables remote desktop administration except for three workstations. You can override a Fail result for the remote desktop rule for each of those three specific assets. This override will apply to all future scans, unless you override it again.

A specific scan result on a single asset: This scope is useful if a policy includes a rule that wasn't relevant at a particular point in time but will be relevant in the future. For example, your organization disables remote desktop administration. However, unusual circumstances required the feature to be enabled temporarily on an asset so that a remote IT engineer could troubleshoot it. During that time window, a policy scan was run, and the asset failed the test for the remote desktop rule. You can override the Fail result for that specific scan, and it will not apply to future scans.

Viewing a rule's override history

It may be helpful to review the overrides of previous users to give you additional context about the rule or a tested asset.

1. Click the **Policies** tab.

   The Security Console displays the *Policies* page.

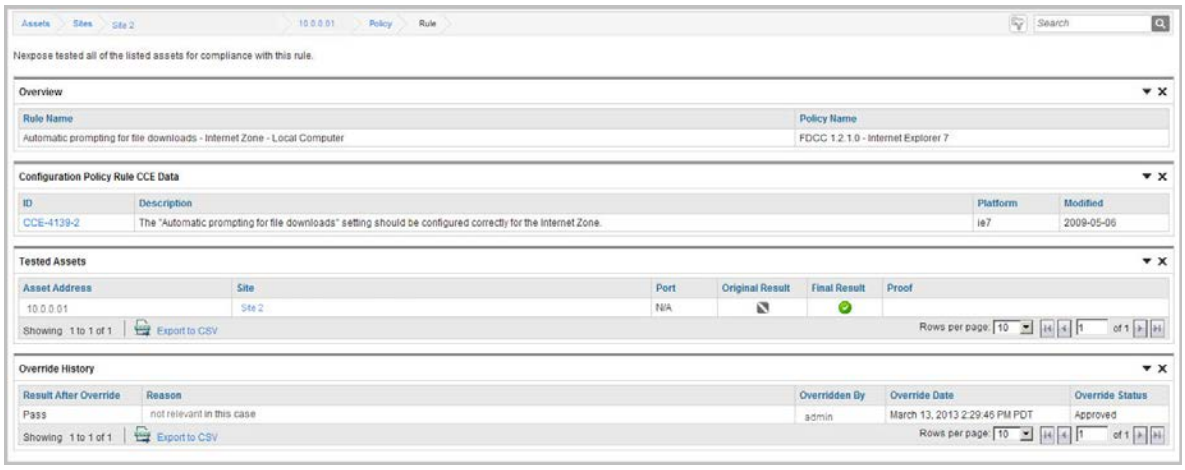
2. In the *Tested Assets* table, click the name or IP address of an asset.

   The Security Console displays the page for the asset.

3. In the Configuration Policy Rules table, click the rule for which you want to view the override history.

   The Security Console displays the page for the rule.

4. See the rule's Override History table, which lists each override for the rule, the date it occurred, and the result after the override. The Override Status column lists whether the override has been submitted, approved, rejected, or expired.



A rule's override history

Submitting an override of a rule for all assets in all sites

1. Click the **Policies** tab.

   The Security Console displays the *Policies* page.

2. In the *Policy Listing* table, click the name of the policy that includes the rule for which you want to override the result.

   The Security Console displays the page for the policy.

3. In the *Policy Rule Compliance Listing* table, click the **Override** icon for the rule that you want to override.

   The Security Console displays a *Create Policy Override* pop-up window.

4. Select an override type from the drop-down list:
   - *Pass* indicates that you consider an asset to be compliant with the rule.
   - *Fail* indicates that you consider an asset to be non-compliant with the rule.
   - *Fixed* indicates that the issue that caused a Fail result has been remediated. A Fixed override will cause the result to appear as a Pass in reports and result listings.
   - *Not Applicable* indicate that the rule does not apply to the asset.

5. Enter your reason for requesting the override. A reason is required.

6. If you only have override request permission, click **Submit** to place the override under review and have another individual in your organization review it. The override request appears in the *Override History* table of the rule page.

   OR

   If you have override approval permission, click **Submit and approve**.

Submitting an override of a rule for all assets in a site

1. Click the **Policies** tab.

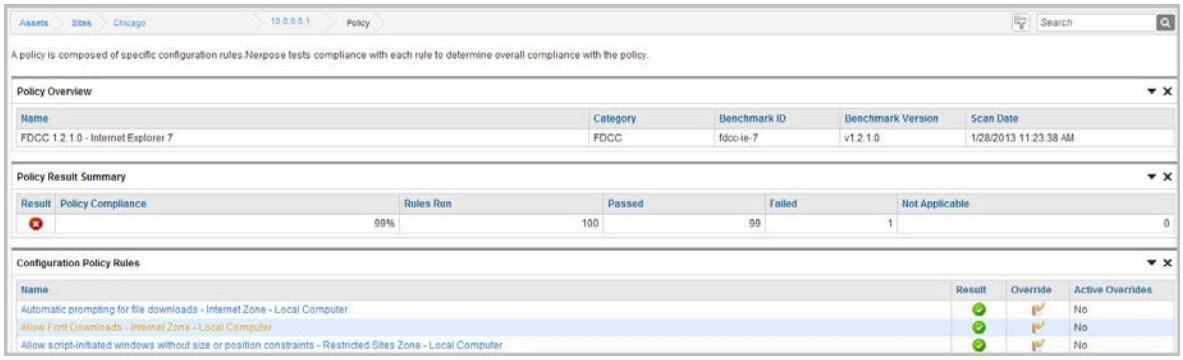
   The Security Console displays the *Policies* page.

2. In the *Policy Listing* table, click the name of the policy that includes the rule for which you want to override the result.

   The Security Console displays the page for the policy.

3. In the *Tested Assets* table, click the name or IP address of an asset.

   The Security Console displays the page for the asset. Note that the navigation bread crumb for the page includes the site that contains the asset.

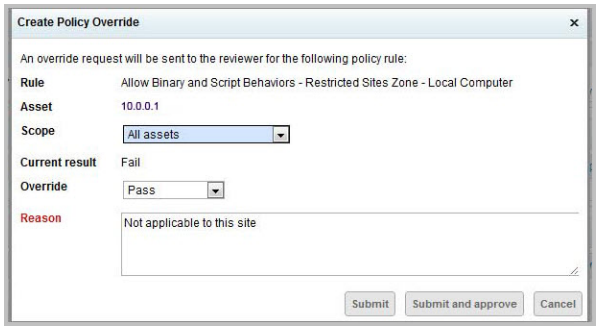


The page for an asset selected from a policy page

4. In the *Configuration Policy Rules* table, click the **Override** icon for the rule that you want to override.

   The Security Console displays a *Create Policy Override* pop-up window.

5. Select *All assets* from the **Scope** drop-down list.
6. Select an override type from the drop-down list:
   - *Pass* indicates that you consider an asset to be compliant with the rule.
   - *Fail* indicates that you consider an asset to be non-compliant with the rule.
   - *Fixed* indicates that the issue that caused a Fail result has been remediated. A Fixed override will cause the result to appear as a Pass in reports and result listings.
   - *Not Applicable* indicates that the rule does not apply to the asset.
7. Enter your reason for requesting the override. A reason is required.



Submitting a site-specific override

8. If you only have override request permission, click **Submit** to place the override under review and have another individual in your organization review it. The override request appears in the *Override History* table of the rule page.

   OR

   If you have override approval permission, click **Submit** and approve.

Submitting an override of a rule for all scans on a specific asset

1. Click the **Policies** tab.

   The Security Console displays the *Policies* page.
2. In the *Policy Listing* table, click the name of the policy that includes the rule for which you want to override the result.

   The Security Console displays the page for the policy.

3. In the *Tested Assets* table, click the name or IP address of an asset.
4. The Security Console displays the page for the asset. Note that the navigation bread crumb for the page includes the site that contains the asset. In the *Configuration Policy Rules* table, click the **Override** icon for the rule that you want to override.

   The Security Console displays a *Create Policy Override* pop-up window.
5. Select *This asset only* from the **Scope** drop-down list.
6. Select an override type from the drop-down list:
   - *Pass* indicates that you consider an asset to be compliant with the rule.
   - *Fail* indicates that you consider an asset to be non-compliant with the rule.
   - *Fixed* indicates that the issue that caused a Fail result has been remediated. A Fixed override will cause the result to appear as a Pass in reports and result listings.
   - *Not Applicable* indicates that the rule does not apply to the asset.
7. Enter your reason for requesting the override. A reason is required.



Submitting an asset-specific override

8. If you only have override request permission, click **Submit** to place the override under review and have another individual in your organization review it. The override request appears in the *Override History* table of the rule page.

   OR

   If you have override approval permission, click **Submit and approve**.

Submitting an override of a rule for a specific scan on a single asset

1. Click the **Policies** tab.

   The Security Console displays the *Policies* page.

2. In the *Policy Listing* table, click the name of the policy that includes the rule for which you want to override the result.

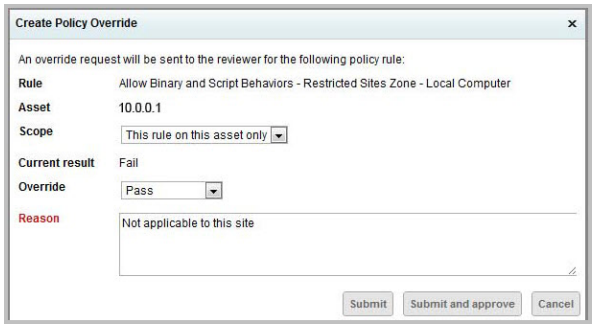
   The Security Console displays the page for the policy.

3. In the *Tested Assets* table, click the name or IP address of an asset.

4. The Security Console displays the page for the asset. Note that the navigation bread crumb for the page includes the site that contains the asset. In the *Configuration Policy Rules* table, click the **Override** icon for the rule that you want to override.

   The Security Console displays a *Create Policy Override* pop-up window.

5. Select *This rule on this asset only* from the **Scope** drop-down list.
6. Select an override type from the drop-down list:
   - *Pass* indicates that you consider an asset to be compliant with the rule.
   - *Fail* indicates that you consider an asset to be non-compliant with the rule.
   - *Fixed* indicates that the issue that caused a Fail result has been remediated. A Fixed override will cause the result to appear as a Pass in reports and result listings.
   - *Not Applicable* indicate that the rule does not apply to the asset.
7. Enter your reason for requesting the override. A reason is required.



Submitting an asset-specific override

8. If you only have override request permission, click **Submit** to place the override under review and have another individual in your organization review it. The override request appears in the *Override History* table of the rule page.

   OR

   If you have override approval permission, click **Submit and approve**.

Reviewing an override request

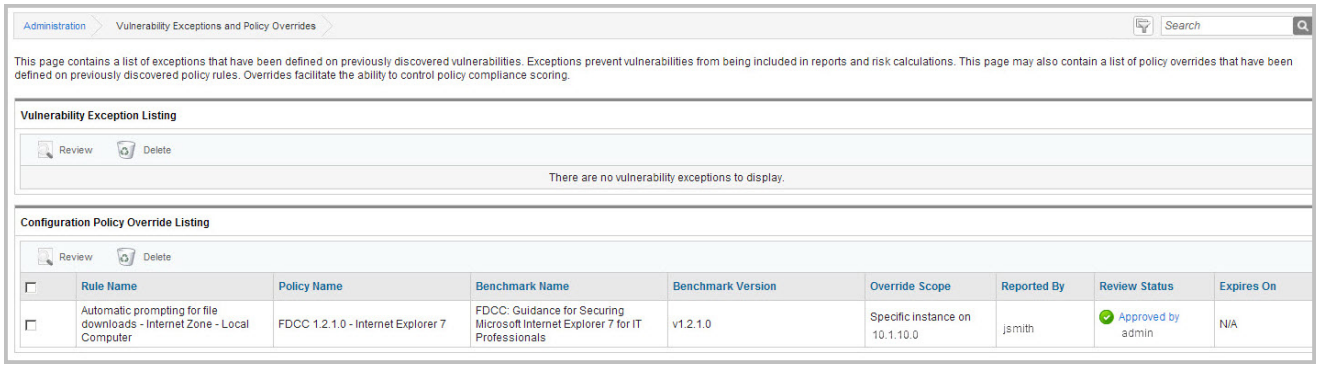
Upon reviewing an override request, you can either approve or reject it.

1. Click the **Administration** tab of the Security Console Web interface.
2. On the *Administration* page, click the **Manage** link next to *Exceptions and Overrides*.
3. Locate the request in the *Configuration Policy Override Listing* table.

To select multiple requests for review, select each desired row.

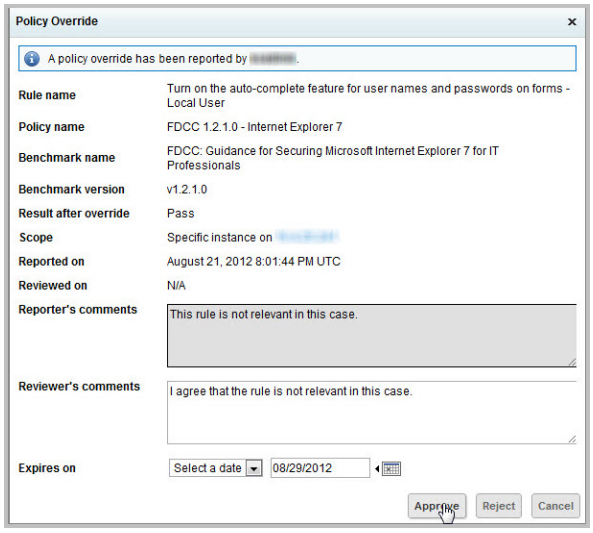
OR, to select all requests for review, select the top row.

4. Click the **Under review** link in the *Review Status* column.
5. In the *Review Status* dialog box, read the comments by the user who submitted the request and decide whether to approve or reject the request.



Selecting an override request to review

6. Enter comments in the **Reviewer's Comments** text box. Doing so may be helpful for the submitter.
7. If you want to select an expiration date for override, click the calendar icon and select a date.
8. Click **Approve** or **Reject**, depending on your decision.



Approving an override request

The result of the review appears in the *Review Status* column. Also, if the rule has never been previously overridden and the override request has been approved, its entry will switch to *Yes* in the *Active Overrides* column in the *Configuration Policy Rules* table of the page. The override will also be noted in the *Override History* table of the rule page.

Deleting an override or override request

You can delete old override exception requests.

1. Click the **Administration** tab of the Security Console Web interface.
2. On the *Administration* page, click the **Manage** link next to *Exceptions and Overrides*.

   Tip: You also can click the top row check box to select all requests and then delete them all in one step.

3. In the *Configuration Policy Override Listing* table, select the check box next to the rule override that you want to delete.

   To select multiple requests for deletion, select each desired row.

   OR, to select all requests for deletion, select the top row.

4. Click the **Delete** icon. The entry no longer appears in the *Configuration Policy Override Listing* table.

Act

After you discover what is running in your environment and assess your security threats, you can initiate actions to remediate these threats.

Act provides guidance on making stakeholders in your organization aware of security priorities in your environment so that they can take action.

Working with asset groups on page 315: Asset groups allow you to create logical groupings so you can discover and scan assets. Asset groups also allow Global Administrators to control which assets are available to different stakeholders.

Working with reports on page 351: With reports, you share critical security information with different stakeholders in your organization. This section guides you through creating and customizing reports and understanding the information they contain.

Using tickets on page 569: This section shows you how to use the ticketing system to manage the remediation work flow and delegate remediation tasks.

Working with asset groups

Asset groups provide different ways for members of your organization to grant access to, view, scan, and report on asset information. Asset groups allow you to create logical groupings that you can configure to dynamically incorporate new assets that meet specific criteria. You can define an asset group within a site in order to scan based on these groupings.

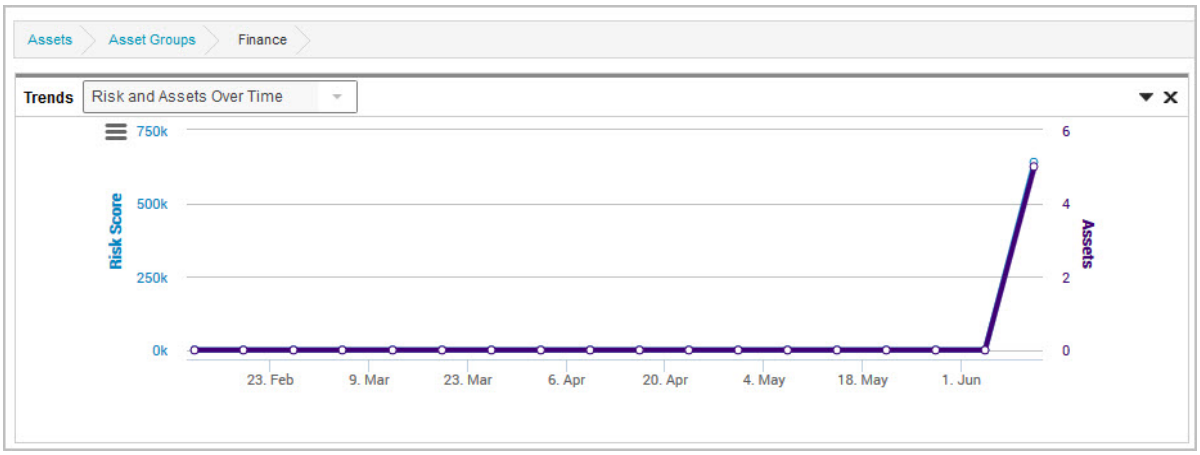
Using asset groups to your advantage

One use case illustrates how asset groups can "spin off" organically from sites. A bank purchases Nexpose with a fixed-number IP address license. The network topology includes one head office and 15 branches, all with similar "cookie-cutter" IP address schemes. The IP addresses in the first branch are all 10.1.1.x.; the addresses in the second branch are 10.1.2.x; and so on. For each branch, whatever integer equals .x is a certain type of asset. For example .5 is always a server.

The security team scans each site and then "chunks" the information in various ways by creating reports for specific asset groups. It creates one set of asset groups based on locations so that branch managers can view vulnerability trends and high-level data. The team creates another set of asset groups based on that last integer in the IP address. The users in charge of remediating server vulnerabilities will only see ".5" assets. If the "x" integer is subject to more granular divisions, the security team can create more finally specialized asset groups. For example .51 may correspond to file servers, and .52 may correspond to database servers.

Another approach to creating asset groups is categorizing them according to membership. For example, you can have an "Executive" asset group for senior company officers who see high-level business-sensitive reports about all the assets within your enterprise. You can have more technical asset groups for different members of your security team, who are responsible for remediating vulnerabilities on specific types of assets, such as databases, workstations, or Web servers.

The page for an asset group displays charts so you can track your risk or number of vulnerabilities in relation to the assets in that group.

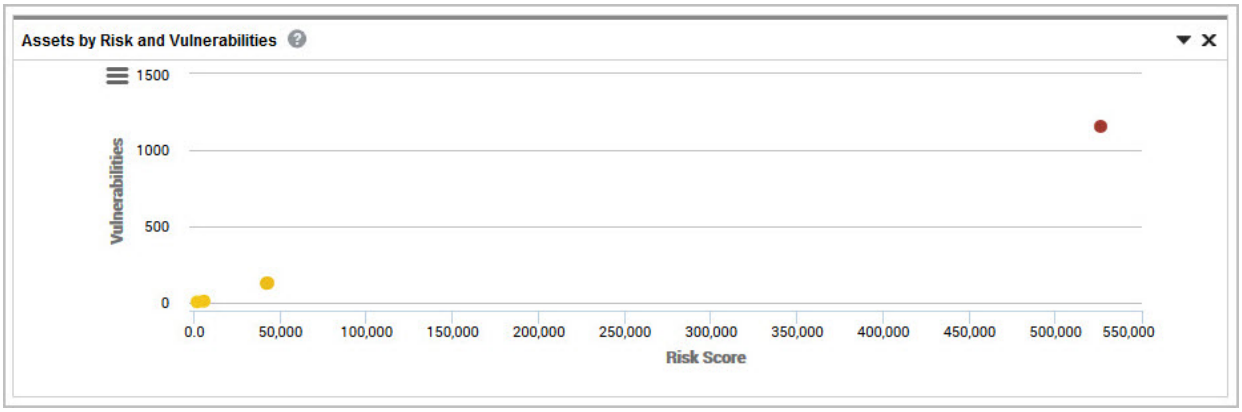


Asset Risk and Vulnerabilites Over Time



For the trend charts, use the drop-down list to switch the view to risk score or vulnerabilities. Click and drag on the chart to zoom to a specific time period.

The *Assets by Risk and Vulnerabilities* chart appears as a scatter chart, unless you have 7,000 assets or more in the asset group. In that case, it appears as a bubble chart, and you can click on a bubble to see a scatter chart of a specific group of assets.



Assets by Risk and Vulnerabilities

On the scatter chart, each dot represents an asset. Hover over the dot to see information about the asset. Click it to go to the page for that asset.

Comparing dynamic and static asset groups

One way to think of an asset group is as a snapshot of your environment.

This snapshot provides important information about your assets and the security issues affecting them:

- their network location
- the operating systems running on them
- the number of vulnerabilities discovered on them
- whether exploits exist for any of the vulnerabilities
- their risk scores

With Nexpose, you can create two different kinds of "snapshots." The dynamic asset group is a snapshot that potentially changes with every scan; and the static asset group is an unchanging snapshot. Each type of asset group can be useful depending on your needs.

Using dynamic asset groups

A dynamic asset group contains scanned assets that meet a specific set of search criteria. You define these criteria with asset search filters, such as IP address range or hosted operating systems. The list of assets in a dynamic group is subject to change with every scan. In this regard, a dynamic asset group differs from a static asset group. See *How are sites different from asset groups?* on page 48. Assets that no longer meet the group's Asset Filter criteria after a scan will be removed from the list. Newly discovered assets that meet the criteria will be added to the list.

Note that the list does not change immediately, but after the application completes a scan and integrates the new asset information in the database.

An ever-evolving snapshot of your environment, a dynamic asset group allows you to track changes to your live asset inventory and security posture at a quick glance, and to create reports based on the most current data. For example, you can create a dynamic asset group of assets with a vulnerability that was included in a Patch Tuesday bulletin. Then, after applying the patch for the vulnerability, you can scan the dynamic asset group to determine if any assets still have this vulnerability. If the patch application was successful, the group theoretically should not include any assets.

You can create dynamic asset groups using the filtered asset search. See *Performing filtered asset searches* on page 324.

You grant user access to dynamic asset groups through the *User Configuration* panel.

A user with access to a dynamic asset group will have access to newly discovered assets that meet group criteria regardless of whether or not those assets belong to a site to which the user does not have access. For example, you have created a dynamic asset group of Windows XP workstations. You grant two users, Joe and Beth, access to this dynamic asset group. You scan a site to which Beth has access and Joe does not. The scan discovers 50 new Windows XP workstations. Joe and Beth will both be able to see the 50 new Windows XP workstations in the dynamic asset group list and include them in reports, even though Joe does not have access to the site that contains these same assets. When managing user access to dynamic asset groups, you need to assess how these groups will affect site permissions. To ensure that a dynamic asset group does not include any assets from a given site, use the site filter. See *Locating assets by sites* on page 243.

Using static asset groups

A static asset group contains assets that meet a set of criteria that you define according to your organization's needs. Unlike with a dynamic asset group, the list of assets in a static group does not change unless you alter it manually.

Static asset groups provide useful time-frozen views of your environment that you can use for reference or comparison. For example, you may find it useful to create a static asset group of Windows servers and create a report to capture all of their vulnerabilities. Then, after applying patches and running a scan for patch verification, you can create a baseline report to compare vulnerabilities on those same assets before and after the scan.

You can create static asset groups through any of three options:

- using the *Group Configuration* panel; see *Configuring a static asset group by manually selecting assets* on page 318
- using the filtered asset search; see *Performing filtered asset searches* on page 324
- copying and modifying an existing asset group; see *Creating a dynamic or static asset group by copying an existing one* on page 321

Configuring a static asset group by manually selecting assets

Note: Only Global Administrators can create asset groups.

Manually selecting assets is one of three ways to create a static asset group. This manual method is ideal for environments that have small numbers of assets. For an approach that is ideal for large numbers of assets, see *Creating a dynamic or static asset group from asset searches* on page 348.

Start a static asset group configuration:

1. Go to the *Assets :: Asset Groups* page by one of the following routes:

   Click the **Assets** tab to go to the *Assets* page, and then click **view** next to *Groups*.

   OR

   Click the **Administration** tab to go to the Administration page, and then click **manage** next to *Groups.*

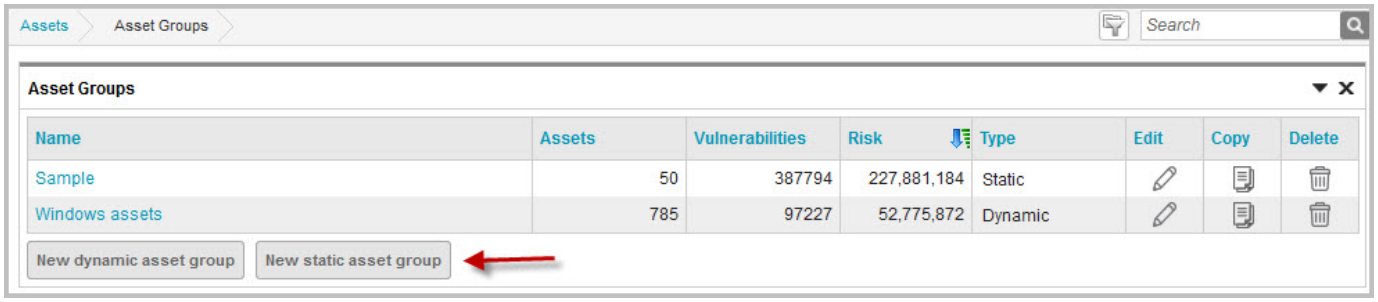
2. Click **New Static Asset Group** to create a new static asset group.

3. Click **Edit** to change any group listed with a static asset group icon.

   The *Asset Group Configuration* panel appears.

Note: You can only create an asset group after running an initial scan of assets that you wish to include in that group.

4. Click **New Static Asset Group**.



Creating a new static asset group

OR

Click **Create** next to *Asset Groups* on the *Administration* page.

The console displays the *General* page of the *Asset Group Configuration* panel.

5. Type a group name and description in the appropriate fields.
6. If you want to, add business context tags to the group. Any tag you add to a group will apply to all of the member assets. For more information and instructions, see *Applying RealContext with tags* on page 254.

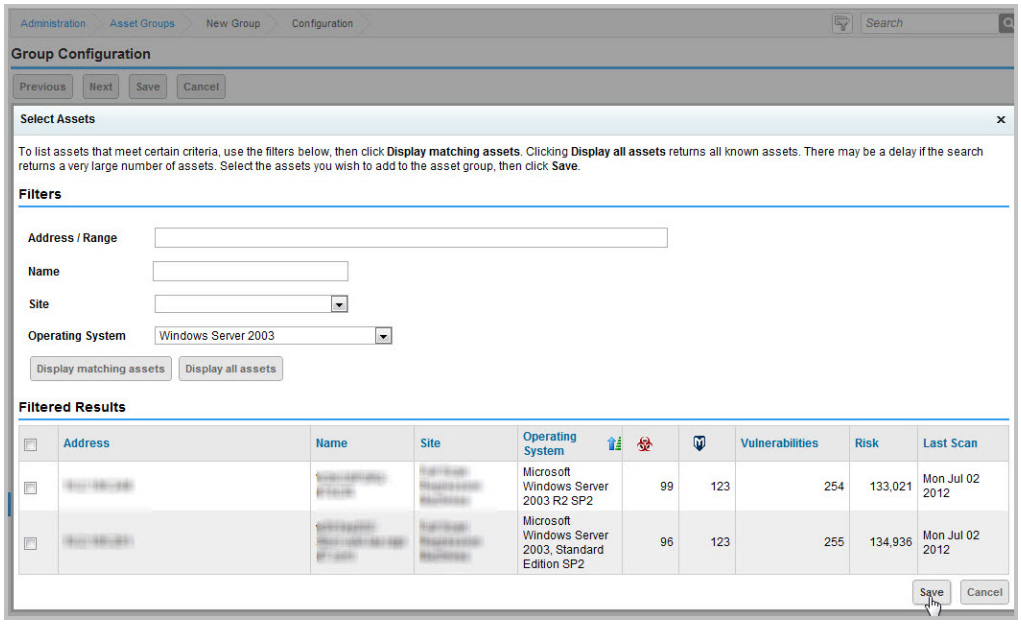
Adding assets to the static asset group:

1. Go to the *Assets* page of the *Asset Group Configuration* panel.

   The console displays a page with search filters.

2. Use any of these filters to find assets that meet certain criteria, then click **Display matching assets** to run the search.

   For example, you can select all of the assets within an IP address range that run on a particular operating system.



Selecting assets for a static asset group

OR

3. Click **Display all assets**, which is convenient if your database contains a small number of assets.

Note: There may be a delay if the search returns a very large number of assets.

4. Select the assets you wish to add to the asset group. To include all assets, select the check box in the header row.
5. Click **Save**.

   The assets appear on the *Assets* page.

   When you use this asset selection feature to create a new asset group, you will not see any assets displayed. When you use this asset selection feature to edit an existing report, you will see the list of assets that you selected when you created, or most recently edited, the report.
6. Click **Save** to save the new asset group information.

You can repeat the asset search to include multiple sets of search results in an asset group. You will need to save a set of results before proceeding to the next results. If you do not save a set of selected search results, the next search will clear that set.

Creating a dynamic or static asset group by copying an existing one

You can create a new dynamic or static group by copying an existing one. This method is useful when you want to create an asset group that is similar to an existing one, but with some differences.

To copy an asset group:

1. From the *Home* page, in the *Asset Groups* listing, select the **Copy** icon for the asset group you want to copy.



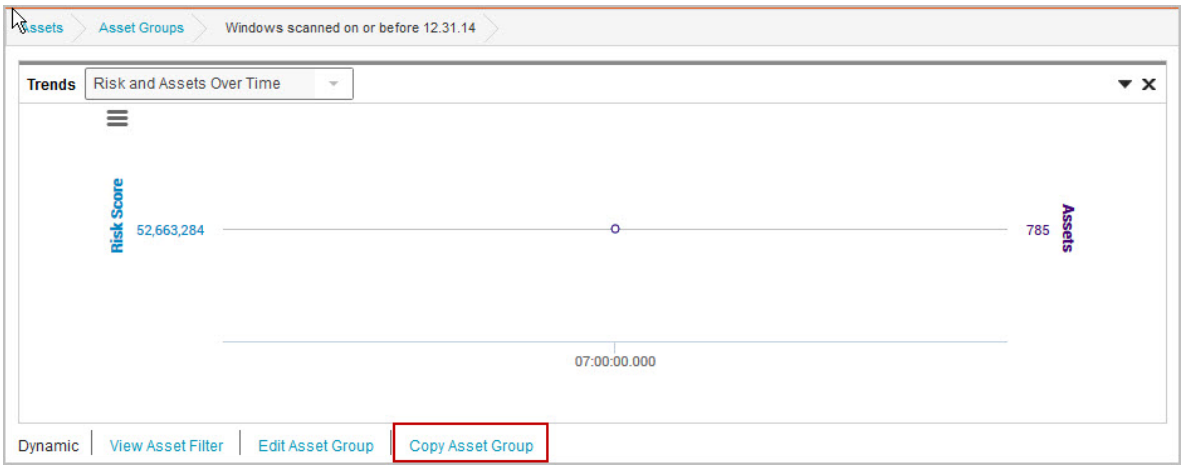
OR

From the asset group listing, select the **Copy** icon for the asset group you want to copy.



OR

From the asset group details, select **Copy Asset Group**.

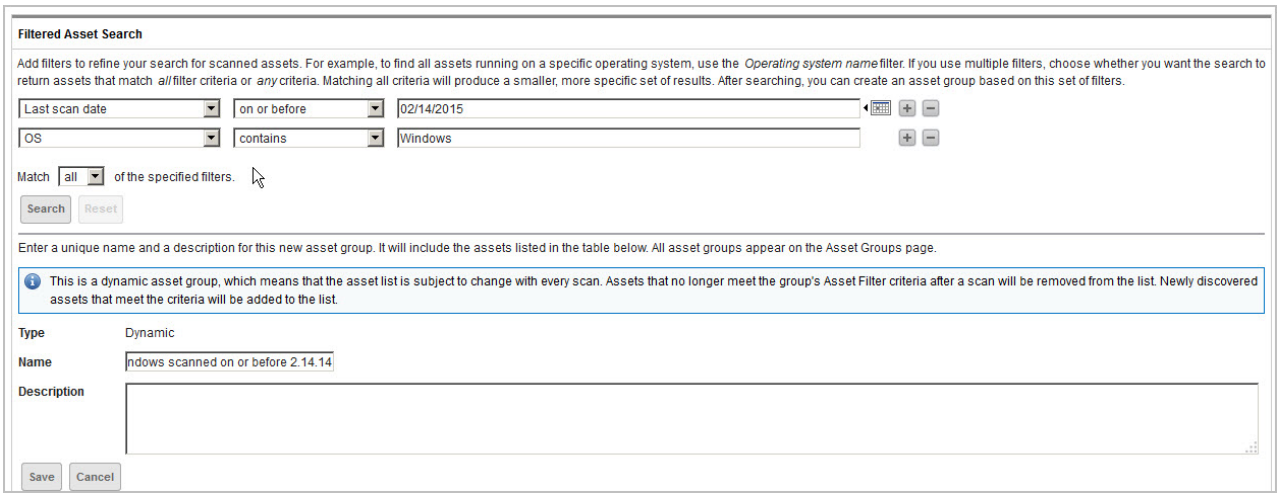


Copying an asset group from the asset group details page

2. The asset group configuration page appears. Make the changes to the settings and rename the asset group appropriately.

   Note: By default, *Copy* will be appended to the original name. Additional copies of the original group will have a number appended (for example, *Copy 2* and so on).

3. Click **Save**. The new asset group will not be created until you save.



Making changes to a copied dynamic asset group configuration

Performing filtered asset searches

When dealing with networks of large numbers of assets, you may find it necessary or helpful to concentrate on a specific subset. The filtered asset search feature allows you to search for assets based on criteria that can include IP address, site, operating system, software, services, vulnerabilities, and asset name. You can then save the results as a dynamic asset group for tracking, scanning, and reporting purposes. See *Using the search feature* on page 34.

Using search filters, you can find assets of immediate interest to you. This helps you to focus your remediation efforts and to manage the sheer quantity of assets running on a large network.

To start a filtered asset search:

Click the **Asset Filter** icon  , which appears next to the **Search** box in the Web interface.

The *Filtered asset search* page appears.

OR

Click the **Administration** tab to go to the *Administration* page, and then click the *dynamic* link next to *Asset Groups.*

OR

Note: Performing a filtered asset search is the first step in creating a dynamic asset group

Click **New Dynamic Asset Group** if you are on the *Asset Groups* page.

Configuring asset search filters

A search filter allows you to choose the attributes of the assets that you are interested in. You can add multiple filters for more precise searches. For example, you could create filters for a given IP address range, a particular operating system, and a particular site, and then combine these filters to return a list of all the assets that simultaneously meet all the specified criteria. Using fewer filters typically increases the number of search results.

You can combine filters so that the search result set contains only the assets that meet all of the criteria in all of the filters (leading to a smaller result set). Or you can combine filters so that the search result set contains any asset that meets all of the criteria in any given filter (leading to a larger result set). See *Combining filters* on page 346.

The following asset search filters are available:

Filtering by asset name on page 327

Filtering by CVE ID on page 327

Filtering by host type on page 328

Filtering by IP address range on page 329

Filtering by IP address type on page 328

Filtering by last scan date on page 330

Filtering by mobile device last sync time on page 331

Filtering by other IP address type on page 332

Filtering by operating system name on page 332

Filtering by PCI compliance status on page 333

Filtering by service name on page 333

Filtering by open port numbers on page 331

Filtering by operating system name on page 332

Filtering by software name on page 334

Filtering by presence of validated vulnerabilities on page 334

Filtering by user-added criticality level on page 335

Filtering by user-added custom tag on page 335

Filtering by user-added tag (location) on page 336

Filtering by user-added tag (owner) on page 337

Filtering by vAsset cluster on page 339

Filtering by vAsset datacenter on page 339

Filtering by vAsset host on page 340

Filtering by vAsset power state on page 340

Filtering by vAsset resource pool path on page 340

Filtering by CVSS risk vectors on page 341

Filtering by vulnerability category on page 342

Filtering by vulnerability CVSS score on page 343

Filtering by vulnerability exposures on page 344

Filtering by vulnerability risk scores on page 345

Filtering by vulnerability title on page 345

To select filters in the *Filtered asset search* panel take the following steps:

1. Use the first drop-down list.

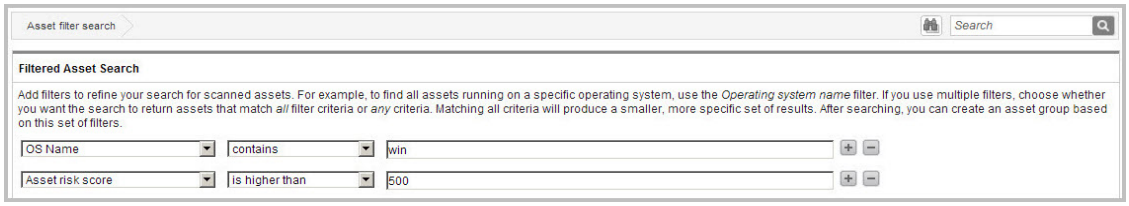
   When you select a filter, the configuration options, *operators*, for that filter dynamically become available.

2. Select the appropriate operator. Note: Some operators allow text searches. You can use the * wildcard in any of the text searches.

3. Use the **+** button to add filters.

4. Use the **-** button to remove filters.

5. Click **Reset** to remove all filters.



Asset search filters

Filtering by asset name

The asset name filter lets you search for assets based on the asset name. The filter applies a search string to the asset names, so that the search returns assets that meet the specified criteria. It works with the following operators:

- *is* returns all assets whose names match the search string exactly.
- *is not* returns all assets whose names do not match the search string.
- *starts with* returns all assets whose names begin with the same characters as the search string.
- *ends with* returns all assets whose names end with the same characters as the search string.
- *contains* returns all assets whose names contain the search string anywhere in the name.
- *does not contain* returns all assets whose names do not contain the search string.

After you select an operator, you type a search string for the asset name in the blank field.

Filtering by CVE ID

The *CVE ID* filter lets you search for assets based on the CVE ID. The CVE identifiers (IDs) are unique, common identifiers for publicly known information security vulnerabilities. For more information, see https://cve.mitre.org/cve/identifiers/index.html. The filter applies a search string to the CVE IDs, so that the search returns assets that meet the specified criteria. It works with the following operators:

- *is* returns all assets whose CVE IDs match the search string exactly.
- *is not* returns all assets whose CVE IDs do not match the search string.
- *contains* returns all assets whose CVE IDs contain the search string anywhere in the name.
- *does not contain* returns all assets whose CVE IDs do not contain the search string.

After you select an operator, you type a search string for the CVE ID in the blank field.

Filtering by host type

The *Host type* filter lets you search for assets based on the type of host system, where assets can be any one or more of the following types:

- *Bare metal* is physical hardware.
- *Hypervisor* is a host of one or more virtual machines.
- *Virtual machine* is an all-software guest of another computer.
- *Unknown* is a host of an indeterminate type.

You can use this filter to track, and report on, security issues that are specific to host types. For example, a hypervisor may be considered especially sensitive because if it is compromised then any guest of that hypervisor is also at risk.

The filter applies a search string to host types, so that the search returns a list of assets that either match, or do not match, the selected host types.

It works with the following operators:

- *is* returns all assets that match the host type that you select from the adjacent drop-down list.
- *is not* returns all assets that do not match the host type that you select from the adjacent drop-down list.

You can combine multiple host types in your criteria to search for assets that meet multiple criteria. For example, you can create a filter for “is Hypervisor” and another for “is virtual machine” to find all-software hypervisors.

Filtering by IP address type

If your environment includes IPv4 and IPv6 addresses, you can find assets with either address format. This allows you to track and report on specific security issues in these different segments of your network. The *IP address type* filter works with the following operators:

- *is* returns all assets that have the specified address format.
- *is not* returns all assets that do not have the specified address formats.

After selecting the filter and desired operator, select the desired format: *IPv4* or *IPv6*.

Filtering by IP address range

The *IP address range* filter lets you specify a range of IP addresses, so that the search returns a list of assets that are either in the IP range, or not in the IP range. It works with the following operators:

- *is* returns all assets with an IP address that falls within the IP address range.
- *is not* returns all assets whose IP addresses do not fall into the IP address range.

When you select the *IP address range filter*, you will see two blank fields separated by the word *to*. You use the left field to enter the start of the IP address range, and use the right to enter the end of the range.

The format for IPv4 addresses is a “dotted quad.” Example:

```
192.168.2.1 to 192.168.2.254
```

Filtering by last scan date

The last scan date filter lets you search for assets based on when they were last scanned. You may want, for example, to run a report on the most recently scanned assets. Or, you may want to find assets that have not been scanned in a long time and then delete them from the database because they are no longer be considered important for tracking purposes. The filter works with the following operators:

- *on or before* returns all assets that were last scanned on or before a particular date. After selecting this operator, click the calendar icon to select the date.
- *on or after* returns all assets that were last scanned on or after a particular date. After selecting this operator, click the calendar icon to select the date.
- *between and including* returns all assets that were last scanned between, and including, two dates. After selecting this operator, click the calendar icon next to the left field to select the first date in the range. Then click the calendar icon next to the right field to select the last date in the range.
- *earlier than* returns all assets that were last scanned earlier than a specified number of days preceding the date on which you initiate the search. After selecting this operator, enter a number in the *days ago* field. The starting point of the search is midnight of the day that the search is performed. For example, you initiate a search at 3 p.m. on January 23. You select this operator and enter *3* in the *days ago* field. The search returns all assets that were last scanned prior to midnight on January 20.
- *within the last* returns all assets that were last scanned within a specified number of preceding days. After selecting this operator, enter a number in the *days* field. The starting point of the search is midnight of the day that the search is performed. For example: You initiate the search at 3 p.m. on January 23. You select this operator and enter *1* in the *days* field. The search returns all assets that were last scanned since midnight on January 22.

Keep several things in mind when using this filter:

- The search only returns *last* scan dates. If an asset was scanned within the time frame specified in the filter, and if that scan was not the most recent scan, it will not appear in the search results.
- Dynamic asset group membership can change as new scans are run.
- Dynamic asset group membership is recalculated daily at midnight. If you create a dynamic asset group based on searches with the relative-day operators (*earlier than* or *within the last*), the asset membership will change accordingly.

Filtering by mobile device last sync time

Note: This filter is only available with WinRM/PowerShell and WinRM/Office 365 Dynamic Discovery connections.

With the *Last Synch Time* filter, you can track mobile devices based on the most recent time they synchronized with the Exchange server. This filter can be useful if you do not want your reports to include data from old devices that are no longer in use on the network. It works with the following operators.

- *earlier than* returns all mobile devices that synchronized earlier than a number of preceding days that you enter in a text box.
- *within the last* returns all mobile devices that synchronized within a number of preceding days that you enter in a text box.

Filtering by open port numbers

Having certain ports open may violate configuration policies. The *open port number* filter lets you search for assets with a specified port open. By isolating assets with open ports, you can then close those ports and then re-scan them to verify that they are closed. Select an operator, and then enter your port or port range. Depending on your criteria, search results will return assets that have open ports, assets that do not have open ports, and assets with a range of open ports.

The filter works with the following operators:

- *is* returns all assets with that port open.
- *is not* returns all assets that do not have that port open.
- *is* in the range of returns all assets within a range of designated ports.

Filtering by operating system name

The *operating system name* filter lets you search for assets based on their hosted operating systems. Depending on the search, you choose from a list of operating systems, or enter a search string. The filter returns a list of assets that meet the specified criteria.

It works with the following operators:

- *contains* returns all assets running on the operating system whose name contains the characters specified in the search string. You enter the search string in the adjacent field. You can use an asterisk (*) as a wildcard character.
- *does not contain* returns all assets running on the operating system whose name does not contain the characters specified in the search string. You enter the search string in the adjacent field. You can use an asterisk (*) as a wildcard character.
- *is empty* returns all assets that do not have an operating system identified in their scan results. If an operating system is not listed for a scanned asset in the Web interface or reports, this means that the asset may not have been fingerprinted. If the asset was scanned with credentials, failure to fingerprint indicates that the credentials were not authenticated on the target asset. Therefore, this operator is useful for finding assets that were scanned with failed credentials or without credentials.
- *is not empty* returns all assets that have an operating system identified in their scan results. This operator is useful for finding assets that were scanned with authenticated credentials and fingerprinted.

Filtering by other IP address type

This filter allows you to find assets that have other IPv4 or IPv6 addresses in addition to the address(es) that you are aware of. When the application scans an IP address that has been included in a site configuration, it discovers any other addresses for that asset. This may include

addresses that have not been scanned. For example: A given asset may have an IPv4 address and an IPv6 address. When configuring scan targets for your site, you may have only been aware of the IPv4 address, so you included only that address to be scanned in the site configuration. When you run the scan, the application discovers the IPv6 address. By using this asset search filter, you can search for all assets to which this scenario applies. You can add the discovered address to a site for a future scan to increase your security coverage.

After you select the filter and operators, you select either *IPv4* or *IPv6* from the drop-down list.

The filter works with one operator:

- *is* returns all assets that have other IP addresses that are either IPv4 or IPv6.

Filtering by PCI compliance status

The *PCI status* filter lets you search for assets based on whether they return Pass or Fail results when scanned with the PCI audit template. Finding assets that fail compliance scans can help you determine at a glance which require remediation in advance of an official PCI audit.

It works with two operators:

- *is* returns all assets that have a *Pass* or *Fail* status.
- *is not* returns all assets that do not have a *Pass* or *Fail* status.

After you select an operator, select the *Pass* or *Fail* option from the drop-down list.

Filtering by service name

The *service name* filter lets you search for assets based on the services running on them. The filter applies a search string to service names, so that the search returns a list of assets that either have or do not have the specified service.

It works with the following operators:

- *contains* returns all assets running a service whose name contains the search string. You can use an asterisk (*) as a wildcard character.
- *does not contain* returns all assets that do not run a service whose name contains the search string. You can use an asterisk (*) as a wildcard character.

After you select an operator, you type a search string for the service name in the blank field.

Filtering by site name

The *site name* filter lets you search for assets based on the name of the site to which the assets belong.

This is an important filter to use if you want to control users' access to newly discovered assets in sites to which users do not have access. See the note in *Using dynamic asset groups* on page 317.

The filter applies a search string to site names, so that the search returns a list of assets that either belong to, or do not belong to, the specified sites.

It works with the following operators:

- *is* returns all assets that belong to the selected sites. You select one or more sites from the adjacent list.
- *is not* returns all assets that do not belong to the selected sites. You select one or more sites from the adjacent list.

Filtering by software name

The *software name* filter lets you search for assets based on software installed on them. The filter applies a search string to software names, so that the search returns a list of assets that either runs or does not run the specified software.

It works with the following operators:

- *contains* returns all assets with software installed such that the software's name contains the search string. You can use an asterisk (*) as a wildcard character.
- *does not contain* returns all assets that do not have software installed such that the software's name does not contain the search string. You can use an asterisk (*) as a wildcard character.

After you select an operator, you enter the search string for the software name in the blank field.

Filtering by presence of validated vulnerabilities

The *Validated vulnerabilities* filter lets you search for assets with vulnerabilities that have been validated with exploits through Metasploit integration. By using this filter, you can isolate assets with vulnerabilities that have been proven to exist with a high degree of certainty. For more information, see *Working with validated vulnerabilities* on page 276.

The filter works with one operator:

- The *are* operator, combined with the *present* drop-down list option, returns all assets with validated vulnerabilities.
- The *are* operator, combined with the *not present* drop-down list option, returns all assets without validated vulnerabilities.

Filtering by user-added criticality level

The *user-added criticality level* filter lets you search for assets based on the criticality tags that you and your users have applied to them. For example, a user may set all assets belonging to company executives to be of a "Very High" criticality in their organization. Using this filter, you could identify assets with that criticality set, regardless of their sites or other associations. You can search for assets with or without a specific criticality level, assets whose criticality is above or below a specific level, or assets with or without any criticality set. For more information on criticality levels, see *Applying RealContext with tags* on page 254.

The filter works with the following operators:

- *is* returns all assets that are set to a specified criticality level.
- *is not* returns all assets are not set to a specified criticality level.
- *is higher than* returns all assets whose criticality level is higher than the specified level.
- *is lower than* returns all assets whose criticality level is lower than the specified level.
- *is applied* returns all assets that have any criticality set.
- *is not applied* returns all assets that have no criticality set.

After you select an operator, you select a criticality level from the drop-down menu. Available criticality levels are *Very High*, *High*, *Medium*, *Low*, and *Very Low*.

Filtering by user-added custom tag

The *user-added custom tag* filter lets you search for assets based on the custom tags that users have applied to them. For example, your company may have assets involved in an online banking process distributed throughout various locations and subnets, and a user may have tagged the involved assets with a custom "Online Banking" tag. Using this filter, you could identify assets with that tag, regardless of their sites or other associations. You can search for assets with or without a specific tag, assets whose custom tags meet certain criteria, or assets with or without any user-

added custom tags. For more information on user-added custom tags, see *Applying RealContext with tags* on page 254.

The filter works with the following operators:

- *is* returns all assets with custom tags that match the search string exactly.
- *is not* returns all assets that do not have a custom tag that matches the exact search string.
- *starts with* returns all assets with custom tags that begin with the same characters as the search string.
- *ends with* returns all assets with custom tags that end with the same characters as the search string.
- *contains* returns all assets whose custom tags contain the search string anywhere in their names.
- *does not contain* returns all assets whose custom tags do not contain the search string.
- *is applied* returns all assets that have any custom tag applied.
- *is not applied* returns all assets that have no custom tags applied.

After you select an operator, you type a search string for the custom tag in the blank field.

Filtering by user-added tag (location)

The *user-added tag (location)* filter lets you search for assets based on the location tags that users have applied to them. For example, a user may have created and applied tags for “Akron” and “Cincinnati” to clarify the physical location of assets in a user-friendly way. Using this filter, you could identify assets with that tag, regardless of their other associations. You can search for assets with or without a specific tag, assets whose location tags meet certain criteria, or assets with or without any user-added location tags. For more information on user-added location tags, see *Applying RealContext with tags* on page 254.

The filter works with the following operators:

- *is* returns all assets with location tags that match the search string exactly.
- *is not* returns all assets that do not have a location tag that matches the exact search string.
- *starts with* returns all assets with location tags that begin with the same characters as the search string.
- *ends with* returns all assets with location tags that end with the same characters as the search string.
- *contains* returns all assets whose location tags contain the search string anywhere in their names.
- *does not contain* returns all assets whose location tags do not contain the search string.
- *is applied* returns all assets that have any location tag applied.
- *is not applied* returns all assets that have no location tags applied.

After you select an operator, you type a search string for the location tag in the blank field.

Filtering by user-added tag (owner)

The *user-added tag (owner)* filter lets you search for assets based on the owner tags that users have applied to them. For example, a company may have different people responsible for different assets. A user can tag the assets each person is responsible for and use this information to track the risk level of those assets. You can search for assets with or without a specific tag, assets whose owner tags meet certain criteria, or assets with or without any user-added owner tags. For more information on user-added owner tags, see *Applying RealContext with tags* on page 254.

The filter works with the following operators:

- *is* returns all assets with owner tags that match the search string exactly.
- *is not* returns all assets that do not have an owner tag that matches the exact search string.
- *starts with* returns all assets with owner tags that begin with the same characters as the search string.
- *ends with* returns all assets with owner tags that end with the same characters as the search string.
- *contains* returns all assets whose owner tags contain the search string anywhere in their names.
- *does not contain* returns all assets whose owner tags do not contain the search string.
- *is applied* returns all assets that have any owner tag applied.
- *is not applied* returns all assets that have no owner tags applied.

After you select an operator, you type a search string for the location tag in the blank field.

Using vAsset filters

The following *vAsset* filters let you search for virtual assets that you track with vAsset discovery. Creating dynamic asset groups for virtual assets based on specific criteria can be useful for analyzing different segments of your virtual environment. For example, you may want to run reports or assess risk for all the virtual assets used by your accounting department, and they are all supported by a specific resource pool. For information about vAsset discovery, see *Discovering virtual machines managed by VMware vCenter or ESX/ESXi* on page 167.

Filtering by vAsset cluster

The *vAsset cluster* filter lets you search for virtual assets that belong, or don't belong, to specific clusters. This filter works with the following operators:

- *is* returns all assets that belong to clusters whose names match an entered string exactly.
- *is not* returns all assets that belong to clusters whose names do not match an entered string.
- *contains* returns all assets that belong to clusters whose names contain an entered string.
- *does not contain* returns all assets that belong to clusters whose names do not contain an entered string.
- *starts with* returns all assets that belong to clusters whose names begin with the same characters as an entered string.

After you select an operator, you enter the search string for the cluster in the blank field.

Filtering by vAsset datacenter

The *vAsset datacenter* filter lets you search for assets that are managed, or are not managed, by specific datacenters. This filter works with the following operators:

- *is* returns all assets that are managed by datacenters whose names match an entered string exactly.
- *is not* returns all assets that are managed by datacenters whose names do not match an entered string.

After you select an operator, you enter the search string for the datacenter name in the blank field.

Filtering by vAsset host

The *vAsset host* filter lets you search for assets that are guests, or are not guests, of specific host systems. This filter works with the following operators:

- *is* returns all assets that are guests of hosts whose names match an entered string exactly.
- *is not* returns all assets that are guests of hosts whose names do not match an entered string.
- *contains* returns all assets that are guests of hosts whose names contain an entered string.
- *does not contain* returns all assets that are guests of hosts whose names do not contain an entered string.
- *starts with* returns all assets that are guests of hosts whose names begin with the same characters as an entered string.

After you select an operator, you enter the search string for the host name in the blank field.

Filtering by vAsset power state

The *vAsset power state* filter lets you search for assets that are in, or are not in, a specific power state. This filter works with the following operators:

- *is* returns all assets that are in a power state selected from a drop-down list.
- *is not* returns all assets that not are in a power state selected from a drop-down list.

After you select an operator, you select a power state from the drop-down list. Power states include *on*, *off*, or *suspended*.

Filtering by vAsset resource pool path

The *vAsset resource pool path* filter lets you discover assets that belong, or do not belong, to specific resource pool paths. This filter works with the following operators:

- *contains* returns all assets that are supported by resource pool paths whose names contain an entered string.
- *does not contain* returns all assets that are supported by resource pool paths whose names do not contain an entered string.

You can specify any level of a path, or you can specify multiple levels, each separated by a hyphen and right arrow: ->. This is helpful if you have resource pool path levels with identical names.

For example, you may have two resource pool paths with the following levels:

Human Resources

Management

Workstations

Advertising

Management

Workstations

The virtual machines that belong to the *Management* and *Workstations* levels are different in each path. If you only specify *Management* in your filter, the search will return all virtual machines that belong to the *Management* and *Workstations* levels in both resource pool paths.

However, if you specify *Advertising -> Management -> Workstations*, the search will only return virtual assets that belong to the *Workstations* pool in the path with *Advertising* as the highest level.

After you select an operator, you enter the search string for the resource pool path in the blank field.

Filtering by CVSS risk vectors

The filters for the following Common Vulnerability Scoring System (CVSS) risk vectors let you search for assets based on vulnerabilities that pose different types or levels of risk to your organization's security:

- *CVSS Access Complexity (AC)*
- *CVSS Access Vector (AV)*
- *CVSS Authentication Required (Au)*
- *CVSS Availability Impact (A)*
- *CVSS Confidentiality Impact (C)*
- *CVSS Integrity Impact (I)*

These filters refer to the industry-standard vectors used in calculating CVSS scores and PCI severity levels. They are also used in risk strategy calculations for risk scores. For detailed information about CVSS vectors, go to the National Vulnerability Database Web site at nvd.nist.gov/cvss.cfm.

Using these filters, you can find assets based on different exploitability attributes of the vulnerabilities found on them, or based on the different types and degrees of impact to the asset in the event of compromise through the vulnerabilities found on them. Isolating these assets can help you to make more informed decisions on remediation priorities or to prepare for a PCI audit.

All six filters work with two operators:

- *is* returns all assets that match a specific risk level or attribute associated with the CVSS vector.
- *is not* returns all assets that do not match a specific risk level or attribute associated with the CVSS vector.

After you select a filter and an operator, select the desired impact level or likelihood attribute from the drop-down list:

- For each of the three impact vectors (*Confidentiality*, *Integrity*, and *Availability*), the options are *Complete*, *Partial*, or *None*.
- For *CVSS Access Vector*, the options are *Local (L)*, *Adjacent (A)*, or *Network (N)*.
- For *CVSS Access Complexity*, the options are *Low*, *Medium*, or *High*.
- For *CVSS Authentication Required*, the options are *None*, *Single*, or *Multiple*.

Filtering by vulnerability category

The *vulnerability category* filter lets you search for assets based on the categories of vulnerabilities that have been flagged on them during scans. This is a useful filter for finding out at a quick glance how many, and which, assets have a particular type of vulnerability, such as ones related to Adobe, Cisco, or Telnet. Lists of vulnerability categories can be found in the *Vulnerability Checks* section of the scan template configuration or the report configuration, where you can filter report scope based on vulnerabilities.

The filter applies a search string to vulnerability categories, so that the search returns a list of assets that either have or do not have vulnerabilities in categories that match that search string. It works with the following operators:

- *contains* returns all assets with a vulnerability whose category contains the search string. You can use an asterisk (*) as a wildcard character.
- *does not contain* returns all assets that do not have a vulnerability whose category contains the search string. You can use an asterisk (*) as a wildcard character.
- *is* returns all assets with that have a vulnerability whose category matches the search string exactly.
- *is not* returns all assets that do not have a vulnerability whose category matches the exact search string.
- *starts with* returns all assets with vulnerabilities whose categories begin with the same characters as the search string.
- *ends with* returns all assets with vulnerabilities whose categories end with the same characters as the search string.

After you select an operator, you type a search string for the vulnerability category in the blank field.

Filtering by vulnerability CVSS score

The *Vulnerability CVSS score* filter lets you search for assets with vulnerabilities that have a specific CVSS score or fall within a range of scores. You may find it helpful to create asset groups according to CVSS score ranges that correspond to PCI severity levels: low (0.0-3.9), medium (4.0-6.9), and high (7.0-10). Doing so can help you prioritize assets for remediation.

The filter works with the following operators:

- *is* returns all assets with vulnerabilities that have a specified CVSS score.
- *is not* returns all assets with vulnerabilities that do not have a specified CVSS score.
- *is in the range of* returns all assets with vulnerabilities that fall within the range of two specified CVSS scores and include the high and low scores in the range.
- *is higher than* returns all assets with vulnerabilities that have a CVSS score higher than a specified score.
- *is lower than* returns all assets with vulnerabilities that have a CVSS score lower than a specified score.

After you select an operator, type a score in the blank field. If you select the range operator, you would type a low score and a high score to create the range. Acceptable values include any numeral from 0.0 to 10. You can only enter one digit to the right of the decimal. If you enter more than one digit, the score is automatically rounded up. For example, if you enter a score of 2.25, the score is automatically rounded up to 2.3.

Filtering by vulnerability exposures

The *vulnerability exposures* filter lets you search for assets based on the following types of exposures known to be associated with vulnerabilities discovered on those assets:

- Malware kit exploits
- Metasploit exploits
- Exploit Database exploits

This is a useful filter for isolating and prioritizing assets that have a higher likelihood of compromise due to these exposures.

The filter applies a search string to one or more of the vulnerability exposure types, so that the search returns a list of assets that either have or do not have vulnerabilities associated with the specified exposure types. It works with the following operators:

- *includes* returns all assets that have vulnerabilities associated with specified exposure types.
- *does not include* returns all assets that do not have vulnerabilities associated with specified exposure types.

After you select an operator, select one or more exposure types in the drop-down list. To select multiple types, hold down the **<Ctrl>** key and click all desired types.

Filtering by vulnerability risk scores

The *vulnerability risk score* filter lets you search for assets with vulnerabilities that have a specific risk score or fall within a range of scores. Isolating and tracking assets with higher risk scores, for example, can help you prioritize remediation for those assets.

The filter works with the following operators:

- *is in the range of* returns all assets with vulnerabilities that fall within the range of two specified risk scores and include the high and low scores in the range.
- *is higher than* returns all assets with vulnerabilities that have a risk score higher than a specified score.
- *is lower than* returns all assets with vulnerabilities that have a risk score lower than a specified score.

After you select an operator, enter a score in the blank field. If you select the range operator, you would type a low score and a high score to create the range. Keep in mind your currently selected risk strategy when searching for assets based on risk scores. For example, if the currently selected strategy is Real Risk, you will not find assets with scores higher than 1,000. Refer to the risk scores in your vulnerability and asset tables for guidance.

Filtering by vulnerability title

The *vulnerability title* filter lets you search for assets based on the vulnerabilities that have been flagged on them during scans. This is a useful filter to use for verifying patch applications, or finding out at a quick glance how many, and which, assets have a particular high-risk vulnerability.

The filter applies a search string to vulnerability titles, so that the search returns a list of assets that either have or do not have the specified string in their titles. It works with the following operators:

- *contains* returns all assets with a vulnerability whose name contains the search string. You can use an asterisk (*) as a wildcard character.
- *does not contain* returns all assets that do not have a vulnerability whose name contains the search string. You can use an asterisk (*) as a wildcard character.
- *is* returns all assets with that have a vulnerability whose name matches the search string exactly.
- *is not* returns all assets that do not have a vulnerability whose name matches the exact search string.
- *starts with* returns all assets with vulnerabilities whose names begin with the same characters as the search string.
- *ends with* returns all assets with vulnerabilities whose names end with the same characters as the search string.

After you select an operator, you type a search string for the vulnerability name in the blank field.

Combining filters

If you create multiple filters, you can have Nexpose return a list of assets that match *all* the criteria specified in the filters, or a list of assets that match *any* of the criteria specified in the filters. You can make this selection in a drop-down list at the bottom of the *Search Criteria* panel.

The difference between *All* and *Any* is that the *All* setting will only return assets that match the search criteria in all of the filters, whereas the *Any* setting will return assets that match any given filter. For this reason, a search with *All* selected typically returns fewer results than *Any*.

For example, suppose you are scanning a site with 10 assets. Five of the assets run Linux, and their names are linux01, linux02, linux03, linux04, and linux05. The other five run Windows, and their names are win01, win02, win03, win04, and win05.

Suppose you create two filters. The first filter is an operating system filter, and it returns a list of assets that run Windows. The second filter is an asset filter, and it returns a list of assets that have “linux” in their names.

If you perform a filtered asset search with the two filters using the *All* setting, the search will return a list of assets that run Windows *and* have “linux” in their asset names. Since no such assets exist, there will be no search results. However, if you use the same filters with the *Any* setting, the search will return a list of assets that run Windows *or* have “linux” in their names. Five of the assets run Windows, and the other five assets have “linux” in their names. Therefore, the result set will contain all of the assets.

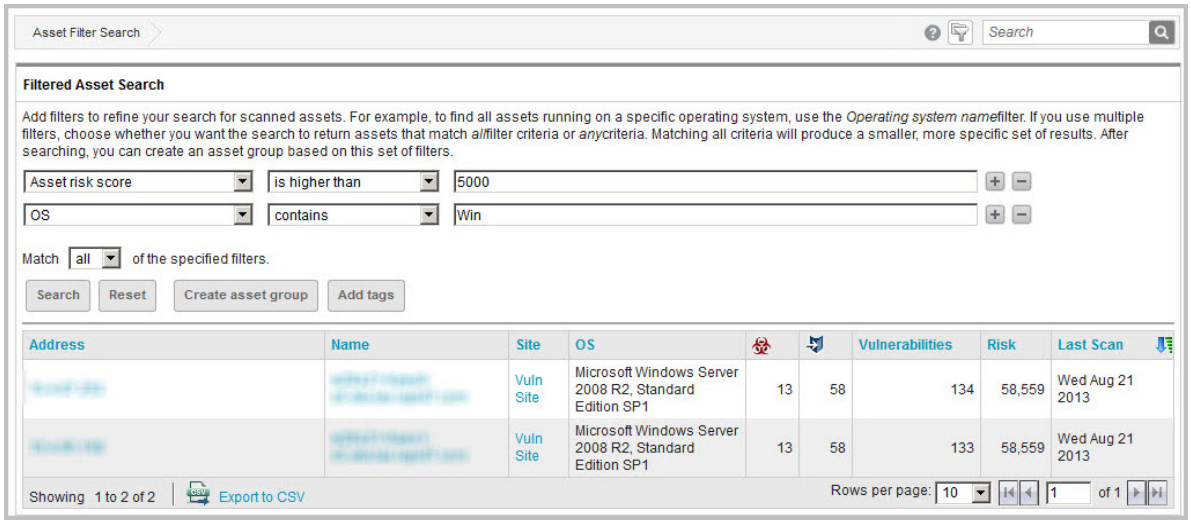
Creating a dynamic or static asset group from asset searches

After you configure asset search filters as described in the preceding section, you can create an asset group based on the search results. Using the assets search is the only way to create a dynamic asset group. It is one of two ways to create a static asset group and is more ideal for environments with large numbers of assets. For a different approach, which involves manually selecting assets, see *Configuring a static asset group by manually selecting assets* on page 318.

Note: If you have permission to create asset groups, you can save asset search results as an asset group.

1. After you configure asset search filters, click **Search**.

   A table of assets that meet the filter criteria appears.



Asset search results

   (Optional) Click the **Export to CSV** link at the bottom of the table to export the results to a comma-separated values (CSV) file that you can view and manipulate in a spreadsheet program.

Note: Only Global Administrators or users with the Manage Group Assets permission can create asset groups, so only these users can save Asset Filter search results.

2. Click **Create Asset Group**.

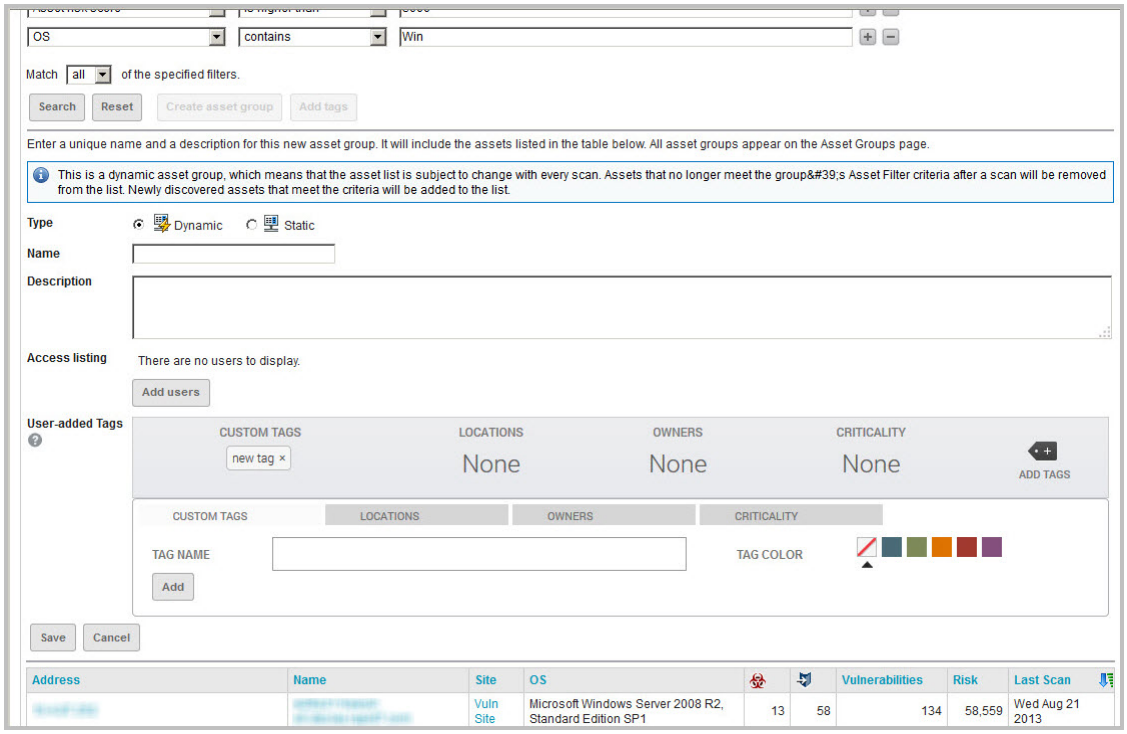
   Controls for creating an asset group appear.

3. Select either the **Dynamic** or **Static** option, depending on what kind of asset group you want to create. See *Comparing dynamic and static asset groups* on page 317.

   If you create a dynamic asset group, the asset list is subject to change with every scan. See *Using dynamic asset groups* on page 317.

4. Enter a unique asset group name and description.

   You must give users access to an asset group for them to be able view assets or perform asset-related operations, such as reporting, with assets in that group.



Creating a new dynamic asset group

Note: You must be a Global Administrator or have Manage Asset Group Access permission to add users to an asset group.

5. Click **Add Users.**

   The *Add Users* dialog box appears.

6. Select the check box for every user account that you want to add to the access list or select the check box in the top row to add all users.

Changing asset membership in a dynamic asset group

You can change search criteria for membership in a dynamic asset group at any time.

To change criteria for a dynamic asset group:

1. Go to the *Assets :: Asset Groups* page by one of the following routes:

   Click the **Administration** tab to go to the *Administration* page, and then click the **manage** link next to *Groups.*

   OR

   Click the **Assets** tab to go to the *Assets* page, and then click **view** next to *Groups*.

2. Click **Edit** to find a dynamic asset group that you want to modify.

   OR

   Click the link for the name of the desired asset group.



Starting to edit a dynamic asset group

   The console displays the page for that group.

3. Click **Edit Asset Group** or click **View Asset Filter** to review a summary of filter criteria.

   Any of these approaches causes the application to display the *Filtered asset search* panel with the filters set for the most recent asset search.

4. Change the filters according to your preferences, and run a search. See *Configuring asset search filters* on page 324.

5. Click **Save**.

Working with reports

You may want any number of people in your organization to view asset and vulnerability data without actually logging on to the Security Console. For example, a chief information security officer (CISO) may need to see statistics about your overall risk trends over time. Or members of your security team may need to see the most critical vulnerabilities for sensitive assets so that they can prioritize remediation projects. It may be unnecessary or undesirable for these stakeholders to access the application itself. By generating reports, you can distribute critical information to the people who need it via e-mail or integration of exported formats such as XML, CSV, or database formats.

Reports provide many, varied ways to look at scan data, from business-centric perspectives to detailed technical assessments. You can learn everything you need to know about vulnerabilities and how to remediate them, or you can just list the services are running on your network assets.

You can create a report on a site, but reports are not tied to sites. You can parse assets in a report any number of ways, including all of your scanned enterprise assets, or just one.

Note: For information about other tools related to compliance with Policy Manager policies, see *What are your compliance requirements?*, which you can download from the *Support* page in Help.

If you are verifying compliance with PCI, you will use the following report templates in the audit process:

- Attestation of Compliance
- PCI Executive Summary
- Vulnerability Details

If you are verifying compliance with United States Government Configuration Baseline (USGCB) or Federal Desktop Core Configuration (FDCC) policies, you can use the following report formats to capture results data:

- XCCDF Human Readable CSV Report
- XCCDF Results XML Report

Note: You also can click the top row check box to select all requests and then approve or reject them in one step.

You can also generate an XML export reports that can be consumed by the CyberScope application to fulfill the U.S. Government's Federal Information Security Management Act (FISMA) reporting requirements.

Reports are primarily how your asset group members view asset data. Therefore, it's a best practice to organize reports according to the needs of asset group members. If you have an asset group for Windows 2008 servers, create a report that only lists those assets, and include a section on policy compliance.

Creating reports is very similar to creating scan jobs. It's a simple process involving a configuration panel. You select or customize a report template, select an output format, and choose assets for inclusion. You also have to decide what information to include about these assets, when to run the reports, and how to distribute them.

All panels have the same navigation scheme. You can either use the navigation buttons in the upper-right corner of each panel page to progress through each page of the panel, or you can click a page link listed on the left column of each panel page to go directly to that page.

Note: Parameters labeled in red denote required parameters on all panel pages.

To save configuration changes, click **Save** that appears on every page. To discard changes, click **Cancel**.

Viewing, editing, and running reports

You may need to view, edit, or run existing report configurations for various reasons:

- On occasion, you may need to run an automatically recurring report immediately. For example, you have configured a recurring report on Microsoft Windows vulnerabilities. Microsoft releases an unscheduled security bulletin about an Internet Explorer vulnerability. You apply the patch for that flaw and run a verification scan. You will want to run the report to demonstrate that the vulnerability has been resolved by the patch.
- You may need to change a report configuration. For example, you may need add assets to your report scope as new workstations come online.

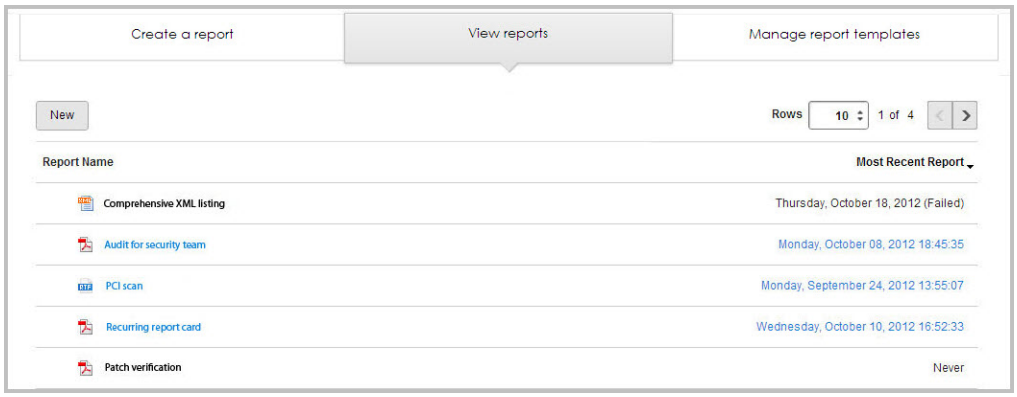
The application lists all report configurations in a table, where you can view run or edit them, or view the histories of when they were run in the past.

Note: On the *View Reports* panel, you can start a new report configuration by clicking the **New** button.

To view existing report configurations, take the following steps.

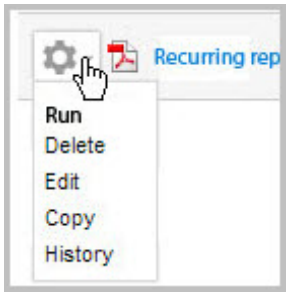
1. Click the **Reports** tab that appears on every page of the Web interface. The Security Console displays the *Reports* page.
2. Click the **View reports** panel to see all the reports of which you have ownership. A Global Administrator can see all reports.

A table list reports by name and most recent report generation date. You can sort reports by either criteria by clicking the column heading. Report names are unique in the application.



The View Reports panel

To edit or run a listed report, hover over the row for that report, and click the tool icon that appears.



Accessing report tools

- To run a report, click **Run**.

  Every time the application writes a new instance of a report, it changes the date in the *Most Recent Report* column. You can click the link for that date to view the most recent instance of the report.

- You also change a report configuration by clicking **Edit**.

- Or you can copy a configuration by clicking **Copy** on the tools drop-down menu for the report. Copying a template allows you to create a modified version that incorporates some the original template's attributes. It is a quick way to create a new report configuration that will have properties similar to those of another.

For example, you may have a report that only includes Windows vulnerabilities for a given set of assets. You may still want to create another report for those assets, focusing only on Adobe

vulnerabilities. Copying the report configuration would make the most sense if no other attributes are to be changed.

Whether you click **Edit** or **Copy**, the Security Console displays the *Configure a Report* panel for that configuration. See *Creating a basic report* on page 356.

- To view all instances of a report that have been run, click **History** in the tools drop-down menu for that report. You can also see the history for a report that has previously run at least once by clicking the report name, which is a hyperlink. If a report name is not a hyperlink, it is because an instance of the report has not yet run successfully. By reviewing the history, you can see any instances of the report that failed.
- Clicking **Delete** will remove the report configuration and all generated instances from the application database.

Creating a basic report

Creating a basic report involves the following steps:

- Selecting a report template and format
- Selecting assets to report on
- Filtering report scope with vulnerabilities (optional)
- Configuring report frequency (optional)

There are additional configuration steps for the following types of reports:

- Export
- Configuring an XCCDF report
- Configuring an ARF report
- Database Export
- Baseline reports
- Risk trend reports

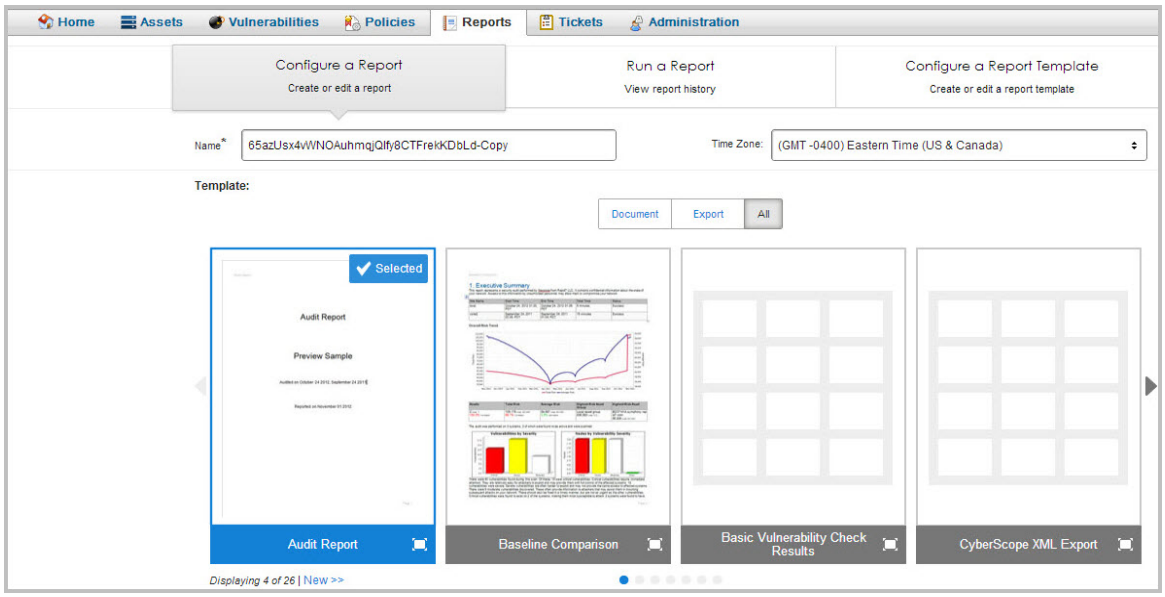
After you complete a basic report configuration, you will have the option to configure additional properties, such as those for distributing the report.

You will have the options to either save and run the report, or just to save it for future use. For example, if you have a saved report and want to run it one time with an additional site in it, you could add the site, save and run, return it to the original configuration, and then just save. See *Viewing, editing, and running reports* on page 353.

Starting a new report configuration

1. Click the **Reports** tab.

   The Security Console displays the *Create a report* panel.



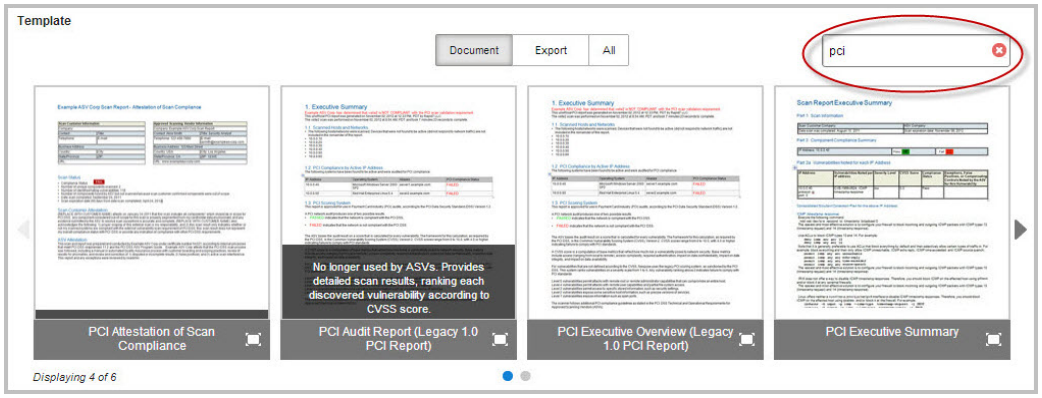
The Create a report panel

2. Enter a name for the new report. The name must be unique in the application.

3. Select a time zone for the report. This setting defaults to the local Security Console time zone, but allows for the time localization of generated reports.

4. *(Optional)* Enter a search term, or a few letters of the template you are looking for, in the **Search templates** field to see all available templates that contain that keyword or phrase. For example, enter `pci` and the display will change to display only PCI templates.

   Search results are dependent on the template type, either **Document** or **Export** templates. If you are unsure which template type you require, make sure you select **All** to search all available templates.



Search report templates

Note: Resetting the **Search templates** field by clicking the close X displays all templates in alphabetical order.

5. Select a template type:

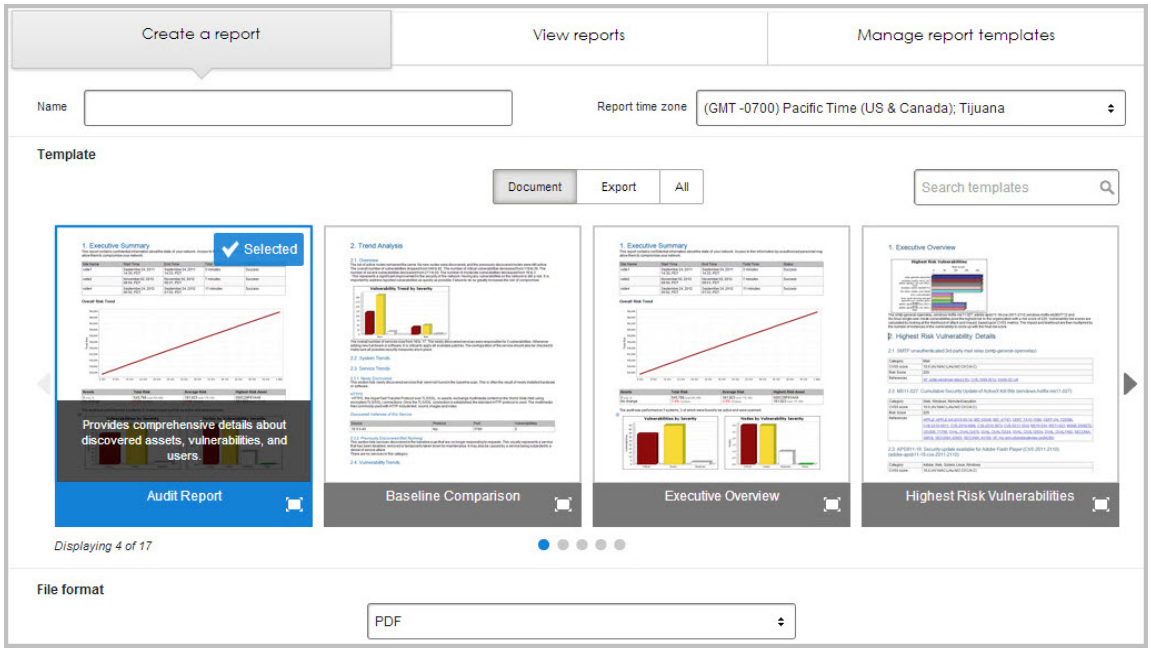
   - *Document* templates are designed for section-based, human-readable reports that contain asset and vulnerability information. Some of the formats available for this template type—Text, PDF, RTF, and HTML—are convenient for sharing information to be read by stakeholders in your organization, such as executives or security team members tasked with performing remediation.

   - *Export* templates are designed for integrating scan information into external systems. The formats available for this type include various XML formats, Database Export, and CSV. For more information, see *Working with report formats* on page 551.

6. Click **Close** on the **Search templates** field to reset the search or enter a new term.

The Security Console displays template thumbnail images that you can browse, depending on the template type you selected. If you selected the *All* option, you will be able to browse all available templates. Click the scroll arrows on the left and the right to browse the templates.

You can roll over the name of any template to view a description.



Selecting a report template

You also can click the **Preview** icon in the lower right corner of any thumbnail (highlighted in the preceding screen shot) to enlarge and click through a preview of template. This can be helpful to see what kind of sections or information the template provides.

When you see the see the desired template, click the thumbnail. It becomes highlighted and displays a *Selected* label in the top, right corner.

7. Select a format for the report. Formats not only affect how reports appear and are consumed, but they also can have some influence on what information appears in reports. For more information, see *Working with report formats* on page 551.

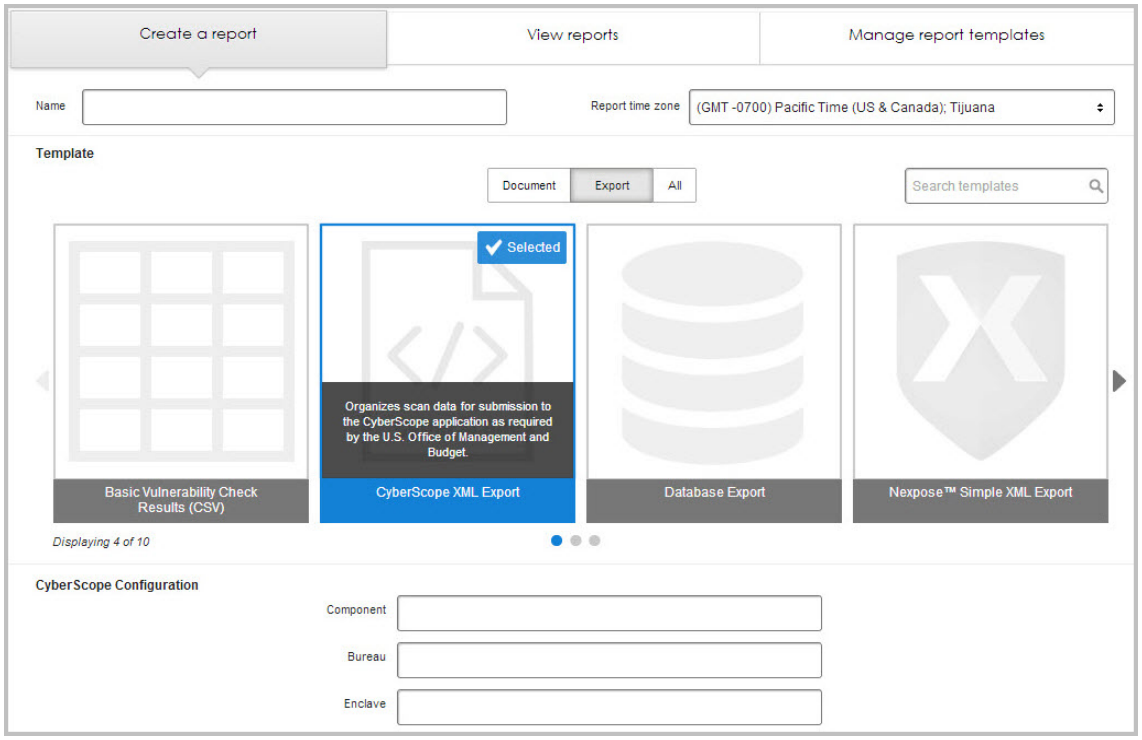
Tip: See descriptions of all available report templates to help you select the best template for your needs.

If you are using the *PCI Attestation of Compliance* or *PCI Executive Summary* template, or a custom template made with sections from either of these templates, you can only use the RTF format. These two templates require ASVs to fill in certain sections manually.

8. (Optional) Select the language for your report: Click **Advanced Settings**, select **Language**, and choose an output language from the drop-down list.

   To change the default language of reports, click your user name in the upper-right corner, select **User Preferences**, and select a language from the drop-down list. The newly selected default will apply to reports that you create after making this change. Reports created prior to the change retain their original language, unless you update them in the report configuration.

9. If you are using the CyberScope XML Export format, enter the names for the component, bureau, and enclave in the appropriate fields. For more information see *Entering CyberScope information* on page 361. Otherwise, continue with specifying the scope of your report.



Configuring a CyberScope XML Export report

Entering CyberScope information

When configuring a CyberScope XML Export report, you must enter additional information, as indicated in the *CyberScope Automated Data Feeds Submission Manual* published by the U.S. Office of Management and Budget. The information identifies the entity submitting the data:

- **Component** refers to a reporting component such as *Department of Justice*, *Department of Transportation*, or *National Institute of Standards and Technology*.
- **Bureau** refers to a component-bureau, an individual Federal Information Security Management Act (FISMA) reporting entity under the component. For example, a bureau under Department of Justice might be *Justice Management Division* or *Federal Bureau of Investigation*.
- **Enclave** refers to an enclave under the component or bureau. For example, an enclave under Department of Justice might be *United States Mint*. Agency administrators and agency points of contact are responsible for creating enclaves within CyberScope.

Consult the *CyberScope Automated Data Feeds Submission Manual* for more information.

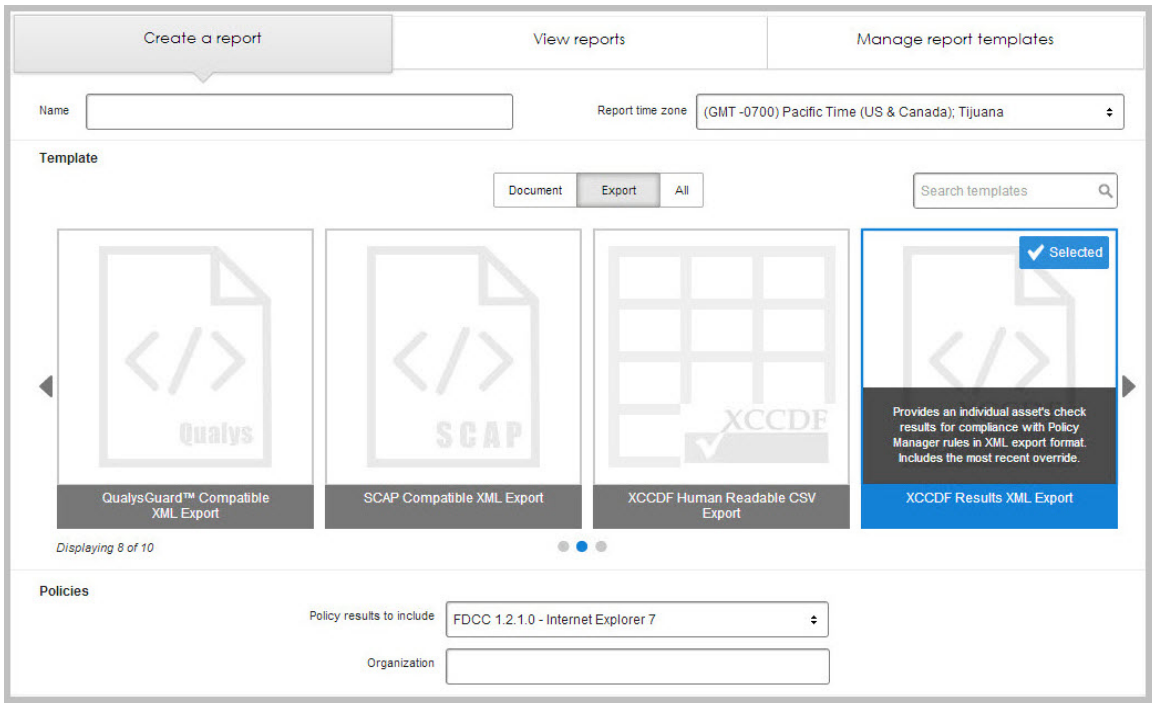
You must enter information in all three fields.

Configuring an XCCDF report

If you are creating one of the XCCDF reports, and you have selected one of the XCCDF formatted templates on the *Create a report* panel take the following steps:

Note: You cannot filter vulnerabilities by category if you are creating an XCCDF or CyberScope XML report.

1. Select an XCCDF report template on the *Create a report* panel.



Select an XCCDF formatted report template

2. Select the policy results to include from the drop-down list.

   The **Policies** option only appears when you select one of the XCCDF formats in the *Template* section of the *Create a report* panel.

3. Enter a name in the **Organization** field.

4. Proceed with asset selection. Asset selection is only available with the XCCDF Human Readable CSV Export.

Note: As described in Selecting Policy Manager checks, the major policy groups regularly release updated policy checks. The XCCDF report template will only generate reports that include the updated policy. To be able to run a report of this type on a scan that includes a policy that just changed, re-run the scan.

Configuring an Asset Reporting Format (ARF) export

Use the Asset Reporting Format (ARF) export template to submit policy or benchmark scan results to the U.S. government in compliance with Security Content Automation Protocol (SCAP) 1.2 requirements. To do so, take the following steps:

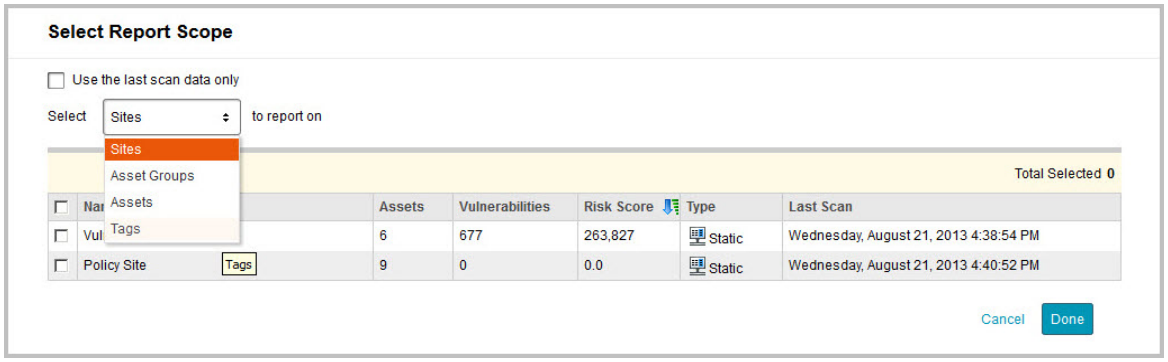
Note: To run ARF reports you must first run scans that have been configured to save SCAP data. See *Selecting Policy Manager checks* on page 608 for more information.

1. Select the ARF report template on the *Create a report* panel.
2. Enter a name for the report in the **Name** field.
3. Select the site, assets, or asset groups to include from *Scope* section.
4. Specify other advanced options for the report, such as report access, file storage, and distribution list settings.
5. Click **Run the report**.

   The report appears on the *View reports* page.

Selecting assets to report on

1. Click **Select sites, assets, asset groups, or tags** in the Scope section of the *Create a report* panel. The tags filter is available for all report templates except Audit Report, Baseline Comparison, Executive overview, Database export and XCCDF Human Readable CSV Export.
2. To use only the most recent scan data in your report, select **Use the last scan data only** check box. Otherwise, the report will include all historical scan data in the report.



Select Report Scope panel

Tip: The asset selection options are not mutually exclusive. You can combine selections of sites, asset groups, and individual assets.

3. Select *Sites*, *Asset Groups*, *Assets*, or *Tags* from the drop-down list.
4. If you selected *Sites*, *Asset Groups*, or *Tags*, click the check box for any displayed site or asset group to select it. You also can click the check box in the top row to select all options.

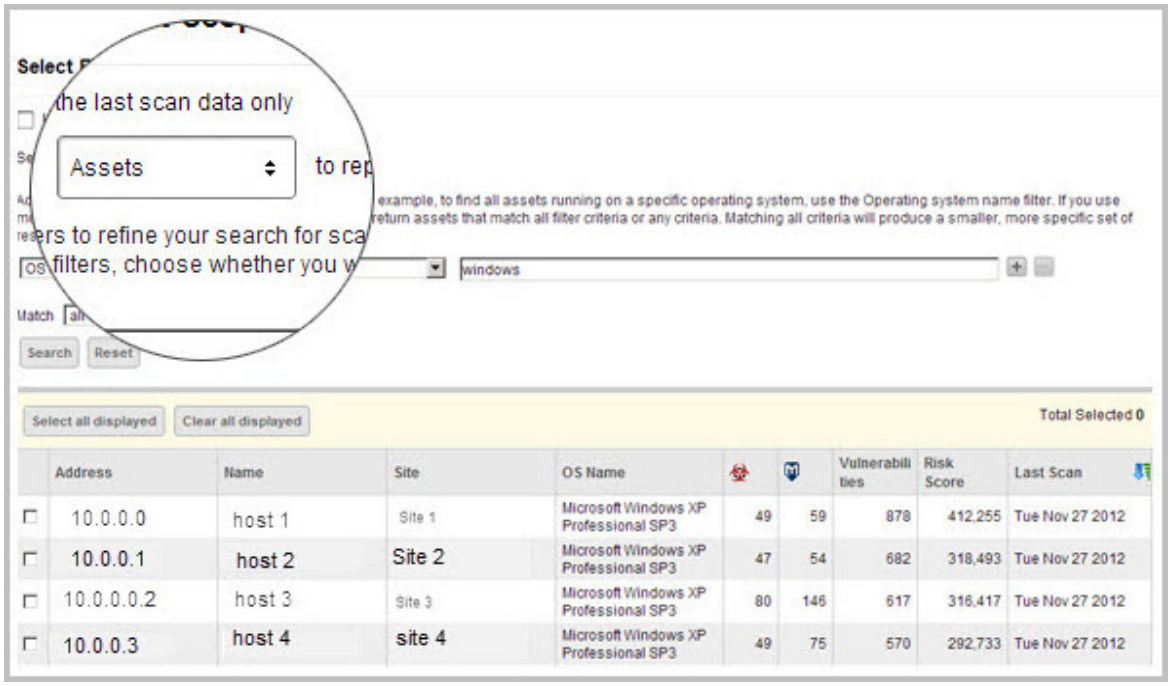
   If you selected *Assets*, the Security Console displays search filters. Select a filter, an operator, and then a value.

   For example, if you want to report on assets running Windows operating systems, select the operating system filter and the *contains* operator. Then enter *Windows* in the text field.

   To add more filters to the search, click the + icon and configure your new filter.

   Select an option to match any or all of the specified filters. Matching any filters typically returns a larger set of results. Matching all filters typically returns a smaller set of results because multiple criteria make the search more specific.

   Click the check box for any displayed asset to select it. You also can click the check box in the top row to select all options.



Selecting assets to report on

5. Click **OK** to save your settings and return the *Create a report* panel. The selections are referenced in the *Scope* section.



The Scope section

Filtering report scope with vulnerabilities

Filtering vulnerabilities means including or excluding specific vulnerabilities in a report. Doing so makes the report scope more focused, allowing stakeholders in your organization to see security-related information that is most important to them. For example, a chief security officer may only want to see critical vulnerabilities when assessing risk. Or you may want to filter out potential vulnerabilities from a CSV export report that you deliver to your remediation team.

You can also filter vulnerabilities based on category to improve your organization's remediation process. For example, a security administrator can filter vulnerabilities to make a report specific to a team or to a risk that requires attention. The security administrator can create reports that contain information about a specific type of vulnerability or vulnerabilities in a specific list of categories.

Reports can also be created to exclude a type of vulnerability or a list of categories. For example, if there is an Adobe Acrobat vulnerability in your environment that is addressed with a scheduled patching process, you can run a report that contains all vulnerabilities except those Adobe Acrobat vulnerabilities. This provides a report that is easier to read as unnecessary information has been filtered out.

Note: You can manage vulnerability filters through the API. See the API guide for more information.

Organizations that have distributed IT departments may need to disseminate vulnerability reports to multiple teams or departments. For the information in those reports to be the most effective, the information should be specific for the team receiving it. For example, a security administrator can produce remediation reports for the Oracle database team that only include vulnerabilities that affect the Oracle database. These streamlined reports will enable the team to more effectively prioritize their remediation efforts.

A security administrator can filter by vulnerability category to create reports that indicate how widespread a vulnerability is in an environment, or which assets have vulnerabilities that are not being addressed during patching. The security administrator can also include a list of historical vulnerabilities on an asset after a scan template has been edited. These reports can be used to monitor compliance status and to ensure that remediation efforts are effective.

The following document report template sections can include filtered vulnerability information:

- Discovered Vulnerabilities
- Discovered Services
- Index of Vulnerabilities
- Remediation Plan
- Vulnerability Exceptions
- Vulnerability Report Card Across Network
- Vulnerability Report Card by Node
- Vulnerability Test Errors

Therefore, report templates that contain these sections can include filtered vulnerability information. See *Fine-tuning information with custom report templates* on page 543.

The following export templates can include filtered vulnerability information:

- Basic Vulnerability Check Results (CSV)
- Nexpose™ Simple XML Export
- QualysGuard™ Compatible XML Export
- SCAP Compatible XML Export
- XML Export
- XML Export 2.0

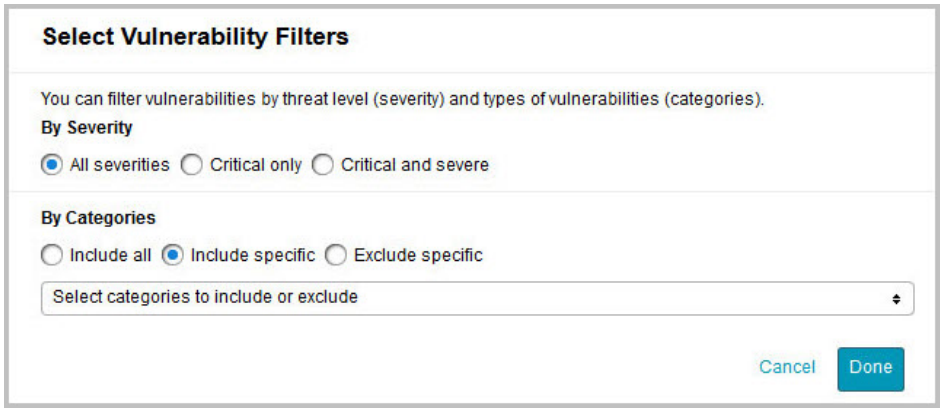
Vulnerability filtering is not supported in the following report templates:

- Cyberscope XML Export
- XCCDF XML
- XCCDF CSV
- Database Export

To filter vulnerability information, take the following steps:

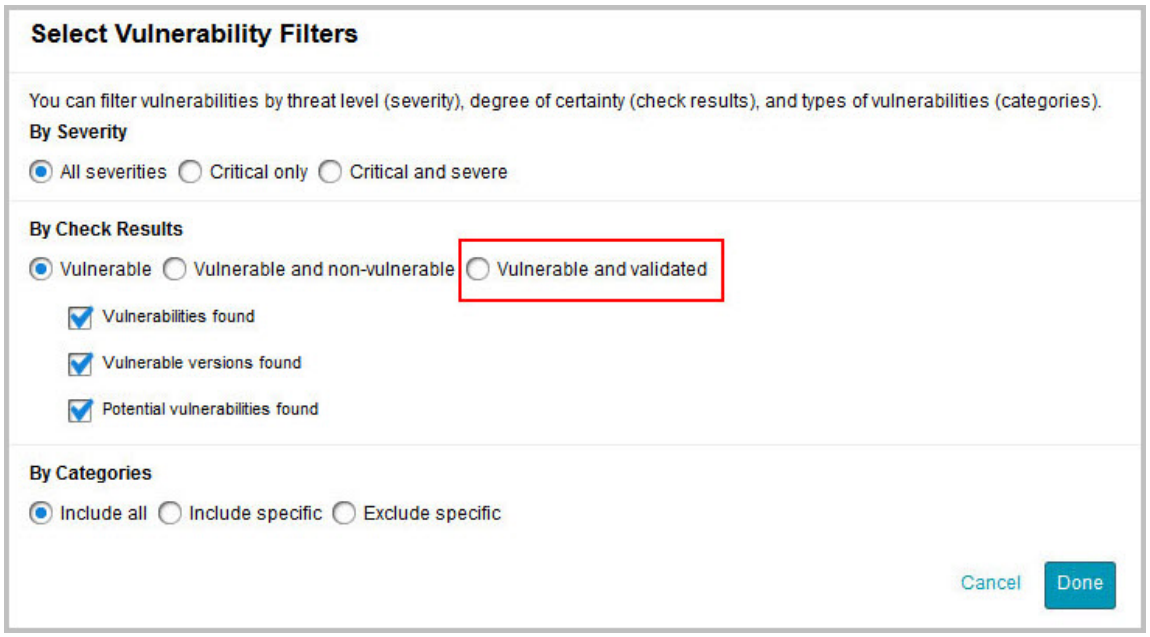
1. Click **Filter by Vulnerabilities** on the *Scope* section of the *Create a report* panel.

   Options appear for vulnerability filters.



Select Vulnerability Filters section

Certain templates allow you to include only validated vulnerabilities in reports: Basic Vulnerability Check Results (CSV), XML Export, XML Export 2.0, Top 10 Assets by Vulnerabilities, Top 10 Assets by Vulnerability Risk, Top Remediations, Top Remediations with Details, and Vulnerability Trends. Learn more about *Working with validated vulnerabilities* on page 276.



Select Vulnerability Filters section with option to include only validated vulnerabilities

2. To filter vulnerabilities by severity level, select the **Critical vulnerabilities** or **Critical and severe vulnerabilities** option. Otherwise, select **All severities**.

   These are not PCI severity levels or CVSS scores. They map to numeric severity rankings that are assigned by the application and displayed in the *Vulnerability Listing* table of the *Vulnerabilities* page. Scores range from 1 to 10:
   1-3=*Moderate*; 4-7=*Severe*; and 8-10=*Critical*.

3. If you selected a CSV report template, you have the option to filter vulnerability result types.

   To include all vulnerability check results (positive and negative), select the **Vulnerable and non-vulnerable** option next to *Results*.

   If you want to include only positive check results, select the **Vulnerable** option.

   You can filter positive results based on how they were determined by selecting any of the check boxes for result types:

   - **Vulnerabilities found**: Vulnerabilities were flagged because asset-specific vulnerability tests produced positive results. Vulnerabilities with this result type appear with the ve (vulnerable exploited) result code in CSV reports.

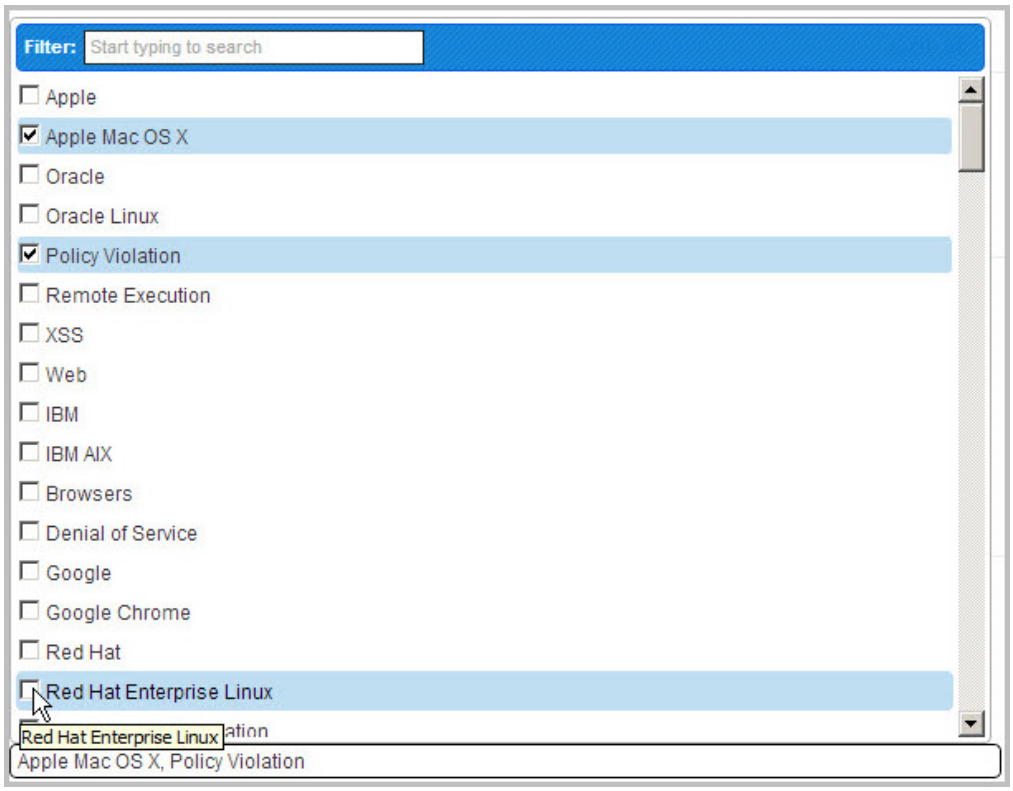
- **Vulnerabilities found**: Vulnerabilities were flagged because asset-specific vulnerability tests produced positive results. Vulnerabilities with this result type appear with the ve (vulnerable exploited) result code in CSV reports.
- **Vulnerabilities found**: Vulnerabilities were flagged because asset-specific vulnerability tests produced positive results. Vulnerabilities with this result type appear with the ve (vulnerable exploited) result code in CSV reports.

4. If you want to include or exclude specific vulnerability categories, select the appropriate option button in the *Categories* section.

   If you choose to include all categories, skip the following step.

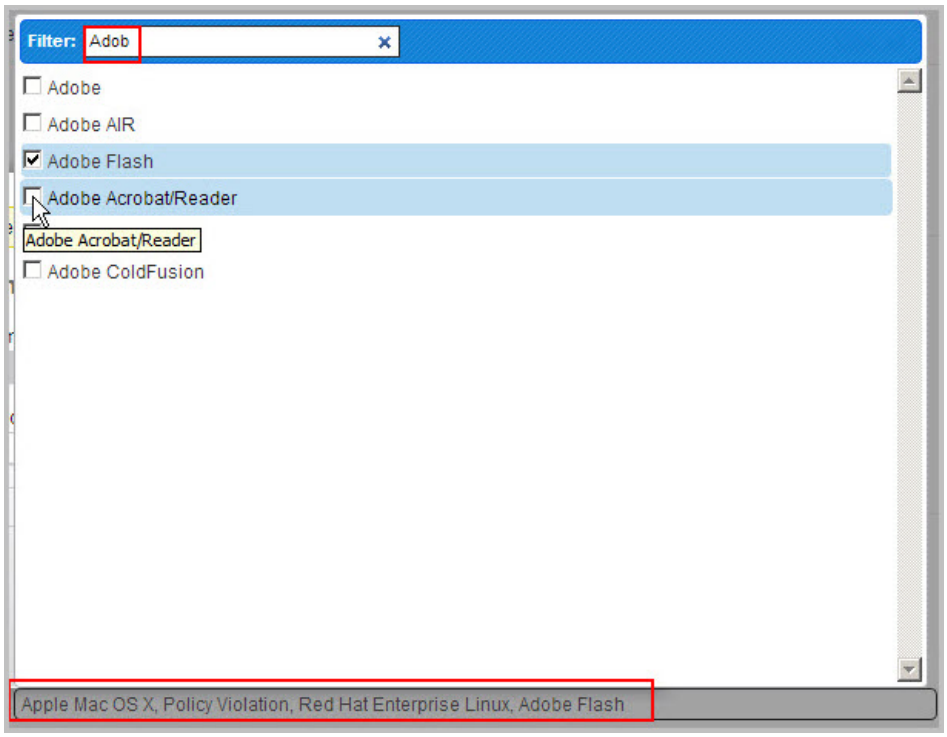
   Tip: Categories that are named for manufacturers, such as Microsoft, can serve as supersets of categories that are named for their products. For example, if you filter by the Microsoft category, you inherently include all Microsoft product categories, such as Microsoft Path and Microsoft Windows. This applies to other "company" categories, such as Adobe, Apple, and Mozilla.To view the vulnerabilities in a category see *Configuration steps for vulnerability check settings* on page 603.

5. If you choose to include or exclude specific categories, the Security Console displays a text box containing the words *Select categories*. You can select categories with two different methods:
   - Click the text box to display a window that lists all available categories. Scroll down the list and select the check box for each desired category. Each selection appears in a text field at the bottom of the window.



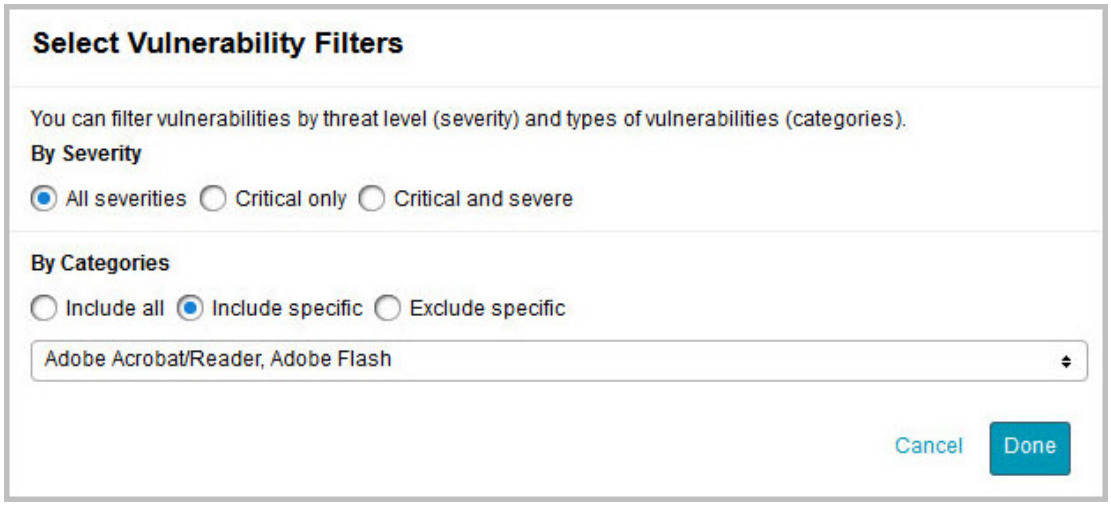
Selecting vulnerability categories by clicking check boxes

- Click the text box to display a window that lists all available categories. Enter part or all a category name in the **Filter:** text box, and select the categories from the list that appears. If you enter a name that applies to multiple categories, all those categories appear. For example, you type *Adobe* or *ado*, several Adobe categories appear. As you select categories, they appear in the text field at the bottom of the window.



Filter by category list

If you use either or both methods, all your selections appear in a field at the bottom of the selection window. When the list includes all desired categories, click outside of the window to return to the *Scope* page. The selected categories appear in the text box.



Selected vulnerability categories appear in the Scope section

Note: Existing reports will include all vulnerabilities unless you edit them to filter by vulnerability category.

6. Click the **OK** button to save scope selections.

Configuring report frequency

You can run the completed report immediately on a one-time basis, configure it to run after every scan, or schedule it to run on a repeating basis. The third option is useful if you have an asset group containing assets that are assigned to many different sites, each with a different scan template. Since these assets will be scanned frequently, it makes sense to run recurring reports automatically.

To configure report frequency, take the following steps:

1. Go to the *Create a report* panel.
2. Click **Configure advanced settings...**
3. Click **Frequency**.
4. Select a frequency option from the drop-down list:
   - Select **Run a one-time report now** to generate a report immediately, on a one-time basis.
   - Select **Run a recurring report after each scan** to generate a report every time a scan is completed on the assets defined in the report scope.
   - Select **Run a recurring report on a repeated schedule** if you wish to schedule reports for regular time intervals.

   If you selected either of the first two options, ignore the following steps.

   If you selected the scheduling option, the Security Console displays controls for configuring a schedule.
5. Enter a start date using the mm/dd/yyyy format.

   OR

   Click the calendar icon to select a start date.

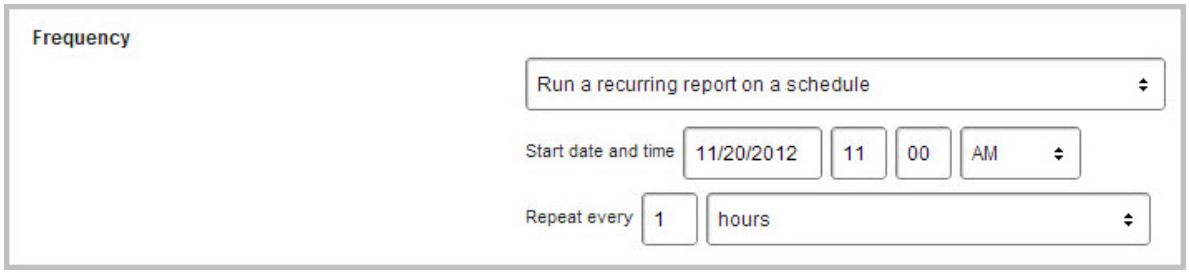
6. Enter an hour and minute for the start time, and click the **Up** or **Down** arrow to select *AM* or *PM*.

7. Enter a value in the field labeled **Repeat every**, and select a time unit from the drop-down list.to set a time interval for repeating the report.

   If you select *months on the specified date*, the report will run every month on the selected calendar date. For example, if you schedule a report to run on October 15, the report will run on October 15 every month.

   If you select *months on the specified day of the month*, the report will run every month on the same ordinal weekday. For example, if you schedule the first report to run on October 15, which is the third Monday of the month, the report will run every third Monday of the month.

   To run a report only once on the scheduled date and time, enter "0" in the field labeled **Repeat every**.



Creating a report schedule

Best practices for scheduling reports

The frequency with which you schedule and distribute reports depends your business needs and security policies. You may want to run quarterly executive reports. You may want to run monthly vulnerability reports to anticipate the release of Microsoft hotfix patches. Compliance programs, such as PCI, impose their own schedules.

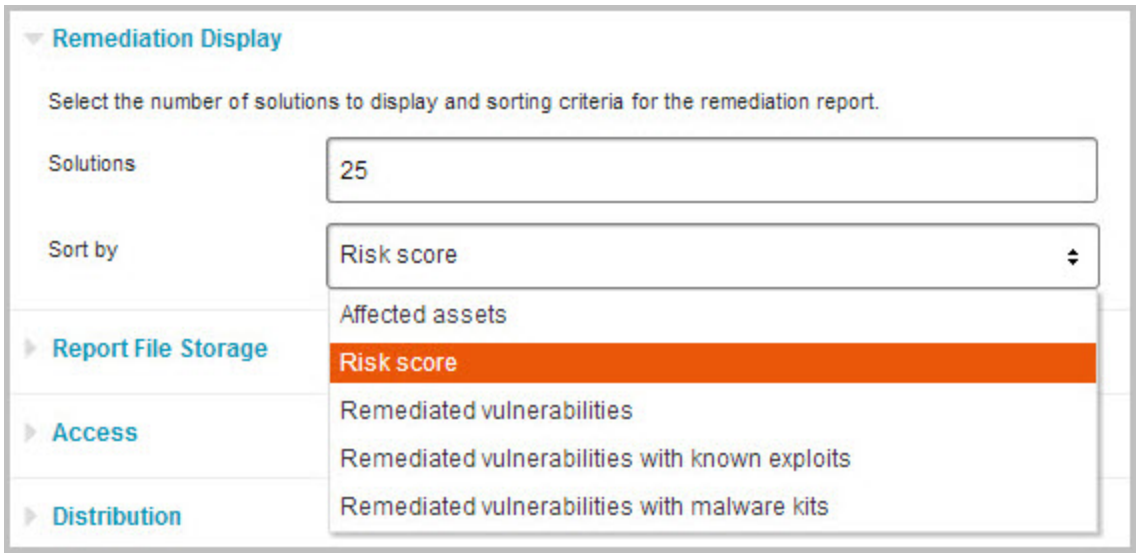
The amount of time required to generate a report depends on the number of included live IP addresses the number of included vulnerabilities–if vulnerabilities are being included–and the level of details in the report template. Generating a PDF report for 100-plus hosts with 2500-plus vulnerabilities takes fewer than 10 seconds.

The application can generate reports simultaneously, with each report request spawning a new thread. Technically, there is no limit on the number supported concurrent reports. This means that you can schedule reports to run simultaneously as needed. Note that generating a large number of concurrent reports–20 or more–can take significantly more time than usual.

Best practices for using remediation plan templates

The remediation plan templates provide information for assessing the highest impact remediation solutions. You can use the Remediation Display settings to specify the number of solutions you want to see in a report. The default is 25 solutions, but you can set the number from 1 to 1000 as you require. Keep in mind that if the number is too high you may have a report with an unwieldy level of data and too low you may miss some important solutions for your assets.

You can also specify the criteria for sorting data in your report. Solutions can be sorted by *Affected asset*, *Risk score*, *Remediated vulnerabilities*, *Remediated vulnerabilities with known exploits*, and *Remediated vulnerabilities with malware kits*.



Remediation display settings

Best practices for using the Vulnerability Trends report template

The Vulnerability Trends template provides information about how vulnerabilities in your environment have changed have changed over time. You can configure the time range for the report to see if you are improving your security posture and where you can make improvements. To ensure readability of the report and clarity of the charts there is a limit of 15 data points that can be included in the report. The time range you set controls the number of data points that appear in the report. For example, you can set your date range for a weekly interval for a two-month period, and you will have eight data points in your report.

Note: Ensure you schedule adequate time to run this report template because of the large amount of data that it aggregates. Each data point is the equivalent of a complete report. It may take a long time to complete.

To configure the time range of the report, use the following procedure:

1. Click **Configure advanced settings...**
2. Select **Vulnerability Trend Date Range**.
3. Select from pre-set ranges of **Past 1 year**, **Past 6 months**, **Past 3 months**, **Past 1 month**, or **Custom range**.

   To set a custom range, enter a start date, end date, and specify the interval, either days, months, or years.



Vulnerability trend data range

4. Configure other settings that you require for the report.
5. Click **Save & run the report** or **Save the report**, depending on what you want to do.

Saving or running the newly configured report

After you complete a basic report configuration, you will have the option to configure additional properties, such as those for distributing the report. You can access those properties by clicking **Configure advanced settings...**

If you have configured the report to run in the future, either by selecting **Run a recurring report after every scan** or **Run a recurring report in a schedule** in the *Frequency* section (see *Configuring report frequency* on page 372), you can save the report configuration by clicking **Save the report** or run it once immediately by clicking **Save & run the report**. Even if you configure the report to run automatically with one of the frequency settings, you can run the report manually any time you want if the need arises. See *Viewing, editing, and running reports* on page 353.

If you configured the report to run immediately on a one-time basis, you will also see buttons allowing you to either save and run the report, or just to save it. See *Viewing, editing, and running reports* on page 353.



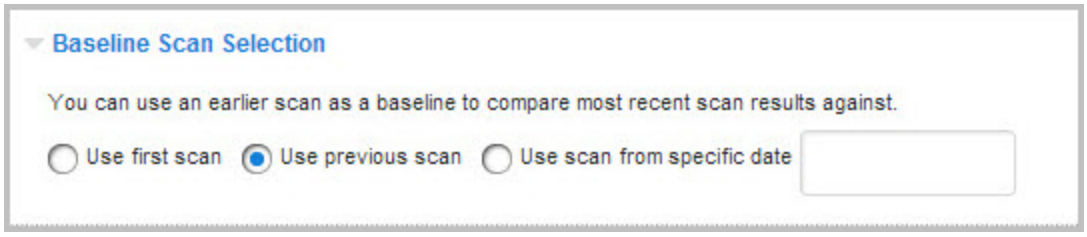
Saving or saving and running a one-time report

Selecting a scan as a baseline

Designating an earlier scan as a baseline for comparison against future scans allows you to track changes in your network. Possible changes between scans include newly discovered assets, services and vulnerabilities; assets and services that are no longer available; and vulnerabilities that were mitigated or remediated.

You must select the *Baseline Comparison* report template in order to be able to define a baseline. See *Starting a new report configuration* on page 356.

1. Go to the *Create a report* panel.
2. Click **Configure advanced settings...**
3. Click **Baseline Scan selection**.



Baseline scan selection

4. Click **Use first scan**, **Use previous scan**, or **Use scan from a specific date** to specify which scan to use as the baseline scan.
5. Click the calendar icon to select a date if you chose **Use scan from a specific date**.
6. Click **Save & run the report** or **Save the report**, depending on what you want to do.

Working with risk trends in reports

Risks change over time as vulnerabilities are discovered and old vulnerabilities are remediated on assets or excluded from reports. As system configurations are changed, assets or sites that have been added or removed also will impact your risk over time. Vulnerabilities can lead to asset compromise that might impact your organization's finances, privacy, compliance status with government agencies, and reputation. Tracking risk trends helps you assess threats to your organization's standings in these areas and determine if your vulnerability management efforts are satisfactorily maintaining risk at acceptable levels or reducing risk over time.

A risk trend can be defined as a long-term view of an asset's potential impact of compromise that may change over a time period. Depending on your strategy you can specify your trend data based on average risk or total risk. Your average risk is based on a calculation of your risk scores on assets over a report date range. For example, average risk gives you an overview of how vulnerable your assets might be to exploits whether it's high or low or unchanged. Your total risk is an aggregated score of vulnerabilities on assets over a specified period. See *Prioritize according to risk score* on page 568 for more information about risk strategies.

Over time vulnerabilities that are tracked in your organization's assets indicate risks that may have be reflected in your reports. Using risk trends in reports will help you understand how vulnerabilities that have been remediated or excluded will impact your organization. Risk trends appear in your Executive Overview or custom report as a set of colored line graphs illustrating how your risk has changed over the report period.

See *Selecting risk trends to be included in the report* on page 380 for information on including risk trends in your Executive Overview report.

Events that impact risk trends

Changes in assets have an impact on risk trends; for example, assets added to a group may increase the number of possible vulnerabilities because each asset may have exploitable vulnerabilities that have not been accounted for nor remediated. Using risk trends you can demonstrate, for example, why the risk level per asset is largely unchanged despite a spike in the overall risk trend due to the addition of an asset. The date that you added the assets will show an increase in risk until any vulnerabilities associated with those assets have been remediated. As vulnerabilities are remediated or excluded from scans your data will show a downward trend in your risk graphs.

Changing your risk strategy will have an impact on your risk trend reporting. Some risk strategies incorporate the passage of time in the determination of risk data. These time-based strategies will demonstrate risk even if there were no new scans and no assets or vulnerabilities were added in

a given time period. For more information, see *Selecting risk trends to be included in the report* on page 1.

Configuring reports to reflect risk trends

Configure your reports to display risk trends to show you the data you need. Select **All assets in report scope** for an overall high-level risk trends report to indicate trends in your organization's exploitable vulnerabilities. Vulnerabilities that are not known to have exploits still pose a certain amount of risk but it is calculated to be much smaller. The highest-risk graphs demonstrate the biggest contributors to your risk on the site, group, or asset level. These graphs disaggregate your risk data, breaking out the highest-risk factors at various asset collection methods included in the scope of your report.

Note: The risk trend settings in the *Advanced Properties* page of the *Report Configuration* panel will not appear if the selected template does not include 'Executive overview' or 'Risk Trend' sections.

You can specify your report configuration on the *Scope* and *Advanced Properties* pages of the *Report Configuration* panel. On the *Scope* page of the report configuration settings you can set the assets to include in your risk trend graphs. On the *Advanced Properties* page you can specify on which asset collections within the scope of your report you want to include in risk trend graphs. You can generate a graph representing how risk has changed over time for all assets in the scope of the report. If you generate this graph, you can choose to display how risk for all the assets has changed over time, how the scope of the assets in the report has changed over time or both. These trends will be plotted on two y-axes. If you want to see how the report scope has changed over the report period, you can do this by trending either the number of assets over the report period or the average risk score for all the assets in the report scope. When choosing to display a trend for all assets in the report scope, you must choose one or both of the two trends.

You may also choose to include risk trend graphs for the five highest-risk sites in the scope of your report, or the five highest-risk asset groups, or the five highest risk assets. You can only display trends for sites or asset groups if your report scope includes sites or asset groups, respectively. Each of these graphs will plot a trend line for each asset, group, or site that comprises the five-highest risk entities in each graph. For sites and groups trend graphs, you can choose to represent the risk trend lines either in terms of the total risk score for all the assets in each collection or in terms of the average risk score of the assets in each collection.

You can select **All assets in report scope** and you can further specify **Total risk score** and indicate **Scope trend** if you want to include either the **Average risk score** or **Number of assets** in your graph. You can also choose to include the five highest risk sites, five highest risk asset groups, and five highest risk assets depending on the level of detail you want and require in

your risk trend report. Setting the date range for your report establishes the report period for risk trends in your reports.

Tip: Including the five highest risk sites, assets, or asset groups in your report can help you prioritize candidates for your remediation efforts.

Asset group membership can change over time. If you want to base risk data on asset group membership for a particular period you can select to include asset group membership history by selecting **Historical asset group membership** on the *Advanced Properties* page of the *Report Configuration* panel. You can also select **Asset group membership** at the time of report generation to base each risk data point on the assets that are members of the selected groups at the time the report is run. This allows you to track risk trends for date ranges that precede the creation of the asset groups.

Selecting risk trends to be included in the report

You must have assets selected in your report scope to include risk trend reports in your report. See *Selecting assets to report on* on page 363 for more information.

To configure reports to include risk trends:

1. Select the Executive Overview template on the *General* page of the *Report Configuration* panel.

   (Optional) You can also create a custom report template to include a risk trend section.

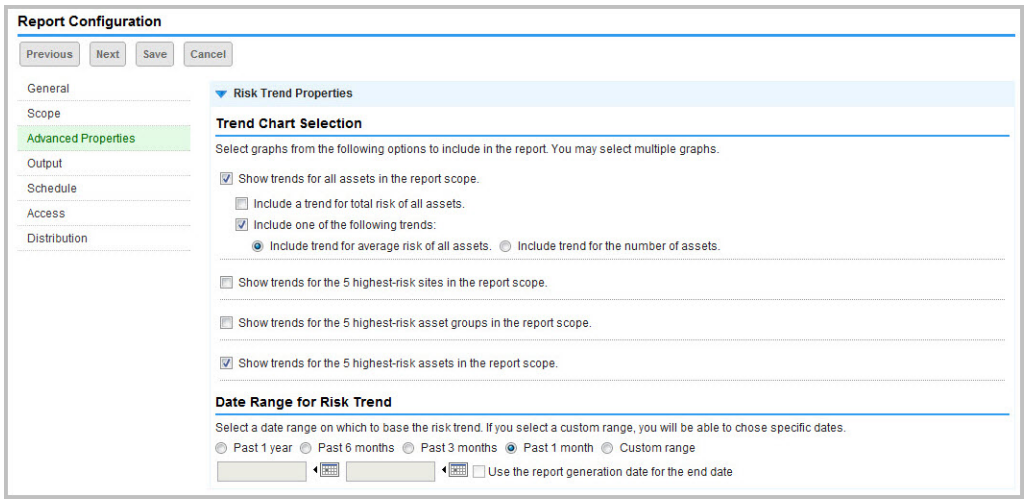
2. Go to the *Advanced Properties* page of the *Report Configuration* panel.

3. Select one or more of the trend graphs you want to include in your report: **All assets in report scope**, **5 highest-risk sites**, **5 highest-risk asset groups**, and **5 highest-risk assets**.

   To include historical asset group membership in your reports make sure that you have selected at least one asset group on the *Scope* page of the *Report Configuration* panel and that you have selected the 5 highest-risk asset group graph.

4. Set the date range for your risk trends. You can select **Past 1 year**, **Past 6 months**, **Past 3 months**, **Past 1 month**, or **Custom range**.

   (Optional) You can select **Use the report generation date for the end date** when you set a custom date range. This allows a report to have a static custom start date while dynamically lengthening the trend period to the most recent risk data every time the report is run.



Configuring risk trend reporting

Your risk trend graphs will be included in the Executive Overview report on the schedule you specified. See *Selecting risk trends to be included in the report* on page 380 for more information about understanding risk trends in reports.

Use cases for tracking risk trends

Risk trend reports are available as part of the Executive Overview reports. Risk trend reports are not constrained by the scope of your organization. They can be customized to show the data that is most important to you. You can view your overall risk for a high level view of risk trends across your organization or you can select a subset of assets, sites, and groups and view the overall risk trend across that subset and the highest risk elements within that subset.

Overall risk trend graphs, available by selecting **All assets in report scope**, provide an aggregate view of all the assets in the scope of the report. The highest-risk graphs provide detailed data about specific assets, sites, or asset groups that are the five highest risks in your environment. The overall risk trend report will demonstrate at a high level where risks are present in your environment. Using the highest-risk graphs in conjunction with the overall risk trend report will provide depth and clarity to where the vulnerabilities lie, how long the vulnerabilities have been an issue, and where changes have taken place and how those changes impact the trend.

For example, Company A has six assets, one asset group, and 100 sites. The overall risk trend report shows the trend covering a date range of six months from March to September. The overall risk graph has a spike in March and then levels off for the rest of the period. The overall report identifies the assets, the total risk, the average risk, the highest risk site, the highest risk asset group, and the highest risk asset.

To explain the spike in the graph the 5 highest-risk assets graph is included. You can see that in March the number of assets increased from five to six. While the number of vulnerabilities has

seemingly increased the additional asset is the reason for the spike. After the asset was added you can see that the report levels off to an expected pattern of risk. You can also display the Average risk score to see that the average risk per asset in the report scope has stayed effectively the same, while the aggregate risk increased. The context in which you view changes to the scope of assets over the trend report period will affect the way the data displays in the graphs.

Creating reports based on SQL queries

You can run SQL queries directly against the reporting data model and then output the results in a comma-separated value (CSV) format. This gives you the flexibility to access and share asset and vulnerability data that is specific to the needs of your security team. Leveraging the capabilities of CSV format, you can create pivot tables, charts, and graphs to manipulate the query output for effective presentation.

Prerequisites

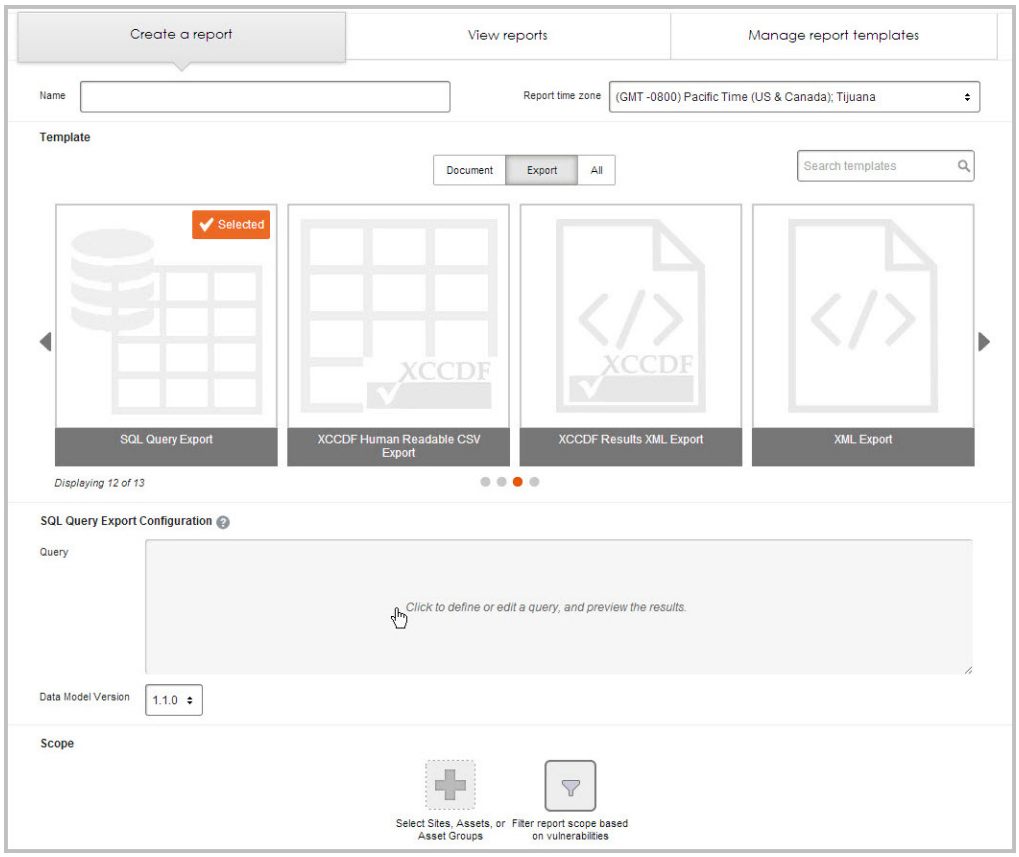
To use the SQL Query Export feature, you will need a working knowledge of SQL, including writing queries and understanding data types.

You will also benefit from an *Understanding the reporting data model: Overview and query design* on page 387, which maps database elements to business processes in your environments.

Defining a query and running a report

1. Click the **Reports** tab in the Security Console Web interface.
2. On the *Create a report* page, select the **Export** option and then select the *SQL Query Export* template from the carousel.

   The Security Console displays a box for defining a query and a drop-down list for selecting a data model version. Currently, versions 1.2.0 and 1.1.0 are available. It is the current version and covers all functionality available in preceding versions.
3. *Optional:* If you want to focus the query on specific assets, click the control to **Select Sites, Assets, or Asset Groups**, and make your selections. If you do not select specific assets, the query results will be based on all assets in your scan history.
4. *Optional:* If you want to limit the query results with vulnerability filters, click the control to **Filter report scope based on vulnerabilities**, and make your selections.



Selecting the SQL Query Export template

5. Click the text box for defining the query.

   The Security Console displays a page for defining a query, with a text box that you can edit.

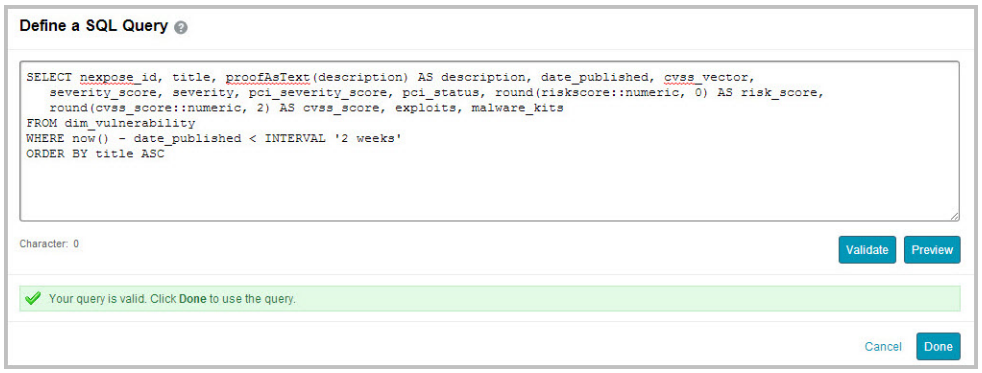
6. In this text box, enter the query.

   Tip: Click the **Help** icon to view a list of sample queries. You can select any listed query to use it for the report.



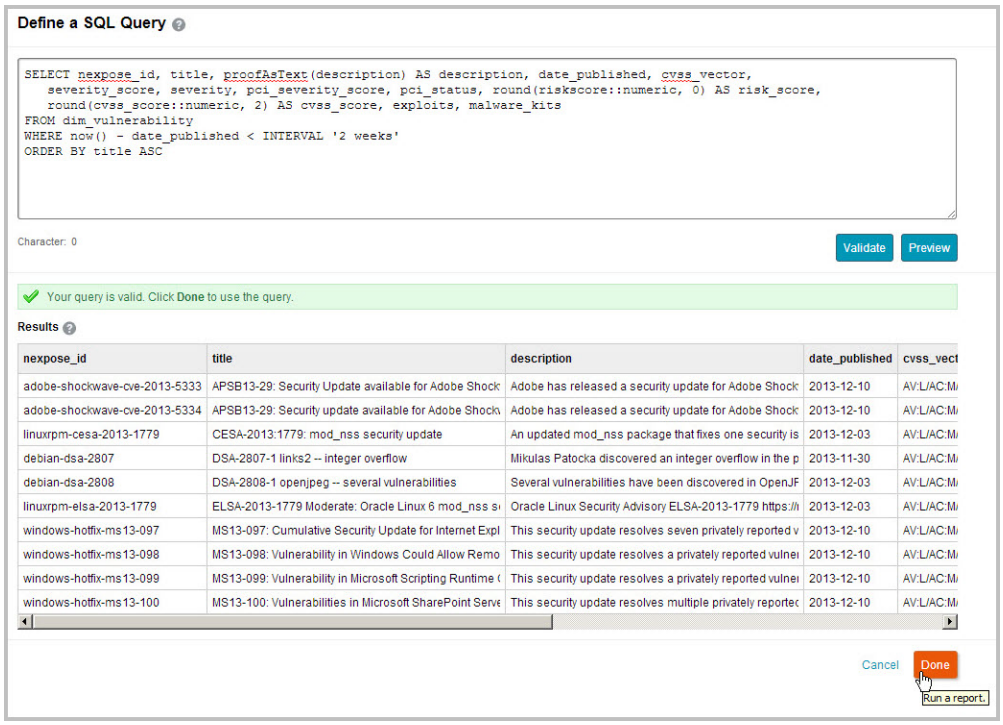
Viewing a list of sample queries that you can use

7. Click the **Validate** button to view and correct any errors with your query. The validation process completes quickly.



Viewing the message for a validated query

8. Click the **Preview** button to verify that the query output reflects what you want to include in the report. The time required to run a preview depends on the amount of data and the complexity of the query.

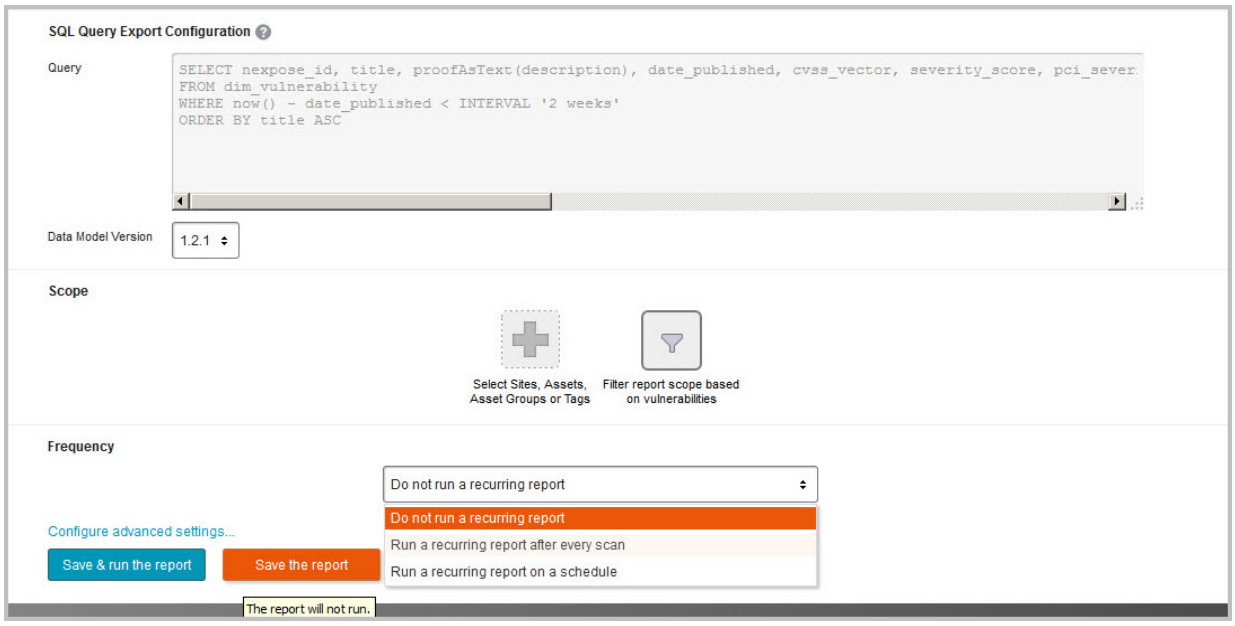


Viewing a preview of the query output

9. If necessary, edit the query based on the validation or preview results. Otherwise, click the **Done** button to save the query and run a report.

Note: If you click **Cancel**, you will not save the query.

The Security Console displays the *Create a report* page with the query displayed for reference.



Running the SQL query report

10. Click **Save & run the report** or **Save the report**, depending on what you want to do.
11. For example, if you have a saved report and want to run it one time with an additional site in it, you could add the site, save and run, return it to the original configuration, and then just save.
12. In either case, the saved SQL query export report appears on the *View reports* page.

Understanding the reporting data model: Overview and query design

On this page:

- *Overview on page 387*
- *Query design on page 388*

See related sections:

- *Creating reports based on SQL queries* on page 383
- *Understanding the reporting data model: Facts* on page 394
- *Understanding the reporting data model: Dimensions* on page 462
- *Understanding the reporting data model: Functions* on page 521

Overview

The Reporting Data Model is a dimensional model that allows customized reporting. Dimensional modeling is a data warehousing technique that exposes a model of information around business processes while providing flexibility to generate reports. The implementation of the Reporting Data Model is accomplished using the PostgreSQL relational database management system, version 9.0.13. As a result, the syntax, functions, and other features of PostgreSQL can be utilized when designing reports against the Reporting Data Model.

The Reporting Data Model is available as an embedded relational schema that can be queried against using a custom report template. When a report is configured to use a custom report template, the template is executed against an instance of the Reporting Data Model that is scoped and filtered using the settings defined with the report configuration. The following settings will dictate what information is made available during the execution of a custom report template.

Report Owner

The owner of the report dictates what data is exposed with the Reporting Data Model. The report owner's access control and role specifies what scope may be selected and accessed within the report.

Scope Filters

Scope filters define what assets, asset groups, sites, or scans will be exposed within the reporting data model. These entities, along with matching configuration options like “Use only most recent scan data”, dictate what assets will be available to the report at generation time. The scope filters are also exposed within dimensions to allow the designer to output information embedded within the report that identify what the scope was during generation time, if desired.

Vulnerability Filters

Vulnerability filters define what vulnerabilities (and results) will be exposed within the data model. There are three types of filters that are interpreted prior to report generation time:

1. Severity: filters vulnerabilities into the report based on a minimum severity level.
2. Categories: filters vulnerabilities into or out of the report based on metadata associated to the vulnerability.
3. Status: filters vulnerabilities into the report based on what the result status is.

Query design

Access to the information in the Reporting Data Model is accomplished by using queries that are embedded into the design of the custom report templates.

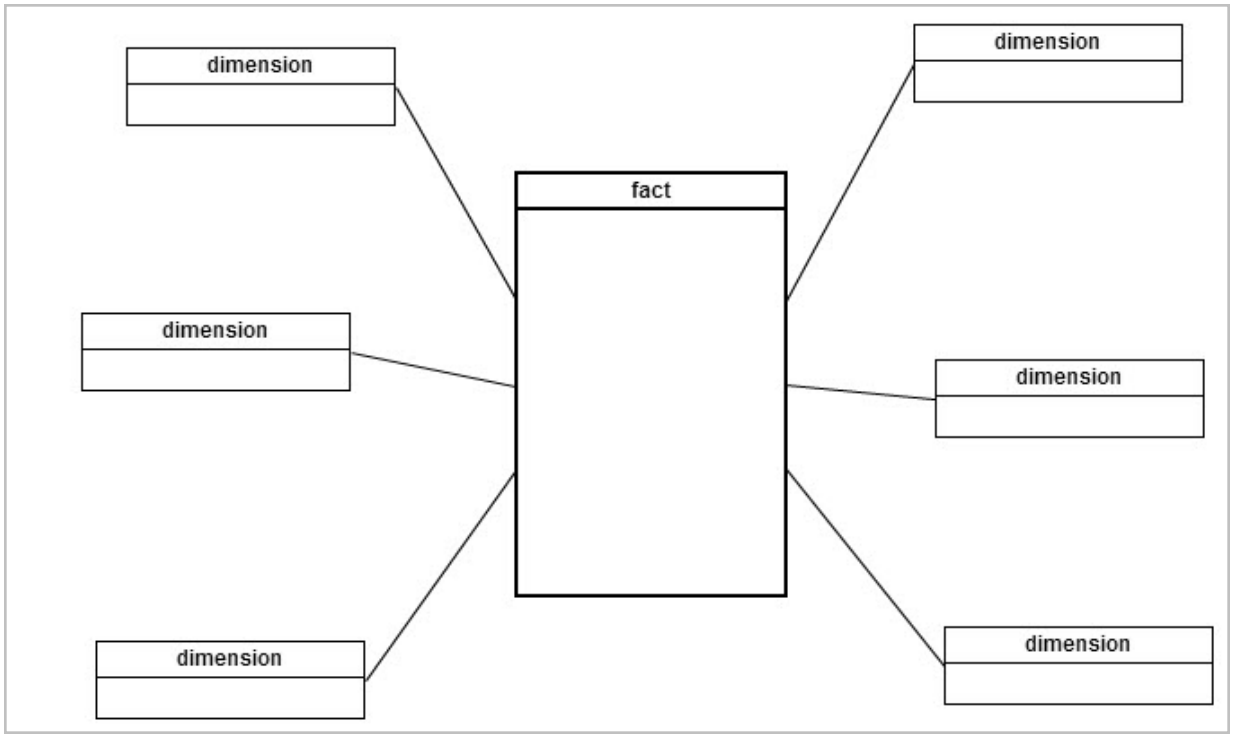
Dimensional Modeling

Dimensional Modeling presents information through a combination of facts and dimensions. A fact is a table that stores measured data, typically numerical and with additive properties. Fact tables are named with the prefix “fact_” to indicate they store factual data. Each fact table record is defined at the same level of grain, which is the level of granularity of the fact. The grain specifies the level at which the measure is recorded.

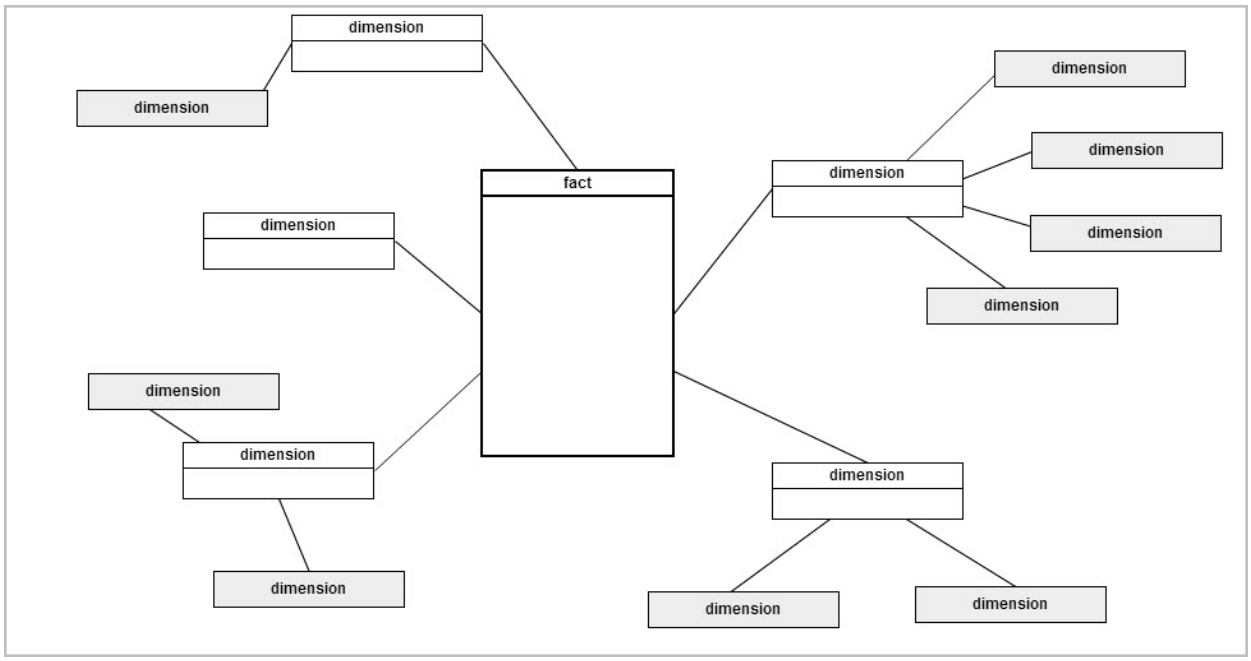
Dimension is the context that accompanies measured data and is typically textual. Dimension tables are named with the prefix “dim_” to indicate that they store context data. Dimensions allow facts to be sliced and aggregated in ways meaningful to the business. Each record in the fact table does not specify a primary key but rather defines a one-to-many set of foreign keys that link to one or more dimensions. Each dimension has a primary key that identifies the associated data that may be joined on. In some cases the primary key of the dimension is a composite of multiple columns. Every primary key and foreign key in the fact and dimension tables are surrogate identifiers.

Normalization & Relationships

Unlike traditional relational models, dimensional models favor denormalization to ease the burden on query designers and improve performance. Each fact and its associated dimensions comprise what is commonly referred to as a “star schema”. Visually a fact table is surrounded by multiple dimension tables that can be used to slice or join on the fact. In a fully denormalized dimensional model that uses the star schema style there will only be a relationship between the fact and a dimension, but the dimension is fully self-contained. When the dimensions are not fully denormalized they may have relationships to other dimensions, which can be common when there are one-to-many relationships within a dimension. When this structure exists, the fact and dimensions comprise a “snowflake schema”. Both models share a common pattern which is a single, central fact table. When designing a query to solve a business question, only one schema (and thereby one fact) *should* be used.



Denormalized “Star schema”



Normalized "Snowflake schema"

Fact Table Types

There exist three different types of fact tables: (1) transaction (2) accumulating snapshot and (3) periodic snapshot. The level of grain of a transaction fact is an event that takes place at a certain point in time. Transaction facts identify measurements that accompany a discrete action, process, or activity that is performed on a non-regular interval or schedule. Accumulating snapshot facts aggregate information that is measured over time or multiple events into a single consolidated measurement. The measurement shows the current state at a certain level of grain. The periodic snapshot fact table provides measurements that are recorded on a regular interval, typically by day or date. Each record measures the state at a discrete moment in time.

Dimension Table Types

Types Dimension tables are often classified based on the nature of the dimensional data they provided, or to indicate the frequency (if any) with which they are updated.

Following are the types of dimensions frequently encountered in a dimensional model, and those used by the Reporting Data Model:

- *slowly changing dimension (SCD)*. A slowly changing dimension is a dimension whose information changes slowly over time at non-regular intervals. Slowly changing dimensions are further classified by types, which indicate the nature by which the records in the table change. The most common types used in the Reporting Data Model are Type I and Type II.
    - Type I SCD overwrites the values of the dimensional information over time, therefore it accumulates the present state of information and no historical state.
    - Type II SCD inserts into values into the dimension over time and accumulates historical state.
- *conformed dimension*. A conformed dimension is one which is shared by multiple facts with the same labeling and values.
- *junk dimensions*. Junk dimensions are those which do not naturally fit within traditional core entity dimensions. Junk dimensions are usually comprised of flags or other groups of related values.
- *normal dimension*. A normal dimension is one not labeled in any of the other specialized categories.

Null Values & Unknown

Within a dimensional model it is an anti-pattern to have a NULL value for a foreign key within a fact table. As a result, when a foreign key to a dimension does not apply, a default value for the key will be placed in the fact record (the value of -1). This value will allow a “natural” join against the dimension(s) to retrieve either a “Not Applicable” or “Unknown” value. The value of “Not Applicable” or “N/A” implies that the value is not defined for the fact record or dimension and could never have a valid value. The value of “Unknown” implies that the value could not be determined or assessed, but could have a valid value. This practice encourages the use of natural joins (rather than outer joins) when joining between a fact and its associated dimensions.

Query Language

As the dimensional model exposed by the Reporting Data Model is built on a relational database management system, the queries to access the facts and dimensions are written using the Structured Query Language (SQL). All SQL syntax supported by the PostgreSQL DBMS can be

leveraged. The use of the star or snowflake schema design encourages the use of a repeatable SQL pattern for most queries. This pattern is as follows:

Typical Design of a Dimensional Model Query

```
SELECT column, column, ...

FROM fact_table

JOIN dimension_table ON dimension_table.primary_key = fact_table.foreign_key

JOIN ...

WHERE dimension_table.column = some condition ...

... and other SQL constructs such as GROUP BY, HAVING, and LIMIT.
```

The SELECT clause projects all the columns of data that need to be returned to populate or fill the various aspects of the report design. This clause can make use of aggregate expressions, functions, and similar SQL syntax. The FROM clause is built by first pulling data from a single fact table and then performing JOINs on the surrounding dimensions. Typically only natural joins are required to join against dimensions, but outer joins may be required on a case-by-case basis. The WHERE clause in queries against a dimensional model will filter on conditions from the data either in the fact or dimension based on whether the filter numerical or textual.

The data types of the columns returned from the query will any of those supported by the PostgreSQL DBMS. If a column projected within the query is a foreign key to a dimension and there is no appropriate value, a sentinel will be used depending on the data type. These values signify either not applicable or unknown depending on the dimension. If the data type cannot support translation to the text “Unknown” or a similar sentinel value, then NULL will be used.

Data type	Unknown value
text	‘Unknown’
macaddr	NULL
inet	NULL
character, character varying	‘-’
bigint, integer	-1

Note: Data model 2.0.0 exposes information about linking assets across sites. All previous information is still available, and in the same format. As of data model 2.0.0, there is a *sites* column in the dim_asset dimension that lists the sites to which an asset belongs.

Understanding the reporting data model: Facts

See related sections:

- *Creating reports based on SQL queries* on page 383
- *Understanding the reporting data model: Overview and query design* on page 387
- *Understanding the reporting data model: Dimensions* on page 462
- *Understanding the reporting data model: Functions* on page 521

The following facts are provided by the Reporting Data Model. Each fact table provides access to only information allowed by the configuration of the report. Any vulnerability status, severity or category filters will be applied in the facts, only allowing those results, findings, and counts for vulnerabilities in the scope to be exposed. Similarly, only assets within the scope of the report configuration are made available in the fact tables. By default, all facts are interpreted to be asset-centric, and therefore expose information for all assets in the scope of the report, regardless as to whether they were configured to be in scope with the use of an asset, scan, asset group, or site selection.

Note: Data model 2.0.0 exposes information about linking assets across sites. All previous information is still available, and in the same format. As of data model 2.0.0, there is a *sites* column in the dim_asset dimension that lists the sites to which an asset belongs.

For each fact, a dimensional star or snowflake schema is provided. For brevity and readability, only one level in a snowflake schema is detailed, and only two levels of dimensions are displayed. For more information on the attributes of these dimensions, refer to the Dimensions section below.

When dates are displayed as measures of facts, they will always be converted to match the time zone specified in the report configuration.

Only data from fully completed scans of assets are included in the facts. Results from aborted or interrupted scans will not be included.

Common measures

It will be helpful to keep in mind some characteristics of certain measures that appear in the following tables.

asset_compliance

This attribute measures the ratio of assets that are compliant with the policy rule to the total number of assets that were tested for the policy rule.

assets

This attribute measures the number of assets within a particular level of aggregation.

compliant_assets

This attribute measures the number of assets that are compliant with the policy rule (taking into account policy rule overrides.)

exploits

This attribute measures the number of distinct exploit modules that can be used exploit vulnerabilities on each asset. When the level of grain aggregates multiple assets, the total is the summation of the exploits value for each asset. If there are no vulnerabilities found on the asset or there are no vulnerabilities that can be exploited with a exploit module, the count will be zero.

malware_kits

This attribute measures the number of distinct malware kits that can be used exploit vulnerabilities on each asset. When the level of grain aggregates multiple assets, the total is the summation of the malware kits value for each asset. If there are no vulnerabilities found on the asset or there are no vulnerabilities that can be exploited with a malware kit, the count will be zero.

noncompliant_assets

This attribute measures the number of assets that are not compliant with the policy rule (taking into account policy rule overrides.)

not_applicable_assets

This attribute measures the number of assets that are not applicable for the policy rule (taking into account policy rule overrides.)

riskscore

This attribute measures the risk score of each asset, which is based on the vulnerabilities found on that asset. When the level of grain aggregates multiple assets, the total is the summation of the *riskscore* value for each asset.

rule_compliance

This attribute measures the ratio of policy rule test result that are compliant or not applicable to the total number of rule test results.

vulnerabilities

This attribute measures the number of vulnerabilities discovered on each asset. When the level of grain aggregates multiple assets, the total is the summation of the vulnerabilities on each asset.

If a vulnerability was discovered multiple times on the same asset, it will only be counted once per asset. This count may be zero if no vulnerabilities were found vulnerable on any asset in the latest scan, or if the scan was not configured to perform vulnerability checks (as in the case of discovery scans).

The vulnerabilities count is also provided for each severity level:

- *Critical:* The number of vulnerabilities that are critical.
- *Severe:* The number of vulnerabilities that are severe.
- *Moderate:* The number of vulnerabilities that are moderate.

vulnerabilities_with_exploit

This attribute measures the total number of a vulnerabilities on all assets that can be exploited with a published exploit module. When the level of grain aggregates multiple assets, the total is the summation of the vulnerabilities_with_exploit value for each asset. This value is guaranteed to be less than the total number of vulnerabilities. If no vulnerabilities are present, or none are subject to an exploit, the value will be zero.

vulnerabilities_with_malware_kit

This attribute measures the number of vulnerabilities on each asset that are exploitable with a malware kit. When the level of grain aggregates multiple assets, the total is the summation of the vulnerabilities_with_malware_kit value for each asset. This value is guaranteed to be less than the total number of vulnerabilities. If no vulnerabilities are present, or none are subject to a malware kit, the value will be zero.

vulnerability_instances

This attribute measures the number of occurrences of all vulnerabilities found on each asset. When the level of grain aggregates multiple assets, the total is the summation of the vulnerability_instances value for each asset. This value will count each instance of a vulnerability on each asset. This value may be zero if no instances were tested or found vulnerable (e.g. discover scans).

Attributes with a timestamp datatype, such as a first_discovered, honor the time zone specified in the report configuration.

fact_all

added in version 1.1.0

Level of Grain: The summary of the current state of all assets within the scope of the report.

Fact Type: accumulating snapshot

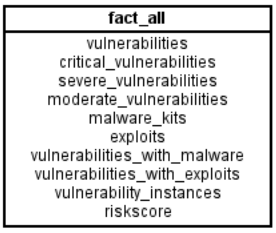
Description: Summaries of the latest vulnerability details across the entire report. This is an accumulating snapshot fact that updates after every scan of any asset within the report completes. This fact will include the data for the most recent scan of each asset that is contained within the scope of the report. As the level of aggregation is all assets in the report, this fact table is guaranteed to return one and only one row always.

Columns

Column	Data type	Nullable	Description	Associated dimension
vulnerabilities	bigint	No	The number of vulnerabilities across all assets.	
critical_ vulnerabilities	bigint	No	The number of critical vulnerabilities across all assets.	
severe_ vulnerabilities	bigint	No	The number of severe vulnerabilities across all assets.	
moderate_ vulnerabilities	bigint	No	The number of moderate vulnerabilities across all assets.	
malware_kits	integer	No	The number of malware kits across all assets.	
exploits	integer	No	The number of exploit modules across all assets.	
vulnerabilities_ with_malware_kit	integer	No	The number of vulnerabilities with a malware kit across all assets.	
vulnerabilities_ with_exploit	integer	No	The number of vulnerabilities with an exploit module across all assets.	

Column	Data type	Nullable	Description	Associated dimension
vulnerability_ instances	bigint	No	The number of vulnerability instances across all assets.	
riskscore	double precision	No	The risk score across all assets.	
pci_status	text	No	The PCI compliance status; either *Pass* or *Fail.*	

Dimensional model



Dimensional model for fact_all

fact_asset

Level of Grain: An asset and its current summary information.

Fact Type: accumulating snapshot

Description: The *fact_asset* fact table provides the most recent information for each asset within the scope of the report. For every asset in scope there will be one record in the fact table.

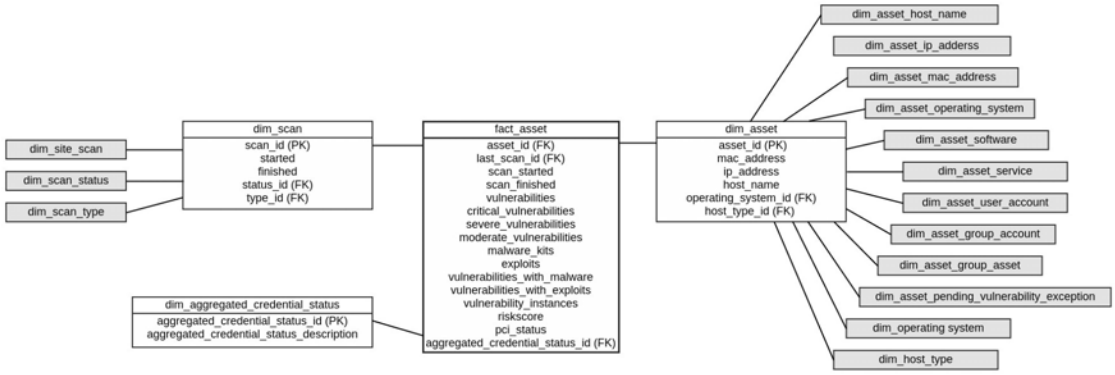
Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset.	*dim_asset*
last_scan_id	bigint	No	The identifier of the scan with the most recent information being summarized.	*dim_scan*

Column	Data type	Nullable	Description	Associated dimension
scan_started	timestamp with time zone	No	The date and time at which the latest scan for the asset started.	
scan_finished	timestamp with time zone	No	The date and time at which the latest scan for the asset completed.	
vulnerabilities	bigint	No	The number of all distinct vulnerabilities on the asset	
critical_ vulnerabilities	bigint	No	The number of critical vulnerabilities on the asset.	
severe_ vulnerabilities	bigint	No	The number of severe vulnerabilities on the asset.	
moderate_ vulnerabilities	bigint	No	The number of moderate vulnerabilities on the asset.	
malware_kits	integer	No	The number of malware kits associated with any vulnerabilities discovered on the asset.	
exploits	integer	No	The number of exploits associated with any vulnerabilities discovered on the asset.	
vulnerabilities_ with_malware	integer	No	The number of vulnerabilities with a known malware kit discovered on the asset.	
vulnerabilities_ with_exploits	*integer*	No	The number of vulnerabilities with a known exploit discovered on the asset.	
vulnerability_ instances	bigint	No	The number of vulnerability instances discovered on the asset	

Column	Data type	Nullable	Description	Associated dimension
riskscore	double precision	No	The risk score of the asset.	
pci_status	text	No	The PCI compliance status; either *Pass* or *Fail.*	
aggregated_ credential_ status_id	integer	No	The status aggregated across all available services for the given asset in the given scan.	dim_ aggregated_ credential_ status

Dimensional model



Dimensional model for fact_asset

fact_asset_date (startDate, endDate, dateInterval)

Added in version 1.1.0

Level of Grain: An asset and its summary information on a specific date.

Fact Type: periodic snapshot

Description: This fact table provides a periodic snapshot for summarized values on an asset by date. The fact table takes three dynamic arguments, which refine what data is returned. Starting from startDate and ending on endDate, a summarized value for each asset in the scope of the report will be returned for every dateInterval period of time. This will allow trending on asset information by a customizable interval of time. In terms of a chart, startDate represents the lowest value in the range, the endDate the largest value in the range, and the dateInterval is the

separation of the ticks of the range axis. If an asset did not exist prior to a summarization date, it will have no record for that date value. The summarized values of an asset represent the state of the asset in the most recent scan prior to the date being summarized; therefore, if an asset has not been scanned before the next summary interval, the values for the asset will remain the same.

For example, fact_asset_date('2013-01-01', '2014-01-01', INTERVAL '1 month') will return a row for each asset for every month in the year 2013.

Arguments

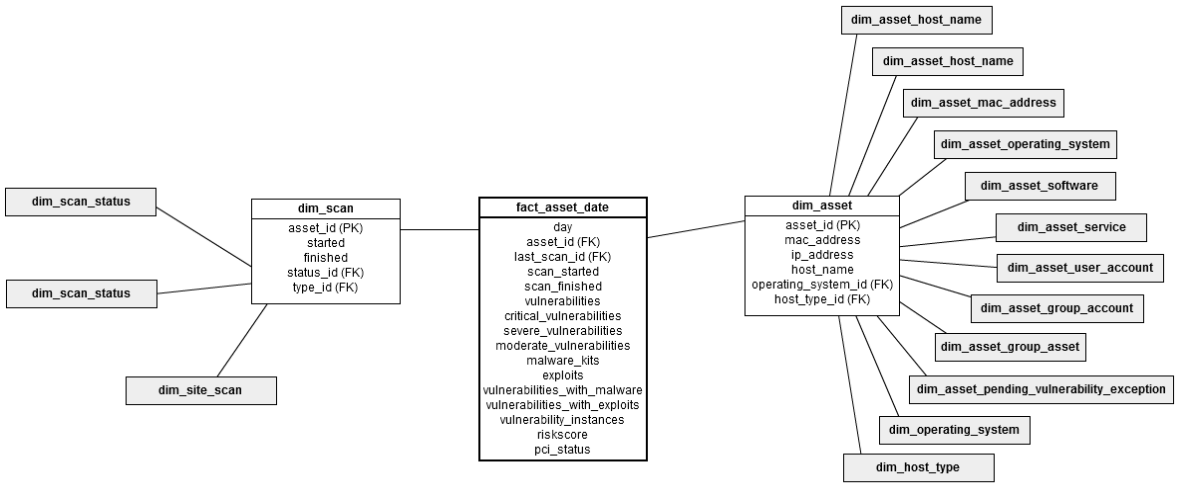
Column	Data type	Description
startDate	date	The first date to return summarizations for.
endDate	date	The last date to return summarizations for.
dateInterval	interval	The interval between the start and end date to return summarizations for.

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset.	*dim_asset*
last_scan_id	bigint	No	The identifier of the scan with the most recent information being summarized.	*dim_scan*
scan_started	timestamp with time zone	No	The date and time at which the latest scan for the asset started.	
scan_finished	timestamp with time zone	No	The date and time at which the latest scan for the asset completed.	
vulnerabilities	bigint	No	The number of all distinct vulnerabilities on the asset	
critical_ vulnerabilities	bigint	No	The number of critical vulnerabilities on the asset.	

Column	Data type	Nullable	Description	Associated dimension
severe_ vulnerabilities	bigint	No	The number of severe vulnerabilities on the asset.	
moderate_ vulnerabilities	bigint	No	The number of moderate vulnerabilities on the asset.	
malware_kits	integer	No	The number of malware kits associated with any vulnerabilities discovered on the asset.	
exploits	integer	No	The number of exploits associated with any vulnerabilities discovered on the asset.	
vulnerabilities_ with_malware	integer	No	The number of vulnerabilities with a known malware kit discovered on the asset.	
vulnerabilities_ with_exploits	*integer*	No	The number of vulnerabilities with a known exploit discovered on the asset.	
vulnerability_ instances	bigint	No	The number of vulnerability instances discovered on the asset	
riskscore	double precision	No	The risk score of the asset.	
pci_status	text	No	The PCI compliance status; either *Pass* or *Fail.*	
day	date	No	The date of the summarization of the asset.	

Dimensional model



Dimensional model for fact_asset_date(startDate, endDate, dateInterval)

fact_asset_discovery

Level of Grain: A snapshot of the discovery dates for an asset.

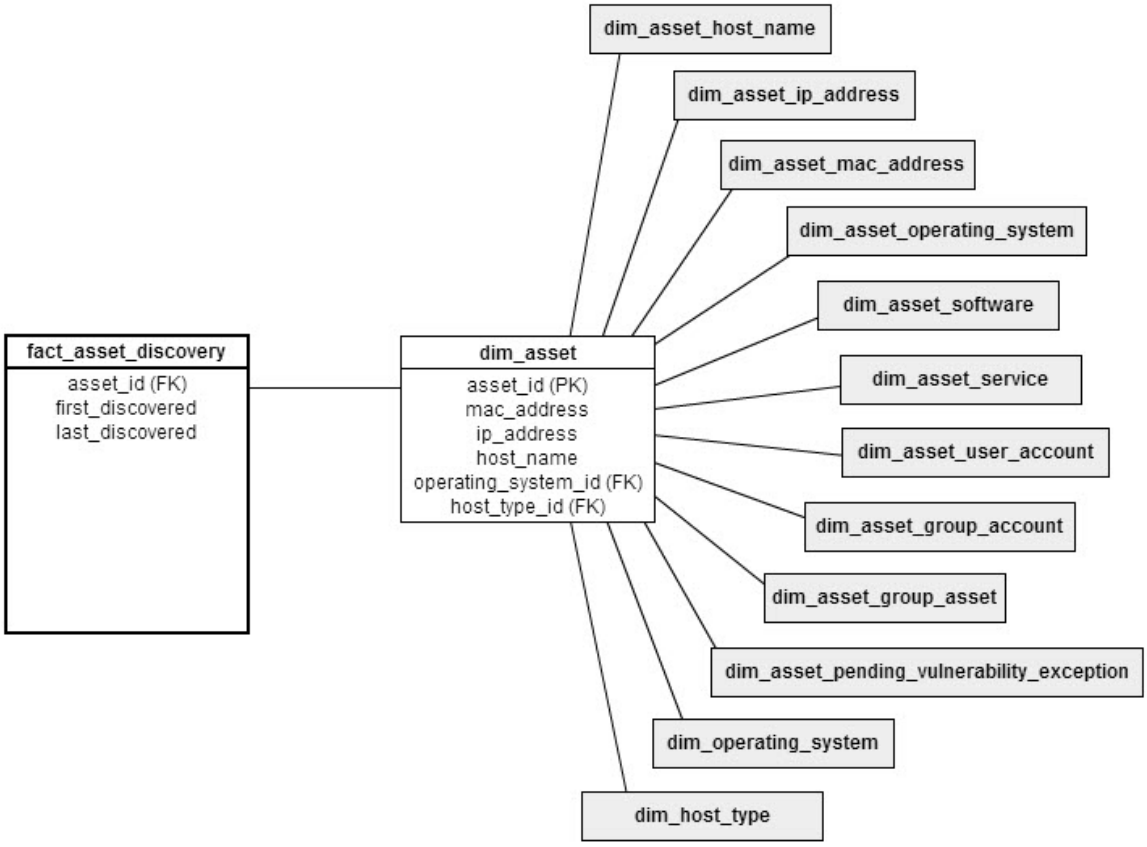
Fact Type: accumulating snapshot

Description: The *fact_asset_discovery* fact table provides an accumulating snapshot for each asset within the scope of the report and details when the asset was first and last discovered. The discovery date is interpreted as the precise time that the asset was first communicated with during a scan, during the discovery phase of the scan. If an asset has only been scanned once both the *first_discovered* and *last_discovered* dates will be the same.

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	big_int	No	The identifier of the asset.	dim_asset
first_ discovered	timestamp without time zone	No	The date and time the asset was first discovered during any scan.	
last_ discovered	timestamp without time zone	No	The date and time the asset was last discovered during any scan.	

Dimensional model



Dimensional model for fact_asset_discovery

fact_asset_group

Level of Grain: An asset group and its current summary information.

Fact Type: accumulating snapshot

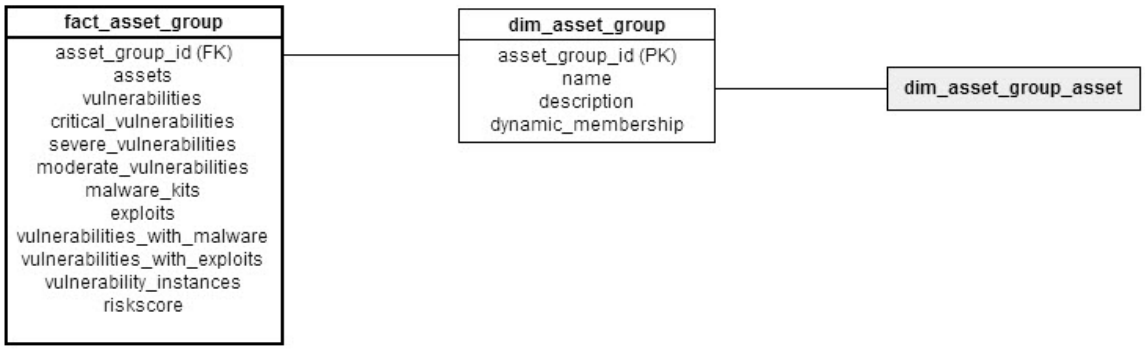
Description: The *fact_asset_group* fact table provides the most recent information for each asset group within the scope of the report. Every asset group that any asset within the scope of the report is currently a member of will be available within the scope (not just those specified in the configuration of the report). There will be one fact record for every asset group in the scope of the report. As scans are performed against assets, the information in the fact table will accumulate the most recent information for the asset group (including discovery scans).

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_group_id (as named in versions 1.2.0 and later of the data model) *group_id* (as named in version 1.1.0)	bigint	No	The identifier of the asset group.	*dim_asset_group*
assets	bigint	No	The number of distinct assets associated to the asset group. If the asset group contains no assets, the count will be zero.	
vulnerabilities	bigint	No	The number of all vulnerabilities discovered on assets in the asset group.	
critical_vulnerabilities	bigint	No	The number of all critical vulnerabilities discovered on assets in the asset group.	
severe_vulnerabilities	bigint	No	The number of all severe vulnerabilities discovered on assets in the asset group.	
moderate_vulnerabilities	bigint	No	The number of all moderate vulnerabilities discovered on assets in the asset group.	
malware_kits	integer	No	The number of malware kits associated with vulnerabilities discovered on assets in the asset group.	
exploits	integer	No	The number of exploits associated with vulnerabilities discovered on assets in the asset group.	

Column	Data type	Nullable	Description	Associated dimension
vulnerabilities_with_malware	integer	No	The number of vulnerabilities with a known malware kit discovered on assets in the asset group.	
vulnerabilities_with_exploits	integer	No	The number of vulnerabilities with a known exploit discovered on assets in the asset group.	
vulnerability_instances	bigint	No	The number of vulnerability instances discovered on assets in the asset group.	
riskscore	double precision	No	The risk score of the asset group.	
pci_status	text	No	The PCI compliance status; either *Pass* or *Fail.*	

Dimensional model



Dimensional model for fact_asset_group

fact_asset_group_date (startDate, endDate, dateInterval)

Added in version 1.1.0

Level of Grain: An asset group and its summary information on a specific date.

Fact Type: periodic snapshot

Description: This fact table provides a periodic snapshot for summarized values on an asset group by date. The fact table takes three dynamic arguments, which refine what data is returned. Starting from startDate and ending on endDate, a summarized value for each asset group in the scope of the report will be returned for every dateInterval period of time. This will allow trending on asset group information by a customizable interval of time. In terms of a chart, startDate represents the lowest value in the range, the endDate the largest value in the range, and the dateInterval is the separation of the ticks of the range axis. If an asset group did not exist prior to a summarization date, it will have no record for that date value. The summarized values of an asset group represent the state of the asset group prior to the date being summarized; therefore, if the assets in an asset group have not been scanned before the next summary interval, the values for the asset group will remain the same.

For example, fact_asset_group_date('2013-01-01', '2014-01-01', INTERVAL '1 month') will return a row for each asset group for every month in the year 2013.

Arguments

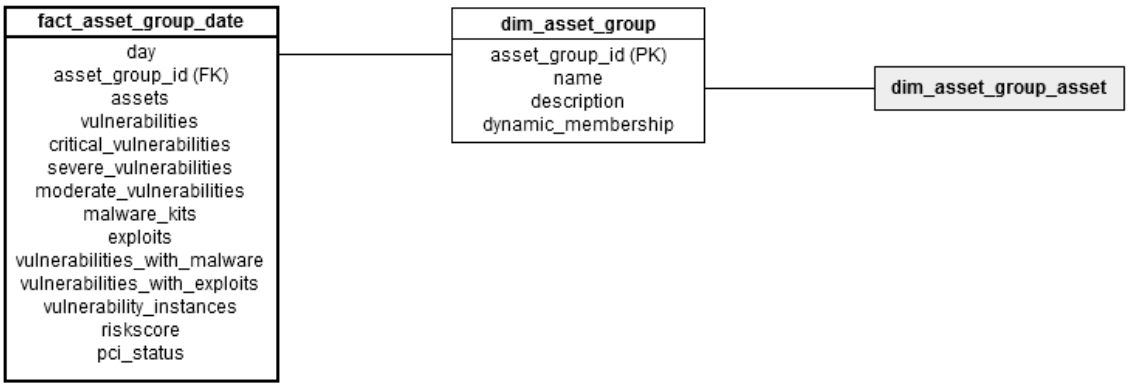
Column	Data type	Description
startDate	date	The first date to return summarizations for.
endDate	date	The last date to return summarizations for.
dateInterval	interval	The interval between the start and end date to return summarizations for.

Columns

Column	Data type	Nullable	Description	Associated dimension
group_id	bigint	No	The identifier of the asset group.	*dim_asset_group*
assets	bigint	No	The number of distinct assets associated to the asset group. If the asset group contains no assets, the count will be zero.	
vulnerabilities	bigint	No	The number of all vulnerabilities discovered on assets in the asset group.	
critical_vulnerabilities	bigint	No	The number of all critical vulnerabilities discovered on assets in the asset group.	

Column	Data type	Nullable	Description	Associated dimension
severe_vulnerabilities	bigint	No	The number of all severe vulnerabilities discovered on assets in the asset group.	
moderate_vulnerabilities	bigint	No	The number of all moderate vulnerabilities discovered on assets in the asset group.	
malware_kits	integer	No	The number of malware kits associated with vulnerabilities discovered on assets in the asset group.	
exploits	integer	No	The number of exploits associated with vulnerabilities discovered on assets in the asset group.	
vulnerabilities_with_malware	integer	No	The number of vulnerabilities with a known malware kit discovered on assets in the asset group.	
vulnerabilities_with_exploits	integer	No	The number of vulnerabilities with a known exploit discovered on assets in the asset group.	
vulnerability_instances	bigint	No	The number of vulnerability instances discovered on assets in the asset group.	
riskscore	double precision	No	The risk score of the asset group.	
pci_status	text	No	The PCI compliance status; either *Pass* or *Fail.*	
day	date	No	The date of the summarization of the asset.	

Dimensional model



Dimensional model for fact_asset_group_date

fact_asset_group_policy_date

added in version 1.3.0

Type: Periodic snapshot

Description: This fact table provides a periodic snapshot for summarized policy values on an asset group by date. The fact table takes three dynamic arguments, which refine what data is returned. Starting from startDate and ending on endDate, the summarized policy value for each asset group in the scope of the report will be returned for every dateInterval period of time. This will allow trending on asset group information by a customizable interval of time. In terms of a chart, startDate represents the lowest value in the range, the endDate the largest value in the range, and the dateInterval is the separation of the ticks of the range axis. If an asset group did not exist prior to a summarization date, it will have no record for that date value. The summarized policy values of an asset group represent the state of the asset group prior to the date being summarized; therefore, if the assets in an asset group have not been scanned before the next summary interval, the values for the asset group will remain the same.

Arguments

Column	Data type	Nullable	Description
startDate	date	No	The first date to return summarizations for.
endDate	date	No	The last date to return summarizations for.
dateInterval	interval	No	The interval between the start and end date to return summarizations for.

Columns

Column	Data type	Nullable	Description	Associated Dimension
group_id	bigint	Yes	The unique identifier of the asset group.	dim_asset
day	date	No	The date which the summarized policy scan results snapshot is taken.	
policy_id	bigint	Yes	The unique identifier of the policy within a scope.	dim_scan
scope	text	Yes	The identifier for scope of policy. Policies that are automatically available have "Built-in" scope, whereas policies created by users have scope as "Custom".	dim_policy
assets	integer	Yes	The total number of assets that are in the scope of the report and associated to the asset group.	
compliant_ assets	integer	Yes	The number of assets associated to the asset group that have not failed any while passed at least one policy rule test.	
noncompliant_ assets	integer	Yes	The number of assets associated to the asset group that have failed at least one policy rule test.	

Column	Data type	Nullable	Description	Associated Dimension
not_ applicable_ assets	integer	Yes	The number of assets associated to the asset group that have neither failed nor passed at least one policy rule test.	
rule_ compliance	numeric	Yes	The ratio of rule test results that are compliant with or not applicable to the total number of rule test results.	

fact_asset_policy

added in version 1.2.0

Level of Grain: A policy result on an asset

Fact Type: accumulating snapshot

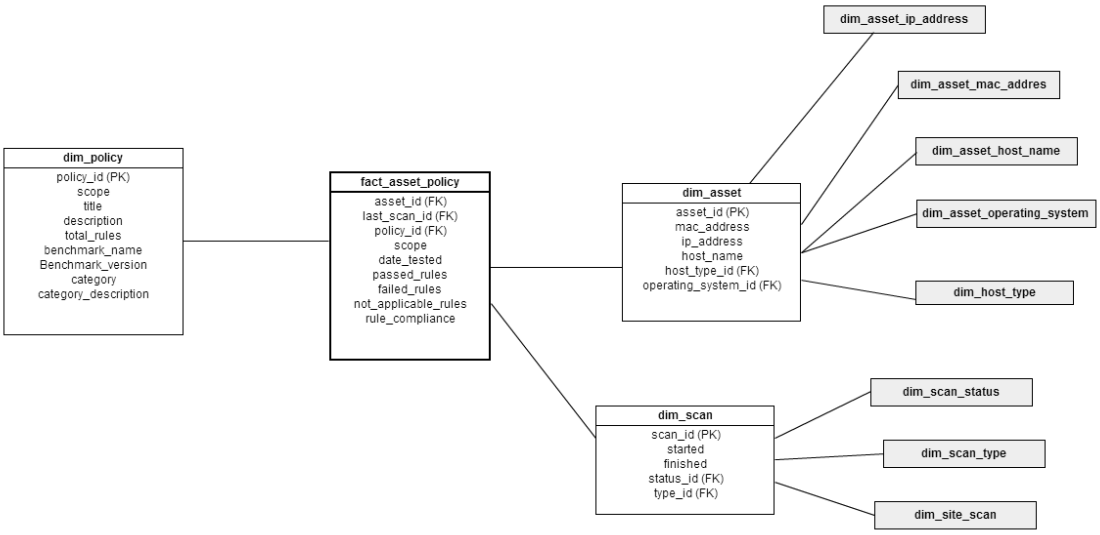
Description: This table provides an accumulating snapshot of policy test results on an asset. It displays a record for each policy that was tested on an asset in its most recent scan. Only policies scanned within the scope of report are included.

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset	dim_asset
last_scan_id	bigint	No	The identifier of the scan	dim_scan
policy_id	bigint	No	The identifier of the policy	dim_policy

Column	Data type	Nullable	Description	Associated dimension
scope	text	No	The identifier for scope of policy. Policies that are automatically available have "Built-in" scope, whereas policies created by users have scope as "Custom".	
date_tested	timestamp without timezone		The end date and time for the scan of the asset that was tested for the policy, in the time zone specified in the report configuration.	
compliant_ rules	bigint		The total number of each policy's rules in which all assets are compliant with the most recent scan.	
noncompliant_ rules	bigint		The total number of each policy's rules which at least one asset failed in the most recent scan.	
not_ applicable_ rules	bigint		The total number of each policy's rules that were not applicable to the asset in the most recent scan.	
rule_ compliance	numeric		The ratio of policy rule test result that are compliant or not applicable to the total number of rule test results.	

Dimensional model



Dimensional model for fact_asset_policy

fact_asset_policy_date

added in version 1.3.0

Type: Periodic snapshot

Description: This fact table provides a periodic snapshot for summarized policy values on an asset by date. The fact table takes three dynamic arguments, which refine what data is returned. Starting from startDate and ending on endDate, the summarized policy value for each asset in the scope of the report will be returned for every dateInterval period of time. This will allow trending on asset information by a customizable interval of time. In terms of a chart, startDate represents the lowest value in the range, the endDate the largest value in the range, and the dateInterval is the separation of the ticks of the range axis. If an asset did not exist prior to a summarization date, it will have no record for that date value. The summarized policy values of an asset represent the state of the asset prior to the date being summarized; therefore, if the assets in an asset group have not been scanned before the next summary interval, the values for the asset will remain the same.

Arguments

Column	Data type	Nullable	Description
startDate	date	No	The first date to return summarizations for.

Column	Data type	Nullable	Description
endDate	date	No	The last date to return summarizations for.
dateInterval	interval	No	The interval between the start and end date to return summarizations for.

Columns

Column	Data type	Nullable	Description	Associated Dimension
asset_id	bigint	Yes	The unique identifier of the asset.	dim_asset
day	date	No	The date which the summarized policy scan results snapshot is taken.	
scan_id	bigint	Yes	The unique identifier of the scan.	dim_scan
policy_id	bigint	Yes	The unique identifier of the policy within a scope.	dim_policy
scope	text	Yes	The identifier for scope of policy. Policies that are automatically available have "Built-in" scope, whereas policies created by users have scope as "Custom".	
date_tested	timestamp without time zone	Yes	The time the asset was tested with the policy rules.	
compliant_ rules	integer	Yes	The number of rules that all assets are compliant with in the scan.	

Column	Data type	Nullable	Description	Associated Dimension
noncompliant_ rules	integer	Yes	The number of rules that at least one asset failed in the scan.	
not_ applicable_ rules	integer	Yes	The number of rules that are not applicable to the asset.	
rule_ compliance	numeric	Yes	The ratio of rule test results that are compliant or not applicable to the total number of rule test results.	

fact_asset_policy_rule

added in version 1.3.0

Level of Grain: A policy rule result on an asset

Fact Type: accumulating snapshot

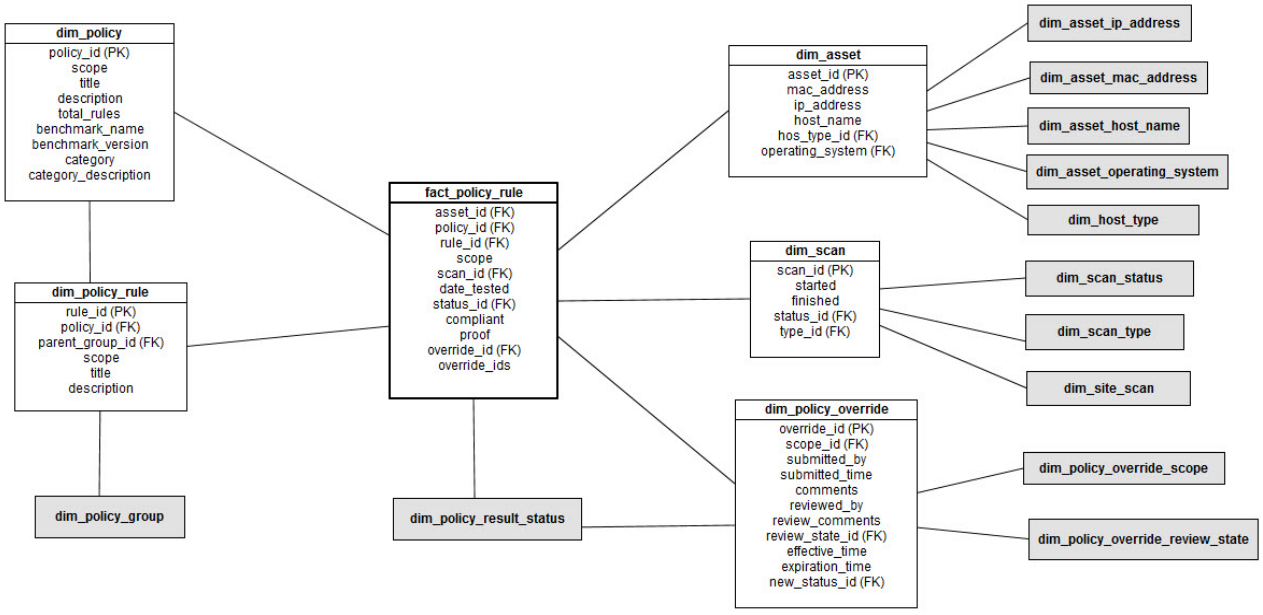
Description: This table provides the rule results of the most recent policy scan for an asset within the scope of the report. For each rule, only assets that are subject to that rule and that have a result in the most recent scan are counted.

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset	dim_asset
policy_id	bigint	No	The identifier of the policy	dim_policy

Column	Data type	Nullable	Description	Associated dimension
scope	text	No	The identifier for scope of policy. Policies that are automatically available have "Built-in" scope, whereas policies created by users have scope as "Custom".	
rule_id	bigint	No	The identifier of the policy rule.	dim_policy_rule
scan_id	bigint	No	The identifier of the scan	dim_scan
date_tested	timestamp without timezone		The end date and time for the scan of the asset that was tested for the policy, in the time zone specified in the report configuration.	
status_id	character (1)	No	The identifier of the status for the policy rule finding on the asset (taking into account policy rule overrides.)	dim_policy_rule_status
compliance	boolean	No	Whether the asset is compliant with the rule. True if and only if all of the policy checks for this rule have not failed, or the rule is overridden with the value true on the asset.	
proof	text	Yes	The proof of the policy checks on the asset.	
override_id	bigint	Yes	The unique identifier of the policy rule override that is applied to the rule on an asset. If multiple overrides apply to the rule at different levels of scope, the identifier of the override having the true effect on the rule (latest override) is returned.	dim_policy_rule_override
override_ids	bigint[]	Yes	The unique identifiers of the policy rule override that are applied to the rule on an asset. If multiple overrides apply to the rule at different levels of scope, the identifier of each override is returned in a comma-separated list.	dim_policy_rule_override

Dimensional model



Dimensional model for fact_policy_rule

fact_asset_scan

Level of Grain: A summary of a completed scan of an asset.

Fact Type: transaction

Description: The *fact_asset_scan* transaction fact provides summary information of the results of a scan for an asset. A fact record will be present for every asset and scan in which the asset was fully scanned in. Only assets configured within the scope of the report and vulnerabilities filtered within the report will take part in the accumulated totals. If no vulnerabilities checks were performed during the scan, for example as a result of a discovery scan, the vulnerability related counts will be zero.

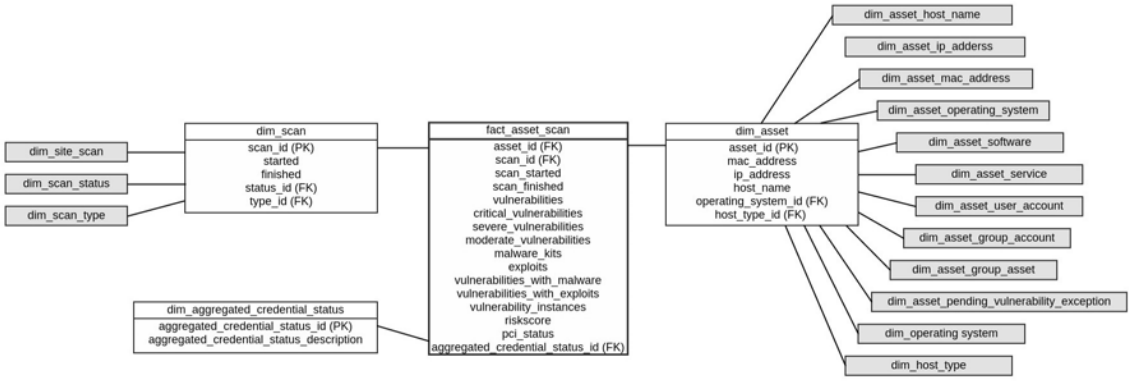
Columns

Column	Data type	Nullable	Description	Associated dimension
scan_id	bigint	No	The identifier of the scan.	dim_scan
asset_id	bigint	No	The identifier of the asset.	dim_asset

Column	Data type	Nullable	Description	Associated dimension
scan_started	timestamp without time zone	No	The time at which the scan for the asset was started.	
scan_finished	timestamp without time zone	No	The time at which the scan for the asset completed.	
vulnerabilities	bigint	No	The number of vulnerabilities found on the asset during the scan.	
critical_ vulnerabilities	bigint	No	The number of critical vulnerabilities found on the asset during the scan.	
severe_ vulnerabilities	bigint	No	The number of severe vulnerabilities found on the asset during the scan.	
moderate_ vulnerabilities	bigint	No	The number of moderate vulnerabilities found on the asset during the scan.	
malware_kits	integer	No	The number of malware kits associated with vulnerabilities discovered during the scan.	
exploits	integer	No	The number of exploits associated with vulnerabilities discovered during the scan.	
vulnerabilities_ with_malware	integer	No	The number of vulnerabilities with a known malware kit discovered during the scan.	
vulnerabilities_ with_exploits	integer	No	The number of vulnerabilities with a known exploit discovered during the scan.	
vulnerability_ instances	bigint	No	The number of vulnerability instances found discovered during the scan.	

Column	Data type	Nullable	Description	Associated dimension
riskscore	double precision	No	The risk score for the scan.	
pci_status	text	No	The PCI compliance status; either *Pass* or *Fail.*	
aggregated_credential_status_id	integer	No	The status aggregated across all available services for the given asset in the given scan.	dim_aggregated_credential_status

Dimensional model



Dimensional model for fact_asset_scan

fact_asset_scan_operating_system

Level of Grain: An operating system fingerprint on an asset in a scan.

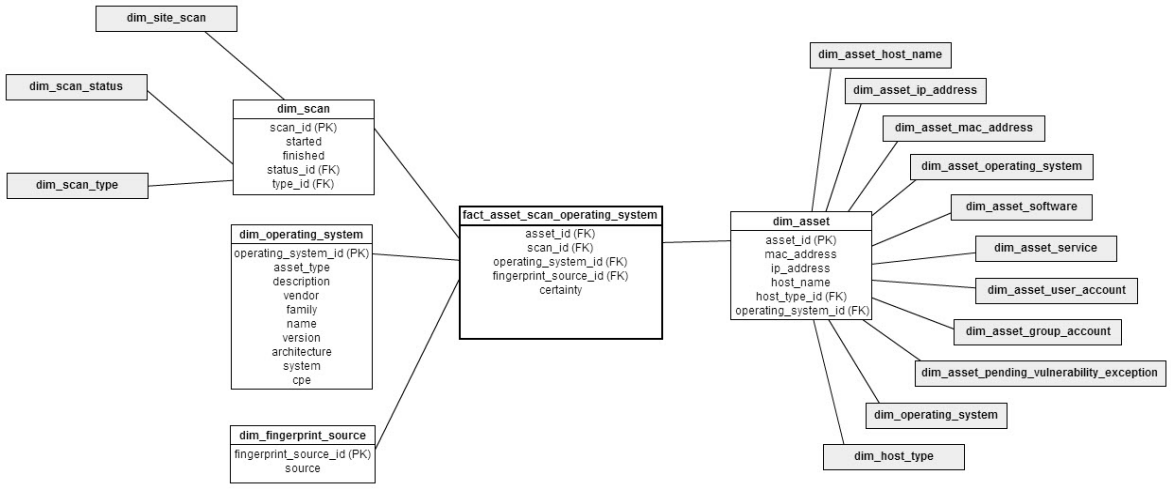
Fact Type: transaction

Description: The *fact_asset_operating_system* fact table provides the operating systems fingerprinted on an asset in a scan. The operating system fingerprints represent all the potential fingerprints collected during a scan that can be chosen as the primary or best operating system fingerprint on the asset. If an asset had no fingerprint acquired during a scan, it will have a record with values indicating an unknown fingerprint.

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset the operating system is associated to.	dim_asset
scan_id	bigint	No	The identifier of the scan the asset was fingerprinted in.	dim_scan
operating_system_id	bigint	No	The identifier of the operating system that was fingerprinted on the asset in the scan. If a fingerprint was not found, the value will be -1.	dim_operating_system
fingerprint_source_id	integer	No	The identifier of the source that was used to acquire the fingerprint. If a fingerprint was not found, the value will be -1.	dim_fingerprint_source
certainty	real	No	A value between 0 and 1 that represents the confidence level of the fingerprint. If a fingerprint was not found, the value will be 0.	

Dimensional model



Dimensional model for fact_asset_scan_operating_system

fact_asset_scan_policy

Available in version 1.2.0

Level of Grain: A policy result for an asset in a scan

Fact Type: transaction

Description: This table provides the details of policy test results on an asset during a scan. Each record provides the policy test results for an asset for a specific scan. Only policies within the scope of report are included.

Columns

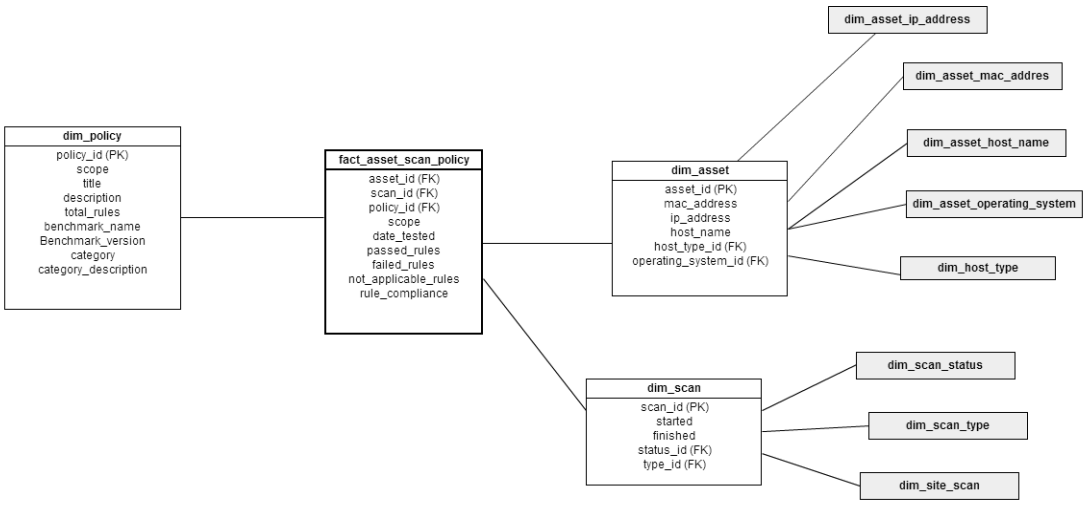
Note: As of version 1.3.0, passed_rules and failed_rules are now called compliant_rules and noncompliant_rules.

Column	Data Type	Nullable	Description	Associated Dimension
asset_id	bigint	No	The identifier of the asset	dim_asset
scan_id	bigint	No	The identifier of the scan	dim_scan
policy_id	bigint	No	The identifier of the policy	dim_policy
scope	text	No	The identifier for scope of policy. Policies that are automatically available have "Built-in" scope, whereas policies created by users have scope as "Custom".	

Column	Data Type	Nullable	Description	Associated Dimension
date_tested	timestamp without timezone		The end date and time for the scan of the asset that was tested for the policy, in the time zone specified in the report configuration.	
compliant_rules	bigint		The total number of each policy's rules for which the asset passed in the most recent scan.	
noncompliant_rules	bigint		The total number of each policy's rules for which the asset failed in the most recent scan.	
not_applicable_ rules	bigint		The total number of each policy's rules that were not applicable to the asset in the most recent scan.	

Column	Data Type	Nullable	Description	Associated Dimension
rule_compliance	numeric		The ratio of policy rule test result that are compliant or not applicable to the total number of rule test results.	

Dimensional model



Dimensional model for fact_asset_scan_policy

fact_asset_scan_software

Level of Grain: A fingerprint for an installed software on an asset in a scan.

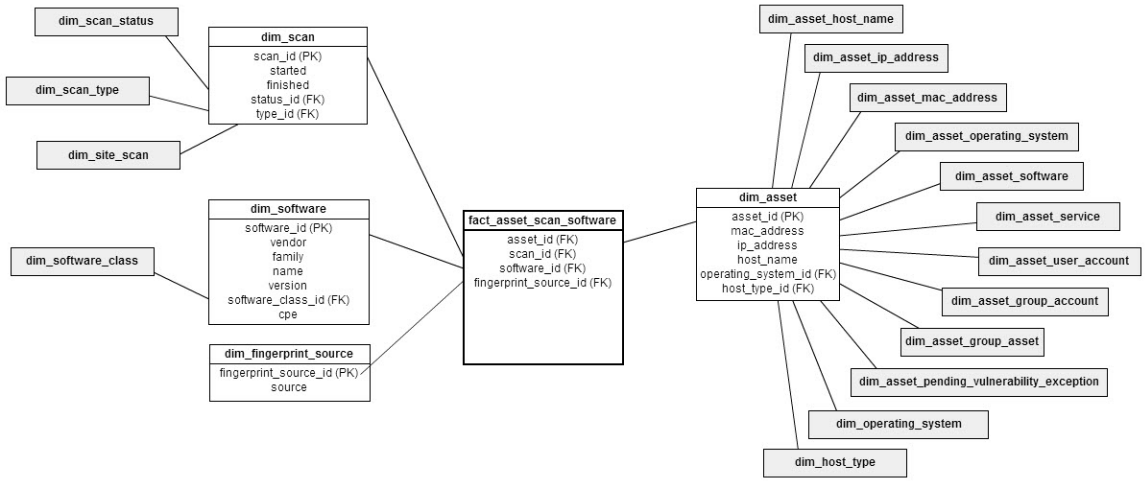
Fact Type: transaction

Description: The *fact_asset_scan_software* fact table provides the installed software packages *enumerated* or *detected* during a scan of an asset. If an asset had no software packages *enumerated* in a scan there will be no records in this fact.

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset	*dim_asset*
scan_id	bigint	No	The identifier of the scan .	*dim_scan*
software_id	bigint	No	The identifier of the software fingerprinted.	*dim_software*
fingerprint_ source_id	bigint	No	The identifier of the source used to fingerprint the software.	*dim_fingerprint_ source*

Dimensional model



Dimensional model for fact_asset_scan_software

fact_asset_scan_service

Level of Grain: A service detected on an asset in a scan.

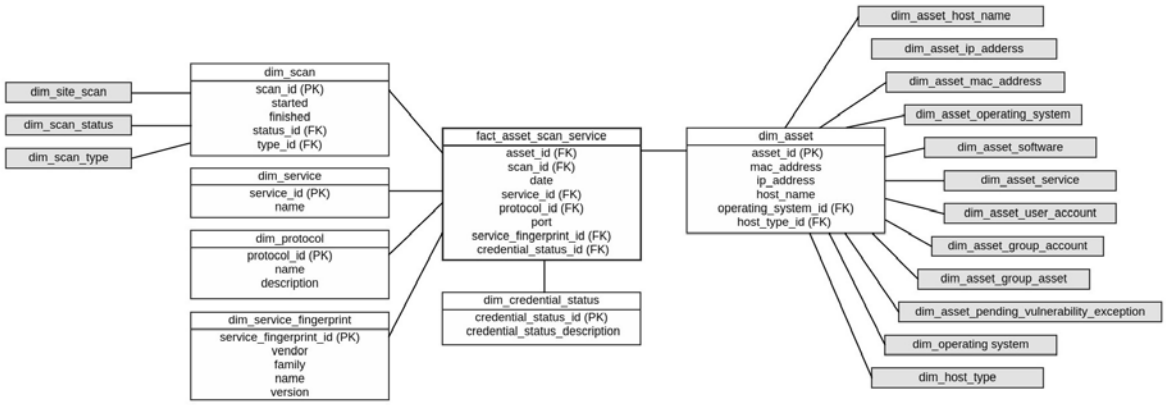
Fact Type: transaction

Description: The *fact_asset_scan_service* fact table provides the services detected during a scan of an asset. If an asset had no services enumerated in a scan there will be no records in this fact.

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset.	*dim_asset*
scan_id	bigint	No	The identifier of the scan.	*dim_scan*
date	timestamp without time zone	No	The date and time at which the service was enumerated.	
service_id	integer	No	The identifier of the service.	*dim_service*
protocol_id	smallint	No	The identifier of the protocol the service was utilizing.	*dim_protocol*
port	integer	No	The port the service was running on.	
service_fingerprint_id	bigint	No	The identifier of the fingerprint of the service describing the configuration of the service.	*dim_service_fingerprint*
credential_status_id	smallint	No	The result of the user-provided credentials per asset per scan per service. Services for which credential status is assessed are: SNMP, SSH, Telnet and CIFS.	dim_credential_status

Dimensional model



Dimensional model for fact_asset_scan_service

fact_asset_scan_vulnerability_finding

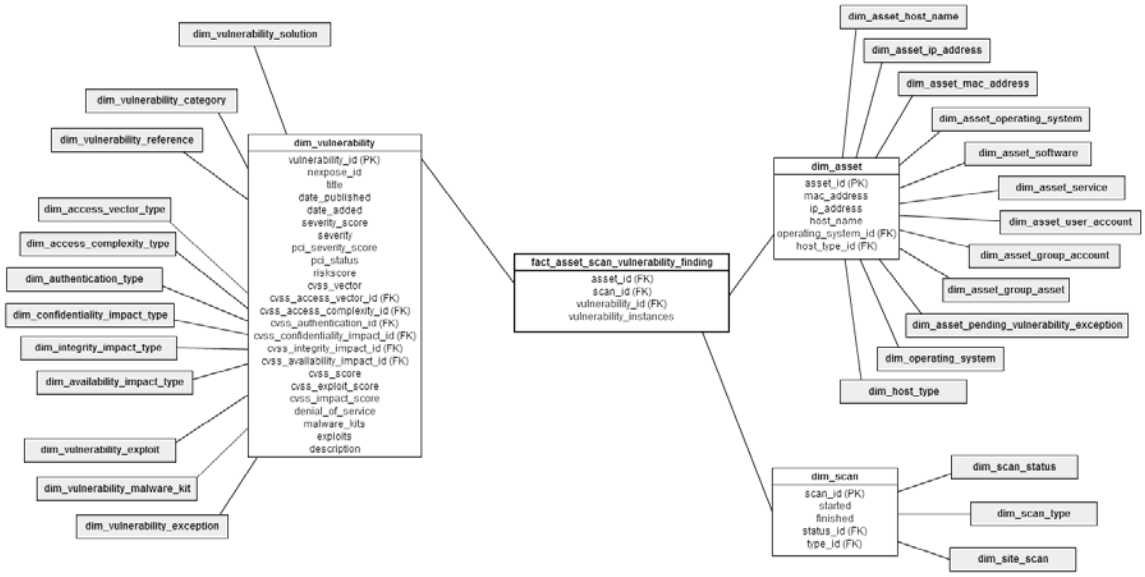
Added in version 1.1.0

Level of Grain: A vulnerability finding on an asset in a scan.

Fact Type: transaction

Description: This fact tables provides an accumulating snapshot for all vulnerability findings on an asset in every scan of the asset. This table will display a record for each unique vulnerability discovered on each asset in the every scan of the asset. If multiple occurrences of the same vulnerability are found on the asset, they will be rolled up into a single row with a *vulnerability_instances* count greater than one. Only vulnerabilities with no active exceptions applies will be displayed.

Dimensional model



Dimensional model for fact_asset_scan_vulnerability_finding

fact_asset_scan_vulnerability_instance

added in version 1.1.0

Level of Grain: A vulnerability instance on an asset in a scan.

Fact Type: transaction

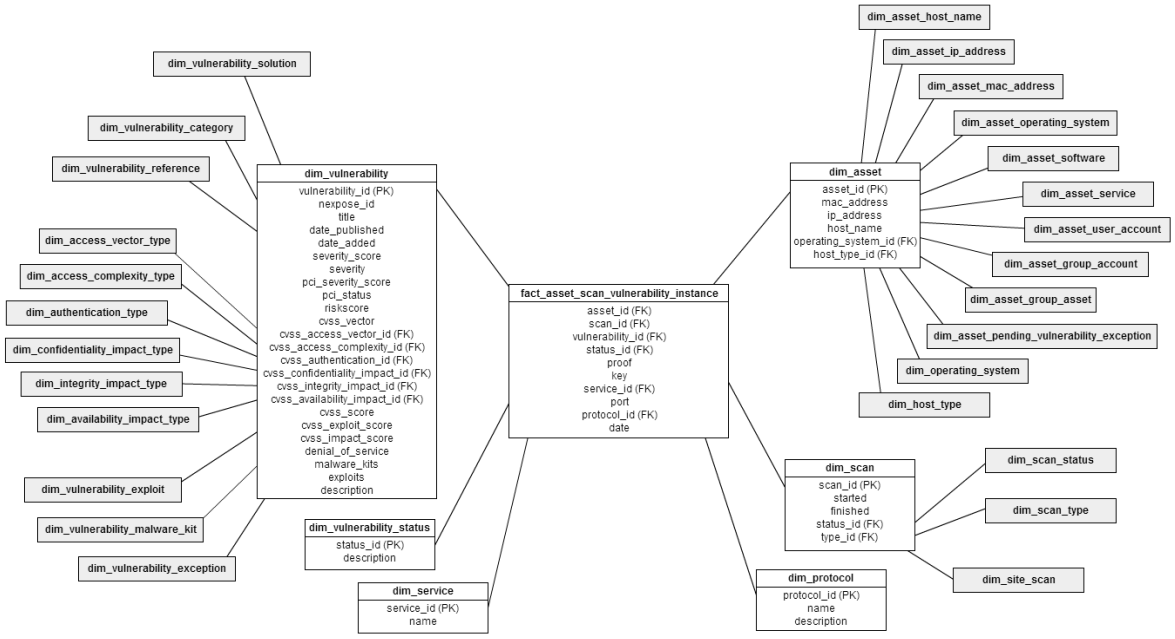
Description: The > *fact_asset_scan_vulnerability_instance* fact table provides the details of a vulnerability instance discovered during a scan of an asset. Only vulnerability instances found to be vulnerable and with no exceptions actively applied will be present within the fact table. A vulnerability instance is a unique vulnerability result found discovered on the asset. If the multiple occurrences of the same vulnerability are found on the asset, one row will be present for each instance.

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset .	*dim_asset*
scan_id	bigint	No	The identifier of the scan.	*dim_scan*
vulnerability_id	integer	No	The identifier of the vulnerability the finding is for.	*dim_vulnerability*
date	timestamp without time zone	No	The date and time at which the vulnerability finding was detected. This time is the time at which the asset completed scanning during the scan.	
status_id	character (1)	No	The identifier of the status of the vulnerability finding that indicates the level of confidence of the finding.	*dim_vulnerability_status*
proof	text	No	The proof indicating the reason that the vulnerability exists. The proof is exposed in formatting markup that can be striped using the function *proofAsText* .	
key	text	Yes	The secondary identifier of the vulnerability finding that discriminates the result from similar results of the same vulnerability on the same asset. This value is optional and will be *null* when a vulnerability does not need a secondary discriminator.	

Column	Data type	Nullable	Description	Associated dimension
service_id	integer	No	The service the vulnerability was discovered on, or -1 if the vulnerability is not associated with a service.	*dim_service*
port	integer	No	The port on which the vulnerable service was running, or -1 if the vulnerability is not associated with a service.	
protocol_id	integer	No	The protocol the vulnerable service was running, or -1 if the vulnerability is not associated with a service.	*dim_ protocol*

Dimensional model



Dimensional model for fact_asset_scan_vulnerability_instance

fact_asset_scan_vulnerability_instance_excluded

added in version 1.1.0

Level of Grain: A vulnerability instance on an asset in a scan with an active vulnerability exception applied.

Fact Type: transaction

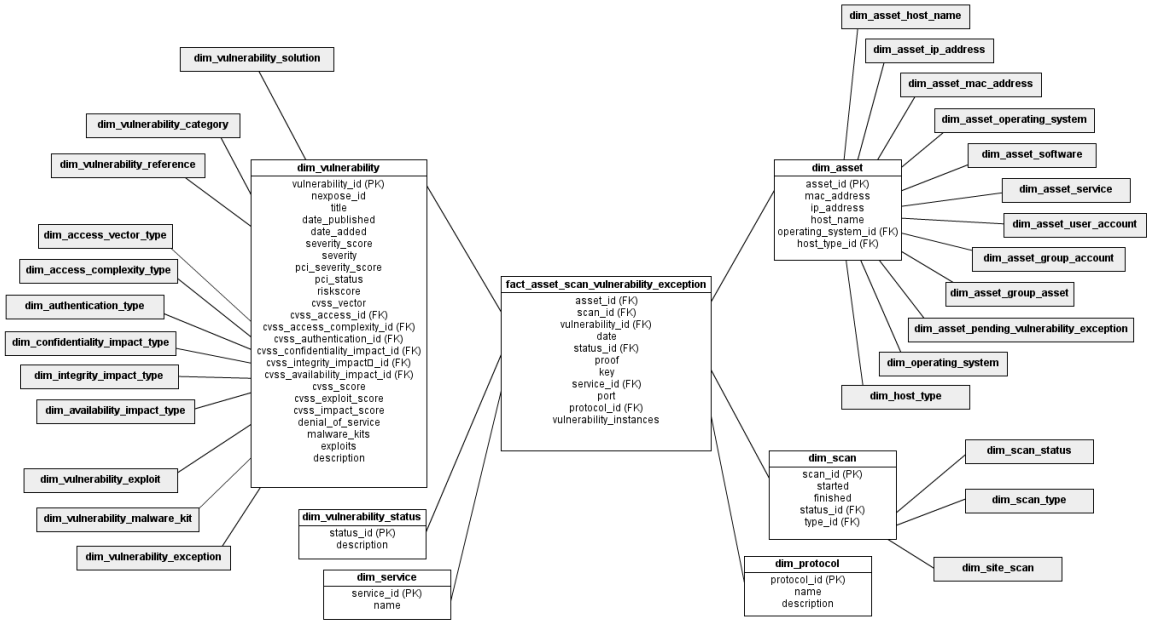
Description: The *fact_asset_scan_vulnerability_instance_excluded* fact table provides the details of a vulnerability instance discovered during a scan of an asset with an exception applied. Only vulnerability instances found to be vulnerable and with exceptions actively applied will be present within the fact table. If the multiple occurrences of the same vulnerability are found on the asset, one row will be present for each instance.

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset.	*dim_asset*
scan_id	bigint	No	The identifier of the scan.	*dim_scan*
vulnerability_id	integer	No	The identifier of the vulnerability.	*dim_vulnerability*
date	timestamp without time zone	No	The date and time at which the vulnerability finding was detected. This time is the time at which the asset completed scanning during the scan.	
status_id	character (1)	No	The identifier of the status of the vulnerability finding that indicates the level of confidence of the finding.	*dim_vulnerability_status*
proof	text	No	The proof indicating the reason that the vulnerability exists. The proof is exposed in formatting markup that can be striped using the function *proofAsText*.	
key	text	Yes	The secondary identifier of the vulnerability finding that discriminates the result from similar results of the same vulnerability on the same asset. This value is optional and will be *null* when a vulnerability does not need a secondary discriminator.	

Column	Data type	Nullable	Description	Associated dimension
service_id	integer	No	The service the vulnerability was discovered on, or -1 if the vulnerability is not associated with a service.	*dim_service*
port	integer	No	The port on which the vulnerable service was running, or -1 if the vulnerability is not associated with a service.	
protocol_id	integer	No	The protocol the vulnerable service was running, or -1 if the vulnerability is not associated with a service.	*dim_ protocol*

Dimensional model



Dimensional model for fact_asset_scan_vulnerability_instance_excluded

fact_asset_vulnerability_age

Added in version 1.2.0

Level of Grain: A vulnerability on an asset.

Fact Type: accumulating snapshot

Description: This fact table provides an accumulating snapshot for vulnerability age and occurrence information on an asset. For every vulnerability to which an asset is currently vulnerable, there will be one fact record. The record indicates when the vulnerability was first found, last found, and its current age. The age is computed as the difference between the time the vulnerability was first discovered on the asset, and the current time. If the vulnerability was temporarily remediated, but rediscovered, the age will be from the first discovery time. If a vulnerability was found on a service, remediated and discovered on another service, the age is still computed as the first time the vulnerability was found on any service on the asset.

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The unique identifier of the asset.	*dim_asset*
vulnerability_id	integer	No	The unique identifier of the vulnerability.	*dim_vulnerability*
age	interval	No	The age of the vulnerability on the asset, in the interval format.	
age_in_days	numeric	No	The age of the vulnerability on the asset, specified in days.	
first_discovered	timestamp without timezone	No	The date on which the vulnerability was first discovered on the asset.	
most_recently_discovered	timestamp without timezone	No	The date on which the vulnerability was most recently discovered on the asset.	

fact_asset_vulnerability_finding

Added in version 1.2.0

Level of Grain: A vulnerability finding on an asset.

Fact Type: accumulating snapshot

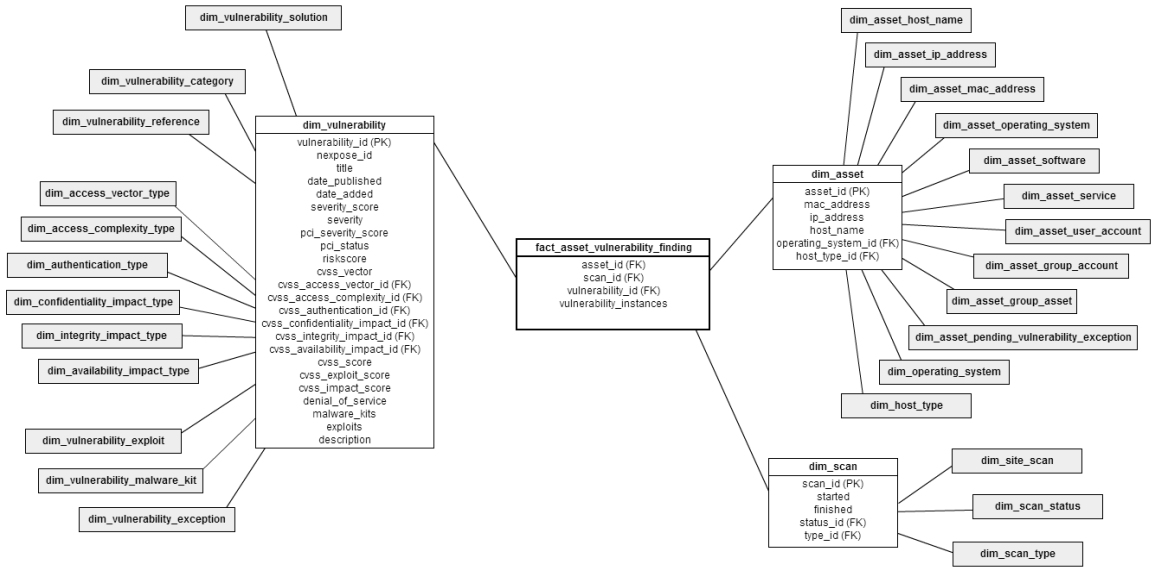
Description: This fact tables provides an accumulating snapshot for all current vulnerability findings on an asset. This table will display a record for each unique vulnerability discovered on each asset in the most recent scan of the asset. If multiple occurrences of the same vulnerability

are found on the asset, they will be rolled up into a single row with a vulnerability_instances count greater than one. Only vulnerabilities with no active exceptions applies will be displayed.

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset.	*dim_asset*
scan_id	bigint	No	The identifier of the last scan for the asset in which the vulnerability was detected.	*dim_scan*
vulnerability_id	integer	No	The identifier of the vulnerability.	*dim_vulnerability*
vulnerability_instances	bigint	No	The number of occurrences of the vulnerability detected on the asset, guaranteed to be greater than or equal to one.	
vulnerability_instances	bigint	No	The number of occurrences of the vulnerability detected on the asset, guaranteed to be greater than or equal to one.	

Dimensional model



Dimensional model for fact_asset_vulnerability_finding

fact_asset_vulnerability_instance

Level of Grain: A vulnerability instance on an asset.

Fact Type: accumulating snapshot

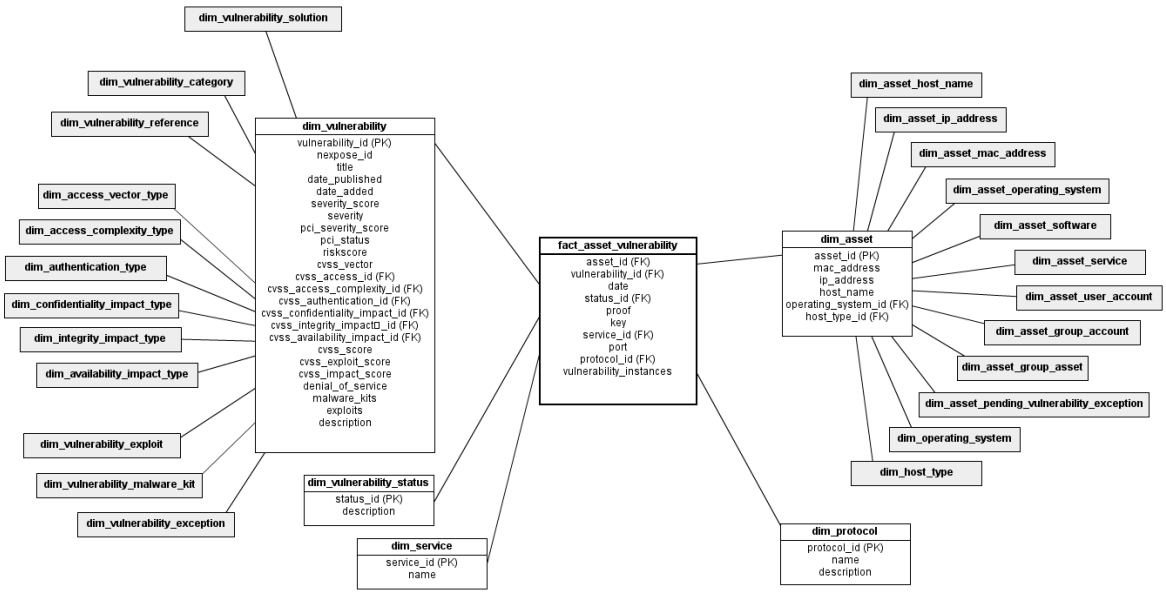
Description: This table provides an accumulating snapshot for all current vulnerability instances on an asset. Only vulnerability instance found to be vulnerable and with no exceptions actively applied will be present within the fact table. If the multiple occurrences of the same vulnerability are found on the asset, a row will be present for each instance.

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset.	*dim_asset*
vulnerability_id	integer	No	The identifier of the vulnerability.	*dim_vulnerability*
date_tested	timestamp without time zone	No	The date and time at which the vulnerability finding was detected. This time is the time at which the asset completed scanning during the scan.	
status_id	character (1)	No	The identifier of the status of the vulnerability finding that indicates the level of confidence of the finding.	*dim_vulnerability_status*
proof	text	No	The proof indicating the reason that the vulnerability exists. The proof is exposed in formatting markup that can be striped using the function *proofAsText*.	

Column	Data type	Nullable	Description	Associated dimension
key	text	Yes	The secondary identifier of the vulnerability finding that discriminates the result from similar results of the same vulnerability on the same asset. This value is optional and will be *null* when a vulnerability does not need a secondary discriminator.	
service_id	integer	No	The service the vulnerability was discovered on, or -1 if the vulnerability is not associated with a service.	*dim_service*
port	integer	No	The port on which the vulnerable service was running, or -1 if the vulnerability is not associated with a service.	
protocol_id	integer	No	The protocol the vulnerable service was running, or -1 if the vulnerability is not associated with a service.	*dim_protocol*

Dimensional model



Dimensional model for fact_asset_vulnerability

fact_asset_vulnerability_instance_excluded

Level of Grain: A vulnerability instance on an asset with an active vulnerability exception applied.

Fact Type: accumulating snapshot

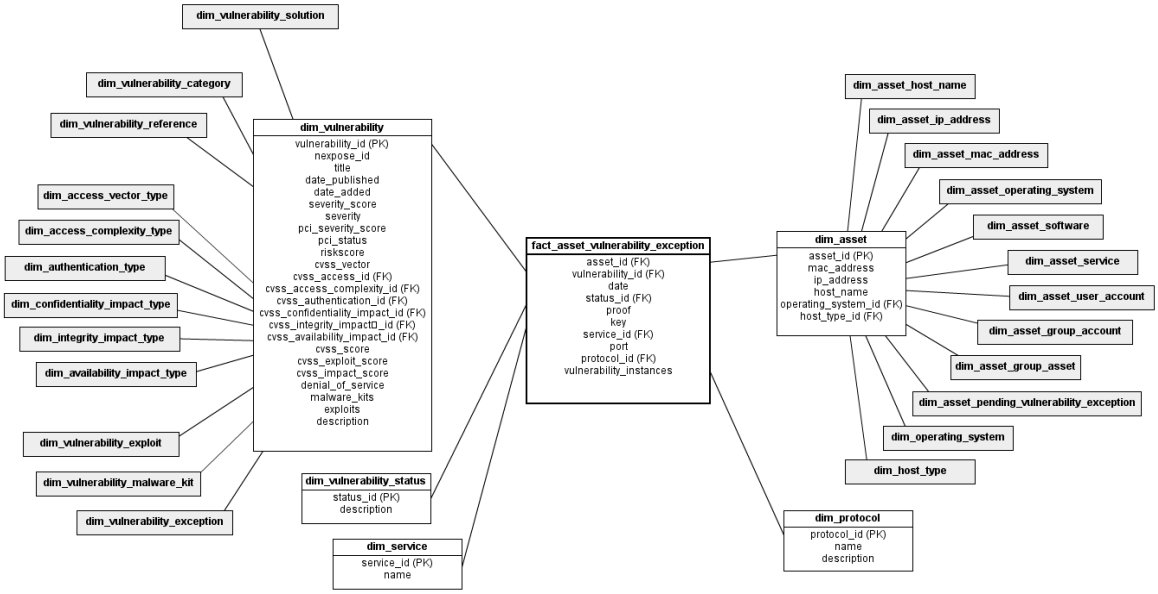
Description: The *fact_asset_vunerability_instance_excluded* fact table provides an accumulating snapshot for all current vulnerability instances on an asset. If the multiple occurrences of the same vulnerability are found on the asset, a row will be present for each instance.

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset.	*dim_asset*
vulnerability_id	integer	No	The identifier of the vulnerability.	*dim_vulnerability*
date_tested	timestamp without time zone	No	The date and time at which the vulnerability finding was detected. This time is the time at which the asset completed scanning during the scan.	
status_id	character (1)	No	The identifier of the status of the vulnerability finding that indicates the level of confidence of the finding.	*dim_vulnerability_status*
proof	text	No	The proof indicating the reason that the vulnerability exists. The proof is exposed in formatting markup that can be striped using the function *proofAsText*.	
key	text	Yes	The secondary identifier of the vulnerability finding that discriminates the result from similar results of the same vulnerability on the same asset. This value is optional and will be *null* when a vulnerability does not need a secondary discriminator.	

Column	Data type	Nullable	Description	Associated dimension
service_id	integer	No	The service the vulnerability was discovered on, or -1 if the vulnerability is not associated with a service.	*dim_service*
port	integer	No	The port on which the vulnerable service was running, or -1 if the vulnerability is not associated with a service.	
protocol_id	integer	No	The protocol the vulnerable service was running, or -1 if the vulnerability is not associated with a service.	*dim_ protocol*

Dimensional model



Dimensional model for fact_asset_vulnerability_exception

fact_pci_asset_scan_service_finding

added in version 1.3.2

Level of Grain: A service finding on an asset in a scan.

Fact Type: Transaction

Description: The *fact_pci_asset_scan_service_finding* table is the transaction fact for a service finding on an asset for a scan. This fact provides a record for each service on every asset within the scope of the report for every scan it was included in. The level of grain is a unique service finding. If no services were found on an asset in a scan, it will have no records in this fact table. For PCI purposes, each service finding is mapped to a vulnerability. Services for which a version was fingerprinted are mapped to an additional vulnerability.

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The unique identifier of the asset.	*dim_asset*
scan_id	bigint	No	The unique identifier of the scan the service finding was found in.	*dim_scan*
service_id	integer	No	The identifier of the definition of the service.	*dim_service*
vulnerability_id	integer	No	The unique identifier of the vulnerability.	*dim_vulnerability*
protocol_id	smallint	No	The identifier of the protocol the service was utilizing.	*dim_protocol*
port	integer	No	The port the service was running on.	

fact_pci_asset_service_finding

added in version 1.3.2

Level of Grain: A service finding on an asset from the latest scan of the asset.

Fact Type: Accumulating snapshot

Description: The *fact_pci_asset_service_finding* fact table provides an accumulating snapshot fact for all service findings on an asset for the latest scan of every asset. The level of grain is a unique service finding. If no services were found on an asset in a scan, it will have no records in this fact table. For PCI purposes, each service finding is mapped to a vulnerability. Services for which a version was fingerprinted are mapped to an additional vulnerability.

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The unique identifier of the asset.	*dim_asset*
scan_id	bigint	No	The unique identifier of the scan the service finding was found in.	*dim_scan*
service_id	integer	No	The identifier of the definition of the service.	*dim_service*
vulnerability_id	integer	No	The unique identifier of the vulnerability.	*dim_vulnerability*
protocol_id	smallint	No	The identifier of the protocol the service was utilizing.	*dim_protocol*
port	integer	No	The port the service was running on.	

fact_pci_asset_special_note

added in version 1.3.2

Level of Grain: A note finding on a vulnerability or service on an asset (plus port and protocol, if applicable) from the latest scan of the asset.

Fact Type: Accumulating snapshot

Description: The *fact_pci_asset_special_note* fact table provides an accumulating snapshot fact for all vulnerability or service findings with applied special notes on an asset for the latest scan of every asset. The level of grain is a unique vulnerability or service finding, determined by asset, port and protocol.

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The unique identifier of the asset.	*dim_asset*
scan_id	bigint	No	The unique identifier of the scan.	*dim_scan*
service_id	integer	No	The identifier of the definition of the service.	*dim_service*

Column	Data type	Nullable	Description	Associated dimension
protocol_id	smallint	No	The identifier of the protocol the service was utilizing.	*dim_protocol*
port	integer	No	The port the service was running on.	
pci_note_id	integer	No	The unique identifier of the pci special note applied to the vulnerability or service finding.	*dim_pci_note*
items_noted	text	No	A list of distinct identifiers for findings on a given asset, port, and protocol.	

fact_policy

added in version 1.2.0

Level of Grain: A summary of findings related to a policy.

Fact Type: accumulating snapshot

Description: This table provides a summary for the results of the most recent policy scan for assets within the scope of the report. For each policy, only assets that are subject to that policy's rules and that have a result in the most recent scan with no overrides are counted.

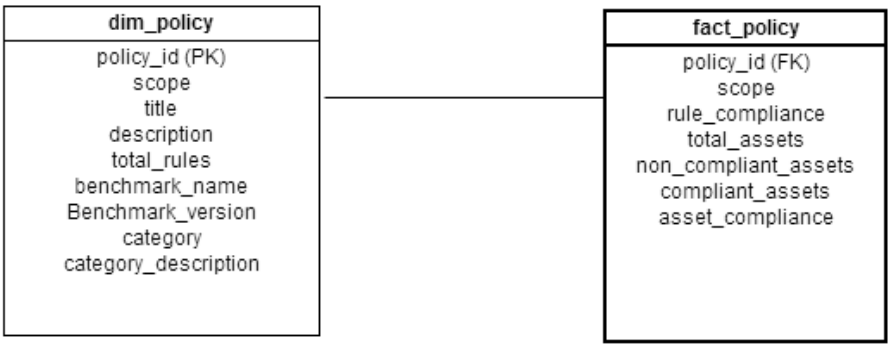
Columns

Note: As of version 1.3.0, a separate value has been created for not_applicable_assets and is no longer included in compliant_assets.

Column	Data Type	Nullable	Description	Associated Dimension
policy_id	bigint	No	The identifier of the policy.	dim_policy
scope	text	No	The identifier for scope of policy. Policies that are automatically available have "Built-in" scope, whereas policies created by users have scope as "Custom".	
rule_compliance	numeric	No	The ratio of policy rule test result that are compliant or not applicable to the total number of rule test results.	

Column	Data Type	Nullable	Description	Associated Dimension
total_ assets	bigint	No	The number of assets within the scope of the report that were tested for the policy.	
compliant_ assets	bigint	No	The number of assets that did not fail but passed at least a rule within the policy in the last test.	
non_ compliant_ assets	bigint	No	The number of assets that failed at least one rule within the policy in the last test.	
not_ applicable_ assets	bigint	No	The number of assets that neither passed nor failed at least a rule within the policy in the last test.	
asset_ compliance	numeric	No	The ratio of assets that are compliant with the policy to the total number of assets that were tested for the policy.	

Dimensional model



Dimensional model for fact_policy

fact_policy_group

added in version 1.3.0

Level of Grain:A summary of findings related to a policy group.

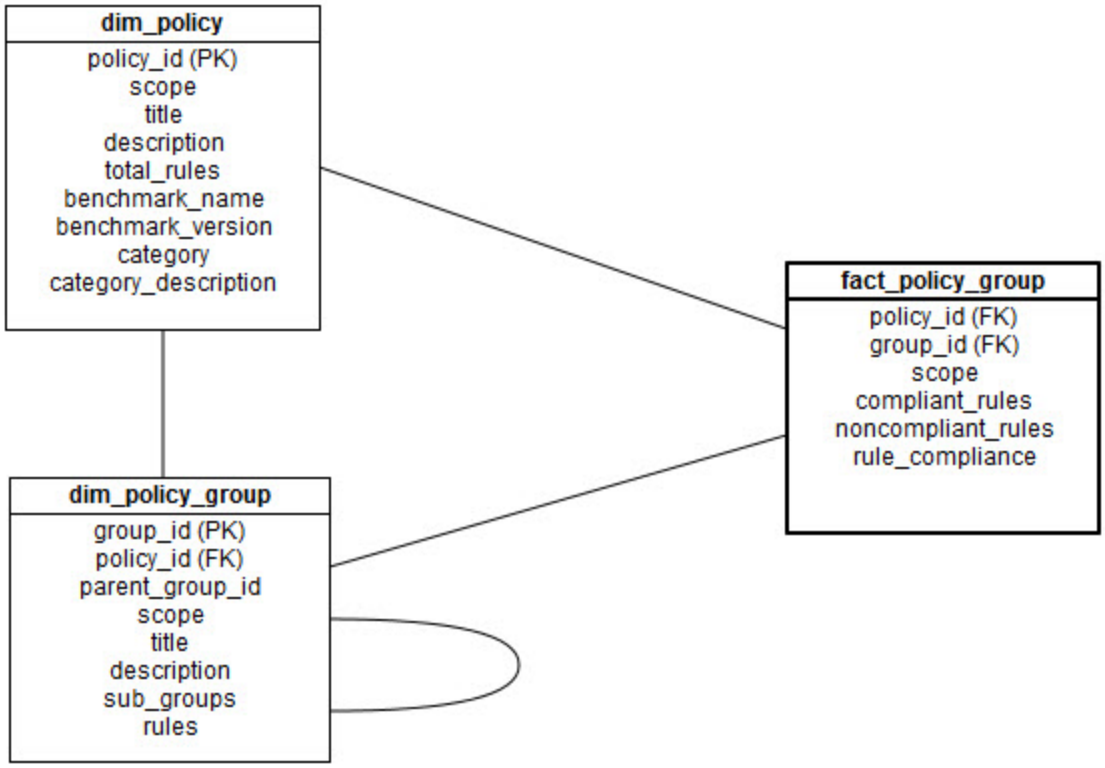
Fact Type: accumulating snapshot

Description: This table provides a summary for the group rules's results of the most recent policy scan for assets within the scope of the report. All rules that are directly or indirectly descend from it and are counted.

Columns

Column	Data Type	Nullable	Description	Associated Dimension
scope	text	No	The identifier for scope of policy. Policies that are automatically available have "Built-in" scope, whereas policies created by users have scope as "Custom".	
policy_id	bigint	No	The identifier of the policy.	dim_policy
group_id	bigint	No	The identifier of the policy group.	dim_policy_group
non_compliant_rules	integer	No	The number of rules that doesn't have 100% asset compliance (taking into account policy rule overrides.)	
compliant_rules	integer	No	The number of rules that have 100% asset compliance (taking into account policy rule overrides.)	
rule_compliance	numeric	True	The ratio of rule test result that are compliant or not applicable to the total number of rule test results within the policy group. If the group has no rule or no testable rules (rule with no check, hence no result exists), this will have a null value.	

Dimensional model



Dimensional model for fact_policy_group

fact_policy_rule

added in version 1.3.0

Level of Grain:A summary of findings related to a policy rule.

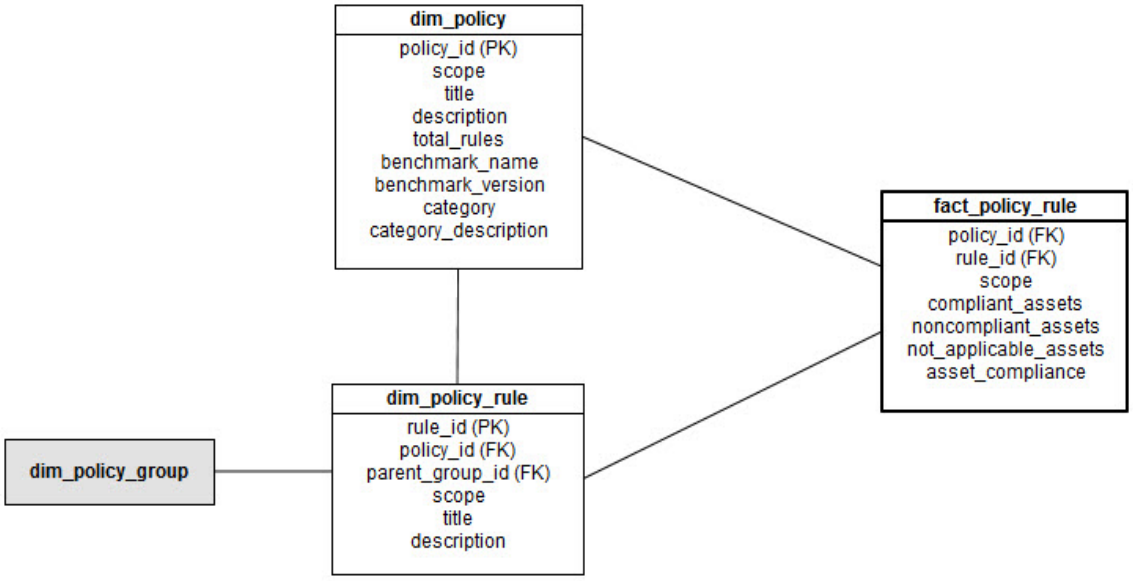
Fact Type: accumulating snapshot

Description: This table provides a summary for the rule results of the most recent policy scan for assets within the scope of the report. For each rule, only assets that are subject to that rule and that have a result in the most recent scan are counted.

Columns

Column	Data Type	Nullable	Description	Associated Dimension
scope	text	No	The identifier for scope of policy. Policies that are automatically available have "Built-in" scope, whereas policies created by users have scope as "Custom".	
policy_id	bigint	No	The identifier of the policy.	dim_policy
rule_id	bigint	No	The identifier of the policy rule.	dim_policy_rule
compliant_assets	integer	No	The number of assets that are compliant with the rule (taking into account policy rule overrides.)	
noncompliant_assets	integer	No	The number of assets that are not compliant with the rule (taking into account policy rule overrides.)	
not_applicable_asset	integer	No	The number of assets that are not applicable for the rule (taking into account policy rule overrides.)	
asset_compliance	numeric	No	The ratio of assets that are compliant with the policy rule to the total number of assets that were tested for the policy rule.	

Dimensional model



Dimensional model for fact_policy_rule

fact_remediation (count, sort_column)

added in version 1.1.0

Level of Grain: A solution with the highest level of supercedence and the effect applying that solution would have on the scope of the report.

Fact Type: accumulating snapshot

Description: A function which returns a result set of the top "count" solutions showing their impact as specified by the sorting criteria. The criteria can be used to find solutions that have a desirable impact on the scope of the report, and can be limited to a subset of all solutions. The aggregate effect of applying each solution is computed and returned for each record. Only the highest-level superceding solutions will be selected, in other words, only solutions which have no superceding solution.

Arguments

Column	Data type	Description
count	integer	The number of solutions to limit the output of this function to. The sorting and aggregation are performed prior to the limit.

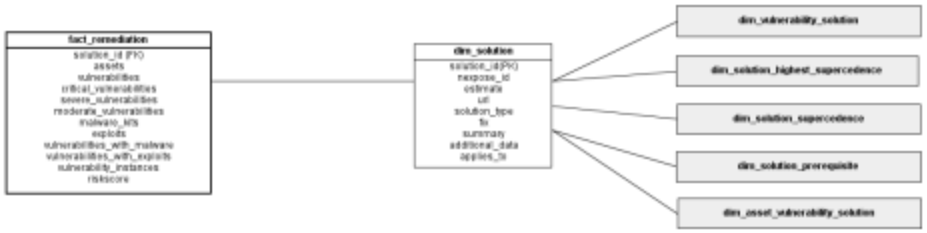
Column	Data type	Description
sort_column	text	The name and sort order of the column to sort results by. Any column within the fact can be used to sort the results prior to them being limited. Multiple columns can be sorted using a traditional SQL fragment (Example: 'assets DESC, *exploits* DESC').

Columns

Column	Data type	Nullable	Description	Associated dimension
solution_id	integer	No	The identifier of the solution.	
assets	bigint	No	The number of assets that require the solution to be applied. If the solution applies to a vulnerability not detected on any asset, the value may be zero.	
vulnerabilities	numeric	No	The total number of vulnerabilities that would be remediated.	
critical_vulnerabilities	numeric	No	The total number of critical vulnerabilities that would be remediated.	
severe_vulnerabilities	numeric	No	The total number of severe vulnerabilities that would be remediated.	
moderate_vulnerabilities	numeric	No	The total number of moderate vulnerabilities that would be remediated.	
malware_kits	integer	No	The total number of malware kits that would no longer be used to exploit vulnerabilities if the solution were applied.	
exploits	integer	No	The total number of exploits that could no longer be used to exploit vulnerabilities if the solution were applied.	

Column	Data type	Nullable	Description	Associated dimension
vulnerabilities_with_malware	integer	No	The total number of vulnerabilities with a known malware kit that would remediated by the solution.	
vulnerabilities_with_exploits	integer	No	The total number of vulnerabilities with a published exploit module that would remediated by the solution.	
vulnerability_instances	numeric	No	The total number of occurrences of any vulnerabilities that are remediated by the solution.	
riskscore	double precision	No	The risk score that is reduced by performing the remediation.	
pci_status	text	No	The PCI compliance status; either *Pass* or *Fail.*	

Dimensional model



Dimensional model for fact_remediation(count, sort_column)

fact_remediation_impact (count, sort_column)

added in version 1.1.0

Level of Grain: A solution with the highest level of supercedence and the affect applying that solution would have on the scope of the report.

Fact Type: accumulating snapshot

Description: Fact that provides a summarization of the impact that applying a subset of all remediations would have on the scope of the report. The criteria can be used to find solutions that have a desirable impact on the scope of the report, and can be limited to a subset of all solutions. The aggregate effect of applying all solutions is computed and returned as a single record. This fact will be guaranteed to return one and only one record.

Arguments

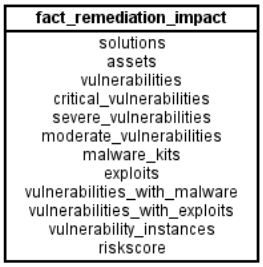
Column	Data type	Description
count	integer	The number of solutions to determine the impact for. The sorting and aggregation are performed prior to the limit.
sort_ column	text	The name and sort order of the column to sort results by. Any column within the fact can be used to sort the results prior to them being limited. Multiple columns can be sorted using a traditional SQL fragment (Example: 'assets DESC, exploits DESC').

Columns

Column	Data type	Nullable	Description	Associated dimension
solutions	integer	No	The number of solutions selected and for which the remediation impact is being summarized (will be less than or equal to count).	
assets	bigint	No	The total number of assets that require a remediation to be applied.	
vulnerabilities	bigint	No	The total number of vulnerabilities that would be remediated.	
critical_ vulnerabilities	bigint	No	The total number of critical vulnerabilities that would be remediated.	
severe_ vulnerabilities	bigint	No	The total number of severe vulnerabilities that would be remediated.	
moderate_ vulnerabilities	bigint	No	The total number of moderate vulnerabilities that would be remediated.	

Column	Data type	Nullable	Description	Associated dimension
malware_kits	integer	No	The total number of malware kits that would no longer be used to exploit vulnerabilities if all selected remediations were applied.	
exploits	integer	No	The total number of exploits that would no longer be used to exploit vulnerabilities if all selected remediations were applied.	
vulnerabilities_with_malware	integer	No	The number of vulnerabilities with a known malware kit that would be remediated.	
vulnerabilities_with_exploits	integer	No	The number of vulnerabilities with a known exploit that would be remediated.	
vulnerability_instances	bigint	No	The total number of occurrences of any vulnerabilities that are remediated by any remediation selected.	
riskscore	double precision	No	The risk score that is reduced by performing all the selected remediations.	
pci_status	text	No	The PCI compliance status; either *Pass* or *Fail.*	

Dimensional model



Dimensional model for fact_remediation_impact(count, sort_column)

fact_scan

Level of Grain: A summary of the results of a scan.

Fact Type: accumulating snapshot

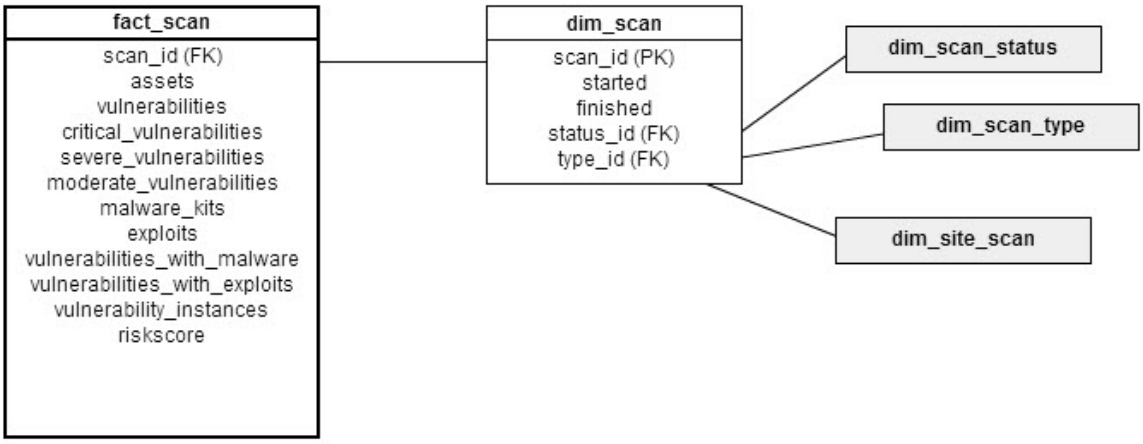
Description: The *fact_scan* fact provides the summarized information for every scan any asset within the scope of the report was scanned during. For each scan, there will be a record in this fact table with the summarized results.

Columns

Column	Data type	Nullable	Description	Associated dimension
scan_id	bigint	No	The identifier of the scan.	*dim_scan*
assets	bigint	No	The number of assets that were scanned	
vulnerabilities	bigint	No	The number of all vulnerabilities discovered in the scan.	
critical_ vulnerabilities	bigint	No	The number of all critical vulnerabilities discovered in the scan.	
severe_ vulnerabilities	bigint	No	The number of all severe vulnerabilities discovered in the scan.	
moderate_ vulnerabilities	bigint	No	The number of all moderate vulnerabilities discovered in the scan.	
malware_kits	integer	No	The number of malware kits associated with vulnerabilities discovered in the scan.	
exploits	integer	No	The number of exploits associated with vulnerabilities discovered in the scan.	
vulnerabilities_ with_malware	integer	No	The number of vulnerabilities with a malware kit discovered in the scan.	
vulnerabilities_ with_exploits	integer	No	The number of vulnerabilities with an exploit discovered in the scan.	
vulnerability_ instances	bigint	No	The number of vulnerability instances discovered during the scan.	

Column	Data type	Nullable	Description	Associated dimension
riskscore	double precision	No	The risk score for the scan results	
pci_status	text	No	The PCI compliance status; either *Pass* or *Fail.*	

Dimensional model



Dimensional model for fact_scan

fact_site

Level of Grain: A summary of the current state of a site.

Fact Type: accumulating snapshot

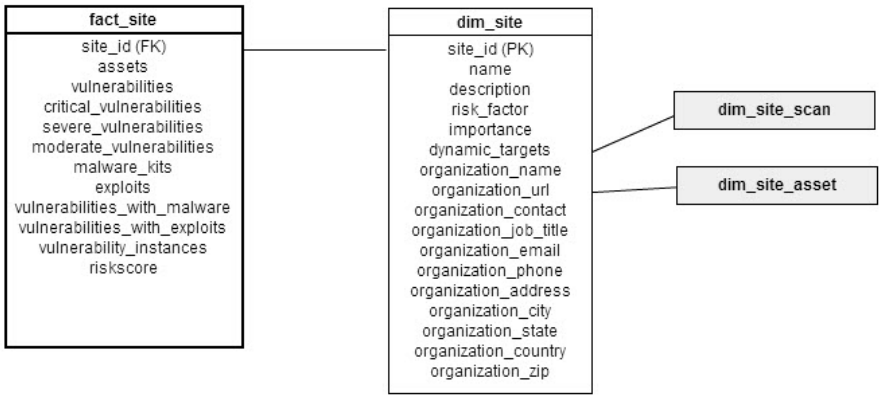
Description: The *fact_site* table provides a summary record at the level of grain for every site that any asset in the scope of the report belongs to. For each site, there will be a record in this fact table with the summarized results, taking into account any vulnerability filters specified in the report configuration. The summary of each site will display the accumulated information for the most recent scan of each asset, not just the most recent scan of the site.

Columns

Column	Data type	Nullable	Description	Associated dimension
site_id	bigint	No	The identifier of the site.	*dim_site*

Column	Data type	Nullable	Description	Associated dimension
assets	bigint	No	The total number of assets in the site.	
last_scan_id	bigint	No	The identifier of the most recent scan for the site.	
vulnerabilities	bigint	No	The number of vulnerabilities discovered on assets in the site.	
critical_ vulnerabilities	bigint	No	The number of critical vulnerabilities discovered on assets in the site.	
severe_ vulnerabilities	bigint	No	The number of severe vulnerabilities discovered on assets in the site.	
moderate_ vulnerabilities	bigint	No	The number of moderate vulnerabilities discovered on assets in the site.	
malware_kits	integer	No	The number malware kits associated with vulnerabilities discovered on assets in the site.	
exploits	integer	No	The number exploits associated with vulnerabilities discovered on assets in the site.	
vulnerabilities_ with_malware	integer	No	The number of vulnerabilities with a malware kit discovered on assets in the site.	
vulnerabilities_ with_exploits	integer	No	The number of vulnerabilities with an exploit kit discovered on assets in the site.	
vulnerability_ instances	bigint	No	The number of vulnerability instances discovered on assets in the site.	
riskscore	double precision	No	The risk score of the site.	
pci_status	text	No	The PCI compliance status; either *Pass* or *Fail.*	

Dimensional model



Dimensional model for fact_site

fact_site_date (startDate, endDate, dateInterval)

Added in version 1.1.0

Level of Grain: A site and its summary information on a specific date.

Fact Type: periodic snapshot

Description: This fact table provides a periodic snapshot for summarized values on a site by date. The fact table takes three dynamic arguments, which refine what data is returned. Starting from startDate and ending on endDate, a summarized value for each site in the scope of the report will be returned for every dateInterval period of time. This will allow trending on site information by a customizable interval of time. In terms of a chart, startDate represents the lowest value in the range, the endDate the largest value in the range, and the dateInterval is the separation of the ticks of the range axis. If a site did not exist prior to a summarization date, it will have no record for that date value. The summarized values of a site represent the state of the site in the most recent scans prior to the date being summarized; therefore, if a site has not been scanned before the next summary interval, the values for the site will remain the same.

For example, fact_site_date('2013-01-01', '2014-01-01', INTERVAL '1 month') will return a row for each site for every month in the year 2013.

Arguments

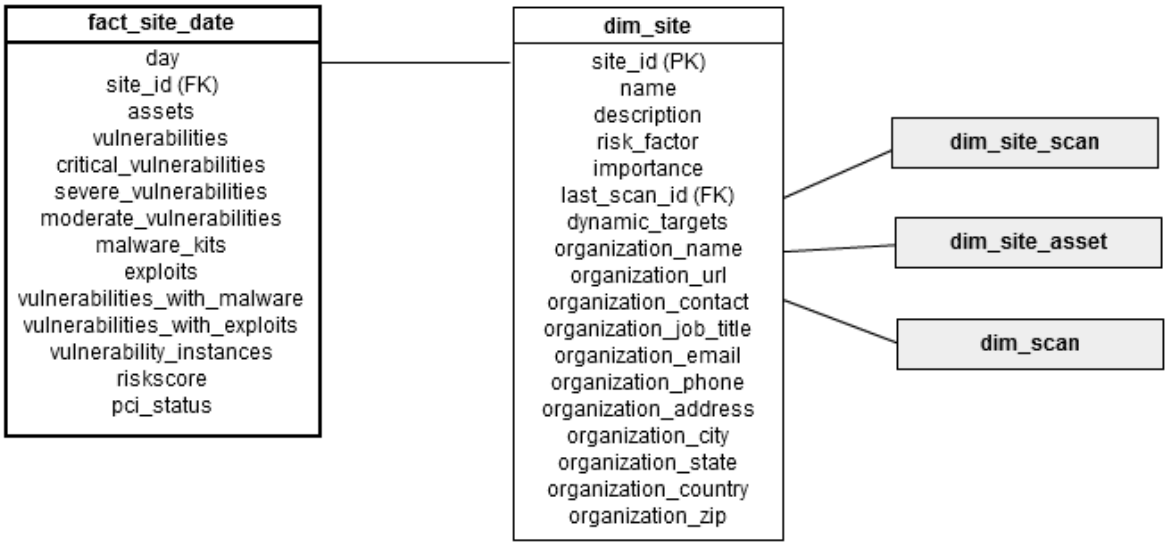
Column	Data type	Description
startDate	date	The first date to return summarizations for.
endDate	date	The last date to return summarizations for.
dateInterval	interval	The interval between the start and end date to return summarizations for.

Columns

Column	Data type	Nullable	Description	Associated dimension
site_id	bigint	No	The identifier of the site.	*dim_site*
assets	bigint	No	The total number of assets in the site.	
last_scan_id	bigint	No	The identifier of the most recent scan for the site.	
vulnerabilities	bigint	No	The number of vulnerabilities discovered on assets in the site.	
critical_ vulnerabilities	bigint	No	The number of critical vulnerabilities discovered on assets in the site.	
severe_ vulnerabilities	bigint	No	The number of severe vulnerabilities discovered on assets in the site.	
moderate_ vulnerabilities	bigint	No	The number of moderate vulnerabilities discovered on assets in the site.	
malware_kits	integer	No	The number malware kits associated with vulnerabilities discovered on assets in the site.	
exploits	integer	No	The number exploits associated with vulnerabilities discovered on assets in the site.	
vulnerabilities_ with_malware	integer	No	The number of vulnerabilities with a malware kit discovered on assets in the site.	
vulnerabilities_ with_exploits	integer	No	The number of vulnerabilities with an exploit kit discovered on assets in the site.	
vulnerability_ instances	bigint	No	The number of vulnerability instances discovered on assets in the site.	
riskscore	double precision	No	The risk score of the site.	
pci_status	text	No	The PCI compliance status; either *Pass* or *Fail.*	

Column	Data type	Nullable	Description	Associated dimension
day	date	No	The date of the summarization of the asset.	

Dimensional model



Dimensional model for fact_site_date(startDate, endDate, dateInterval)

fact_site_policy_date

added in version 1.3.0

Type: Periodic snapshot

Description: This fact table provides a periodic snapshot for summarized policy values on site by date. The fact table takes three dynamic arguments, which refine what data is returned. Starting from startDate and ending on endDate, the summarized policy value for each site in the scope of the report will be returned for every dateInterval period of time. This will allow trending on site information by a customizable interval of time. In terms of a chart, startDate represents the lowest value in the range, the endDate the largest value in the range, and the dateInterval is the separation of the ticks of the range axis. If a site did not exist prior to a summarization date, it will have no record for that date value. The summarized policy values of a site represent the state of the site prior to the date being summarized; therefore, if the site has not been scanned before the next summary interval, the values for the site will remain the same.

Arguments

Column	Data type	Nullable	Description
startDate	date	No	The first date to return summarizations for.
endDate	date	No	The end of the period where the scan results of an asset will be returned. If it is later the the current date, it will be replaced by the later.
dateInterval	interval	No	The interval between the start and end date to return summarizations for.

Columns

Column	Data type	Nullable	Description	Associated Dimension
site_id	bigint	Yes	The unique identifier of the site.	dim_site
day	date	No	The date when the summarized policy scan results snapshot is taken.	
policy_id	bigint	Yes	The unique identifier of the policy within a scope.	dim_site
scope	text	Yes	The identifier for scope of policy. Policies that are automatically available have "Built-in" scope, whereas policies created by users have scope as "Custom".	
assets	integer	Yes	The total number of assets that are in the scope of the report and associated to the asset group.	

Column	Data type	Nullable	Description	Associated Dimension
compliant_ assets	integer	Yes	The number of assets associated to the asset group that have not failed any while passed at least one policy rule test.	
noncompliant_ assets	integer	Yes	The number of assets associated to the asset group that have failed at least one policy rule test.	
not_ applicable_ assets	integer	Yes	The number of assets associated to the asset group that have neither failed nor passed at least one policy rule test.	
rule_ compliance	numeric	Yes	The ratio of policy rule test result that are compliant or not applicable to the total number of rule test results.	

fact_tag

added in version 1.2.0

Level of Grain: The current summary information for a tag.

Fact Type: Accumulating snapshot

Description: The *fact_tag* table provides an accumulating snapshot fact for the summary information of a tag. The summary information provided is based on the most recent scan of every asset associated with the tag. If a tag has no accessible assets, there will be a fact record with zero counts. Only tags associated with assets, sites, or asset groups in the scope of the report will be present in this fact.

Columns

Column	Data type	Nullable	Description	Associated dimension
tag_id	integer	No	The unique identifier of the tag.	*dim_tag*
assets	bigint	No	The total number of accessible assets associated with the tag. If the tag has no accessible assets in the current scope or membership, this value can be zero.	
vulnerabilities	bigint	No	The sum of the count of vulnerabilities on each asset. This value is equal to the sum of the critical_vulnerabilities, severe_vulnerabilities, and moderate_vulnerabilities columns.	
critical_ vulnerabilities	bigint	No	The sum of the count of critical vulnerabilities on each asset.	
severe_ vulnerabilities	bigint	No	The sum of the count of severe vulnerabilities on each asset.	
moderate_ vulnerabilities	bigint	No	The sum of the count of moderate vulnerabilities on each asset.	
malware_kits	integer	No	The sum of the count of malware kits on each asset.	
exploits	integer	No	The sum of the count of exploits on each asset.	
vulnerabilities_ with_ malware_kit	integer	No	The sum of the count of vulnerabilities with malware kits on each asset.	
vulnerabilities_ with_exploit	integer	No	The sum of the count of vulnerabilities with exploits on each asset.	
vulnerability_ instances	bigint	No	The sum of the vulnerability instances on each asset.	

Column	Data type	Nullable	Description	Associated dimension
riskscore	double precision	No	The sum of the risk score on each asset.	
pci_status	text	No	The PCI compliance status; either *Pass* or *Fail* *of the assets that have the tag.*	

fact_tag_policy_date

added in version 1.3.0

Type: Periodic snapshot

Description: The *fact_tag_policy_date* table provides an accumulating snapshot fact for summarized policy information of a tag. The summarized policy information provided is based on the most recent scan of every asset associated with the tag. If a tag has no accessible assets, there will be a fact record with zero counts. Only tags associated with assets, sites, or asset groups in the scope of the report will be present in this fact.

Arguments

Column	Data type	Nullable	Description
startDate	date	No	The first date to return summarizations for.
endDate	date	No	The end of the period where the scan results of an asset will be returned. If it is later the the current date, it will be replaced by the later.
dateInterval	interval	No	The interval between the start and end date to return summarizations for.

Columns

Column	Data type	Nullable	Description	Associated Dimension
tag_id	bigint	Yes	The unique identifier of the tag.	dim_tag
day	date	No	The date which the summarized policy scan results snapshot is taken.	
policy_id	bigint	Yes	The unqique identifier of the policy within a scope.	dim_policy
scope	text	Yes	The identifier for scope of policy. Policies that are automatically available have "Built-in" scope, whereas policies created by users have scope as "Custom".	
assets	integer	Yes	The total number of assets that are in the scope of the report and associated to the asset group.	
compliant_ assets	integer	Yes	The number of assets associated to the asset group that have not failed any while passed at least one policy rule test.	
noncompliant_ assets	integer	Yes	The number of assets associated to the asset group that have failed at least one policy rule test.	

Column	Data type	Nullable	Description	Associated Dimension
not_ applicable_ assets	integer	Yes	The number of assets associated to the asset group that have neither failed nor passed at least one policy rule test.	
rule_ compliance	numeric	Yes	The ratio of PASS or NOT APPLICABLE results for the rules to the total number rule results.	

fact_vulnerability

added in version 1.1.0

Level of Grain: A summary of findings of a vulnerability.

Fact Type: accumulating snapshot

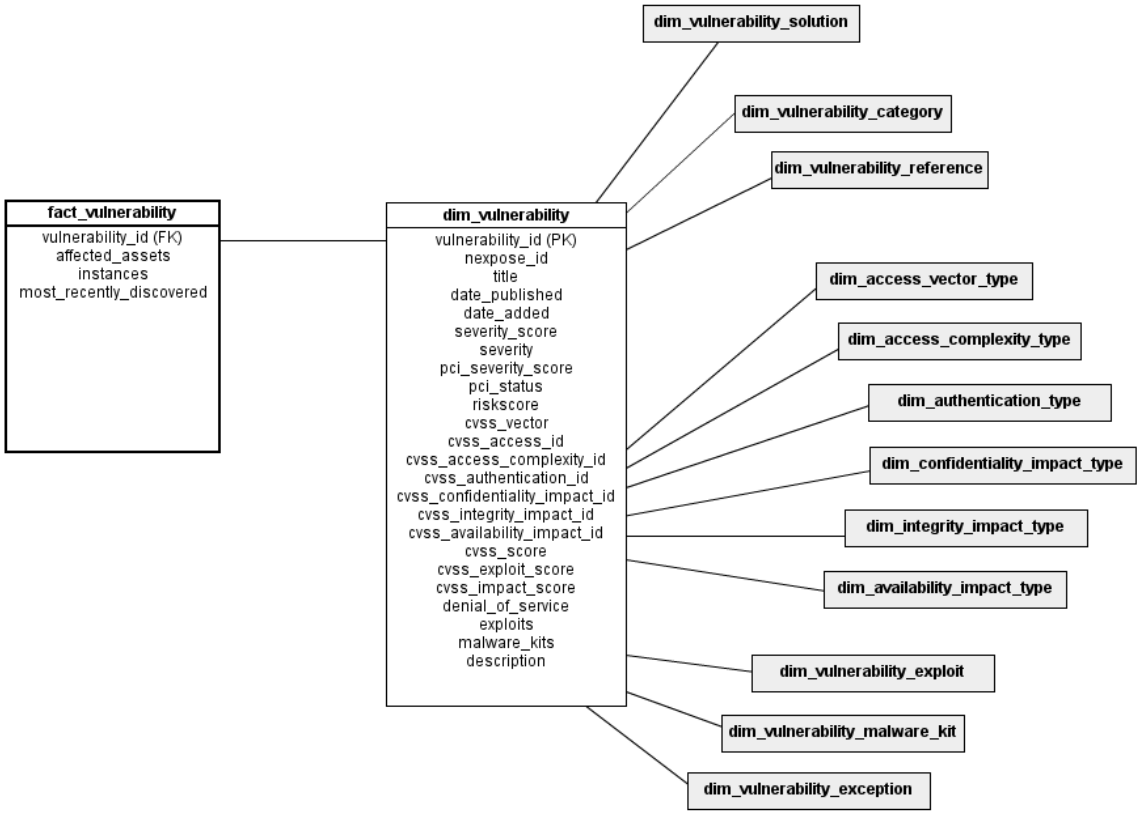
Description: The *fact_vulnerability* table provides a summarized record for each vulnerability within the scope of the report. For each vulnerability, the count of assets subject to the vulnerability is measured. Only assets with a finding in their most recent scan with no exception applied are included in the totals.

Columns

Column	Data type	Nullable	Description	Associated dimension
vulnerability_ id	integer	No	The identifier of the vulnerability.	*dim_ vulnerability*
affected_ assets	bigint	No	The number of assets that have the vulnerability. This count may be zero if no assets are vulnerable.	
vulnerability_ instances	bigint	No	The number of instances or occurrences of the vulnerability across all assets.	

Column	Data type	Nullable	Description	Associated dimension
most_ recently_ discovered	timestamp without time zone	No	The most recent date and time at which any asset within the scope of the report was discovered to be vulnerable to the vulnerability.	

Dimensional model



Dimensional model for fact_vulnerability

Understanding the reporting data model: Dimensions

Note: Data model 2.0.0 exposes information about linking assets across sites. All previous information is still available, and in the same format. As of data model 2.0.0, there is a *sites* column in the dim_asset dimension that lists the sites to which an asset belongs.

On this page:

- *Junk Scope Dimensions* on page 462
- *Core Entity Dimensions* on page 466
- *Enumerated and Constant Dimensions* on page 504

See related sections:

- *Creating reports based on SQL queries* on page 383
- *Understanding the reporting data model: Overview and query design* on page 387
- *Understanding the reporting data model: Facts* on page 394
- *Understanding the reporting data model: Functions* on page 521

Junk Scope Dimensions

The following dimensions are provided to allow the report designer access to the specific configuration parameters related to the scope of the report, including vulnerability filters.

dim_pci_note

added in version 1.3.2

Description: Dimension for the text descriptions of PCI special notes.

Type: junk

Columns

Column	Data type	Nullable	Description	Associated dimension
pci_note_id	integer	No	The code that represents the PCI note description	
pci_note_text	text	No	The text detailing the PCI special note.	

dim_scope_asset

Description: Provides access to the assets specifically configured within the configuration of the report. This dimension will contain a record for each asset selected within the report configuration.

Type: junk

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset .	

dim_scope_asset_group

Description: Provides access to the asset groups specifically configured within the configuration of the report. This dimension will contain a record for each asset group selected within the report configuration.

Type: junk

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_group_id	bigint	No	The identifier of the asset group .	dim_asset_group

dim_scope_filter_vulnerability_category_include

Description: Provides access to the names of the vulnerability categories that are configured to be included within the scope of the report. One record will be present for every category that is included. If no vulnerability categories are enabled for inclusion, this dimension table will be empty.

Type: junk

Columns

Column	Data type	Nullable	Description	Associated dimension
name	text	No	The name of the vulnerability category.	dim_vulnerability_category

dim_scope_filter_vulnerability_severity

Description: Provides access to the severity filter enabled within the report configuration. The severity filter is exposed as the maximum severity score a vulnerability can have to be included within the scope of the report. This dimension is guaranteed to only have one record. If no severity filter is explicitly enabled, the minimum severity value will be 0.

Type: junk

Columns

Column	Data type	Nullable	Description	Associated dimension
min_severity	numeric (2)	No	The minimum severity that a vulnerability must have to be included in the scope of the report. If no filter is applied to severity, defaults to 0.	dim_vulnerability_category
severity_description	text	No	A human-readable description of the severity filter that is enabled.	

dim_scope_filter_vulnerability_status

Description: Provides access to the vulnerability status filters enabled within the configuration of the report. A record will be present for every status filter that is enabled, and is guaranteed to have between a minimum one and maximum three statuses enabled.

Type: junk

Columns

Column	Data type	Nullable	Description	Associated dimension
status_id	character (1)	No	The identifier of the vulnerability status.	dim_vulnerability_status

dim_scope_policy

added in version 1.3.0

Description: This is the dimension for all policies within the scope of the report. It contains one record for every policy defined in the report scope. If none has been defined, it contains one record for every policy that has been scanned with at least one asset in the scope of the report.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description
policy_id	bigint	No	The identifier of the policy.
scope	text	No	The identifier for scope of policy. Policies that are automatically available have "Built-in" scope, whereas policies created by users have scope as "Custom".

dim_scope_scan

Description: Provides access to the scans specifically configured within the configuration of the report. This dimension will contain a record for each scan selected within the report configuration.

Type: junk

Columns

Column	Data type	Nullable	Description	Associated dimension
scan_id	bigint	No	The identifier of the asset scan.	dim_scan

dim_scope_site

Description: Provides access to the sites specifically configured within the configuration of the report. This dimension will contain a record for each site selected within the report configuration.

Type: junk

Columns

Column	Data type	Nullable	Description	Associated dimension
site_id	integer	No	The identifier of the site.	dim_site

Core Entity Dimensions

dim_asset

Description: Dimension that provides access to the textual information of all assets configured to be within the scope of the report. Only the information from the most recent scan of each asset is used to provide an accumulating summary. There will be one record in this dimension for every single asset in scope, including assets specified through configuring scans, sites, or asset groups to be within scope.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset.	
mac_address	macaddr	Yes	The primary MAC address of the asset. If an asset has had no MAC address identified, the value will be *null*. If an asset has multiple MAC addresses, the primary or best address is selected.	
ip_address	inet	No	The primary IP address of the asset. If an asset has multiple IP addresses, the primary or best address is selected. The IP address may be an IPv4 or IPv6 address.	

Column	Data type	Nullable	Description	Associated dimension
host_name	text	Yes	The primary host name of the asset. If an asset has had no host name identified, the value will be *null*. If an asset has multiple host names, the primary or best address is selected. If the asset was scanned as a result of configuring the site with a host name target, that name will be guaranteed to be selected ss the primary host name.	
operating_system_id	bigint	No	The identifier of the operating system fingerprint with the highest certainty on the asset. If the asset has no operating system fingerprinted, the value will be -1.	dim_operating_system
host_type_id	integer	No	The identifier of the type of host the asset is classified as. If the host type could not be detected, the value will be -1.	dim_host_type
sites	string	No	Comma separated list of site names. *Added in version 2.0.0*	

dim_asset_file

added in version 1.2.0

Description: Dimension for files and directories that have been enumerated on an asset. Each record represents one file or directory discovered on an asset. If an asset has no files or groups enumerated, there will be no records in this dimension for the asset.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset.	dim_asset

Column	Data type	Nullable	Description	Associated dimension
file_id	bigint	No	The identifier of the file or directory.	
type	text	No	The type of the item: Directory, File, or Unknown.	
name	text	No	The name of the file or directory.	
size	bigint	No	The size of the file or directory in bytes. If the size is unknown, the value will be -1.	

dim_asset_group_account

Description: Dimension that provides the group accounts detected on an asset during the most recent scan of the asset.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset.	dim_asset
name	text	No	The name of the group detected.	

dim_asset_group

Description: Dimension that provides access to the asset groups within the scope of the report. There will be one record in this dimension for every asset group which any asset in the scope of the report is associated to, including assets specified through configuring scans, sites, or asset groups.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_group_id	integer	No	The identifier of the asset group.	
name	text	No	The name of the asset group.	

Column	Data type	Nullable	Description	Associated dimension
description	text	Yes	The optional description of the asset group. If no description is specified, the value will be *null*.	
dynamic_membership	boolean	No	Indicates whether the membership of the asset group is computed dynamically using a dynamic asset filter, or is static (true if this group is a dynamic asset group).	

dim_asset_group_asset

Description: Dimension that provides access to the relationship between an asset group and its associated assets. For each asset group membership of an asset there will be a record in this table.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_group_id	integer	No	The identifier of the asset group.	dim_asset_group
asset_id	bigint	No	The identifier of the asset that belongs to the asset group.	dim_asset

dim_asset_host_name

Description: Dimension that provides all primary and alternate host names for an asset. Unlike the *dim_asset* dimension, this dimension will provide detailed information for the alternate host names detected on the asset. If an asset has no known host names, a record with an unknown host name will be present in this dimension.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset .	dim_asset
host_name	text	No	The host name associated to the asset, or 'Unknown' if no host name is associated with the asset.	
source_type_id	character (1)	No	The identifier of the type of source which was used to detect the host name, or '-' if no host name is associated with the asset.	dim_host_name_source_type

dim_asset_ip_address

Description: Dimension that provides all primary and alternate IP addresses for an asset. Unlike the *dim_asset* dimension, this dimension will provide detailed information for the alternate IP addresses detected on the asset. As each asset is guaranteed to have at least one IP address, this dimension will contain at least one record for every asset in the scope of the report.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset.	dim_asset
ip_address	inet	No	The IP address associated to the asset.	
type	text	No	A description of the type of the IP address, either of the values: “IPv6” or “IPv4”.	

dim_asset_mac_address

Description: Dimension that provides all primary and alternate MAC addresses for an asset. Unlike the dim_asset dimension, this dimension will provide detailed information for the alternate MAC addresses detected on the asset. If an asset has no known MAC addresses, a record with *null* MAC address will be present in this dimension.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset the MAC address was detected on.	dim_asset
address	macaddr	Yes	The MAC address associated to the asset, or *null* if the asset has no known MAC address.	

dim_asset_operating_system

Description: Dimension that provides the primary and all alternate operating system fingerprints for an asset. Unlike the *dim_asset* dimension, this dimension will provide detailed information for all operating system fingerprints on an asset. If an asset has no known operating system, a record with an unknown operating system fingerprint will be present in this dimension.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset.	dim_asset
operating_system_id	bigint	No	The identifier of the operating system, or -1 if there is no known operating system.	dim_operating_system
fingerprint_source_id	integer	No	The source which was used to detect the operating system fingerprint, or -1 if there is no known operating system.	dim_fingerprint_source
certainty	real	No	A value between 0 and 1 indicating the confidence level of the fingerprint. The value is 0 if there no known operating system.	

dim_asset_service

Description: Dimension that provides the services detected on an asset during the most recent scan of the asset. If an asset had no services enumerated during the scan, there will be no records in this dimension.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset.	dim_asset
service_id	integer	No	The identifier of the service.	dim_service
protocol_id	smallint	No	The identifier of the protocol.	dim_protocol
port	integer	No	The port on which the service is running.	
service_fingerprint_id	bigint	No	The identifier of the fingerprint for the service, or -1 if a fingerprint is not available.	dim_service_fingerprint
certainty	real	No	The confidence level of the fingerprint, which ranges from 0 to 1.0. If there is no fingerprint, the value is 0.	

dim_asset_service_configuration

added in version 1.2.1

Description: Dimension that provides the most recent configurations that have been detected on the services of an asset during the latest scan of that asset. Each record represents a configuration value that has been detected on a service (e.g., banner and header values). If an asset has no services detected on it, there will be no records for the asset in the dimension.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset.	dim_asset
service_id	integer	No	The identifier of the service.	dim_service
name	text	No	The name of the configuration value.	
value	text	Yes	The configuration value, which may be empty or null.	
port	integer	No	The port on which the service was running.	

dim_asset_service_credential

added in version 1.3.1

Description: Dimension that presents the most recent credential statuses asserted for services on an asset in the latest scan.

Type: slowly changing

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset.	dim_asset
service_id	integer	No	The identifier of the service.	dim_service
credential_status_id	smallint	No	The identifier of the credential status for the service credential.	dim_credential_status
protocol_id	smallint	No	The identifier of the protocol of the service.	dim_protocol
port	integer	No	The port on which the service is running.	

dim_asset_software

Description: Dimension that provides the software enumerated on an asset during the most recent scan of the asset. If an asset had no software packages enumerated during the scan, there will be no records in this dimension.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset.	dim_asset
software_id	bigint	No	The identifier of the software package.	dim_software
fingerprint_source_id	integer	No	The source which was used to detect the software.	dim_fingerprint_source

dim_asset_user_account

Description: Dimension that provides the user accounts detected on an asset during the most recent scan of the asset.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset .	dim_asset
name	text	Yes	The short, abbreviated name of the user account, which may be *null* .	
full_name	text	Yes	The longer full name of the user account, which may be *null* .	

dim_asset_vulnerability_solution

added in version 1.1.0

Description: Dimension that provides access to what solutions can be used to remediate a vulnerability on an asset. Multiple solutions may be selected as the means to remediate a vulnerability on an asset. This occurs when either a single solution could not be selected, or if multiple solutions must be applied together to perform the remediation. The solutions provided represent only the most direct solutions associated with the vulnerability (those relationships found within the *dim_vulnerability_solution* table). The highest-level superceding solution may be selected by determining the highest-superceding solution for each direct solution on the asset.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The surrogate identifier of the asset.	dim_asset
vulnerability_id	integer	No	The identifier of the vulnerability.	dim_vulnerability
solution_id	integer	No	The surrogate identifier of the solution that may be used to remediate the vulnerability on the asset.	dim_solution

dim_fingerprint_source

Description: Dimension that provides access to the means by which an operating system or software package were detected on an asset.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
fingerprint_source_id	integer	No	The identifier of the source of a fingerprint.	
source	text	No	The description of the source.	

dim_mobile_asset_attribute

added in version 2.0.1

Description: Dimension that provides information about mobile devices.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
asset_id	bigint	No	The identifier of the asset .	dim_asset
attribute_name	text	No	The host name associated to the asset, or 'Unknown' if no host name is associated with the asset. Possible names include: • Mobile Device ID • Mobile Device Useragent • Mobile Device Owner • Mobile Device Model • Mobile Device OS	
attribute_value	text	Yes	The actual value for each of the attributes listed in the attribute_name column, such as the device model or operating system.	

dim_operating_system

Description: Dimension provides access to all operating system fingerprints detected on assets in any scan of the assets within the scope of the report.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
operating_system_id	bigint	No	The identifier of the operating system.	

Column	Data type	Nullable	Description	Associated dimension
asset_type	integer	No	The type of asset the operating system applies to, which categorizes the operating system fingerprint. This type can distinguish the purpose of the asset that the operating system applies to.	
description	text	No	The verbose description of the operating system, which combines the family, vendor, name, and version .	
vendor	text	No	The vendor or publisher of the operating system. If the vendor was not detected, the value will be 'Unknown'.	
family	text	No	The family or product line of the operating system. If the family was not detected, the value will be 'Unknown'.	
name	text	No	The name of the operating system. If the name was not detected, the value will be 'Unknown'.	
version	text	No	The version of the operating system. If the version was not detected, the value will be 'Unknown'.	
architecture	text	No	The architecture the operating system is built for. If the architecture was not detected, the value will be 'Unknown'.	
system	text	No	The terse description of the operating system, which combines the *vendor* and *family* .	
cpe	text	Yes	The Common Platform Enumeration (CPE) value that corresponds to the operating system.	

dim_policy

Description: This is the dimension for all metadata related to a policy. It contains one record for every policy that currently exists in the application.

Type: slowly changing (Type I)

Columns

Column	Data Type	Nullable	Description
policy_id	bigint	No	The identifier of the policy.
scope	text	No	The identifier for scope of policy. Policies that are automatically available have "Built-in" scope, whereas policies created by users have scope as "Custom".
title	text	No	The title of the policy as visible to the user.
description	text		A description of the policy.
total_rules	bigint		The sum of all the rules within the policy
benchmark_name	text		The name of the collection of policies sharing the same source data to which the policy belongs. It includes metadata such as title, name, and applicable systems.
benchmark_version	text		The version number of the benchmark that includes the policy
category	text		A grouping of similar benchmarks based on their source, purpose, or other criteria. Examples include FDCC, USGCB, and CIS.
category_description	text		A description of the category

dim_policy_group

added in version 1.3.0

Description: This is the dimension for all the metadata for each rule within a policy. It contains one record for every rule within each policy.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description
policy_id	bigint	No	The identifier of the policy.

Column	Data type	Nullable	Description
parent_ group_id	bigint	Yes	The identifier of the group this group directly belongs to. If this group belongs directly to the policy this will be null.
scope	text	No	The identifier for scope of policy. Policies that are automatically available have "Built-in" scope, whereas policies created by users have scope as "Custom".
group_id	bigint	No	The identifier of the group.
title	text	Yes	The title of the group that is visible to the user. It describes a logical grouping of the policy rules.
description	text	Yes	A description of the group.
sub_ groups	integer	No	The number of all groups descending from a group.
rules	integer	No	The number of all rules directly or indirectly belonging to a group.

dim_policy_rule

updated in version 1.3.0

Description: This is the dimension for all the metadata for each rule within a policy. It contains one record for every rule within each policy.

Type: slowly changing (Type I)

Columns

Column	Data Type	Nullable	Description
policy_id	bigint	No	The identifier of the policy.
parent_ group_id	bigint	Yes	
scope	text	No	The identifier of the group the rule directly belongs to. If the rule belongs directly to the policy this will be null.
rule_id	bigint	No	The identifier of the rule.

title	text		The title of the rule, for each policy, that is visible to the user. It describes a state or condition with which a tested asset should comply.
description	text		A description of the rule.

dim_policy_override

added in version 1.3.0

Description: Dimension that provides access to all policy rule overrides in any state that may apply to any assets within the scope of the report. This includes overrides that have expired or have been superceded by newer overrides.

Type: slowly changing (Type II)

Columns

Column	Data type	Nullable	Description
override_id	bigint	No	The identifier of the policy rule override.
scope_id	character(1)	No	The identifier for scope of the override.
submitted_by	text	No	The login name of the user that submitted the policy override.
submitted_time	timestamp without time zone	No	The date the override was originally created and submitted.
comments	text	No	The description given at the time the policy override was submitted.
reviewed_by	text	Yes	The login name of the user that reviewed the policy override. If the override has been submitted and has not been reviewed, the value will be null.
review_comments	text	Yes	The comment that accompanies the latest review action. If the exception is submitted and has not been reviewed, the value will be null.

Column	Data type	Nullable	Description
review_state_id	character(1)	No	The identifier of the review state of the override.
effective_time	timestamp without time zone	Yes	The date at which the rule override become effective. If the rule override is under review, the value will be null.
expiration_time	timestamp without time zone	Yes	The date at which the rule override will expire. If the exception has no expiration date set, the value is will be null.
new_status_id	character(1)	No	The identifier of the new value that this override applies to affected policy rule results.

dim_policy_override_scope

added in version 1.3.0

Description: Dimension for the possible scope for a Policy override, such as *Global*, *Asset*, or *Asset Instance*.

Type: normal

Columns

Column	Data type	Nullable	Description
scope_id	character(1)	No	The identifier of the policy rule override scope.
description	text	No	The description of the policy rule override scope.

dim_policy_override_review_state

added in version 1.3.0

Description: Dimension for the possible states for a Policy override, such as *Submitted*, *Approved*, or *Rejected*.

Type: normal

Columns

Column	Data type	Nullable	Description
state_id	character(1)	No	The identifier of the policy rule override state.
description	text	No	The description of the policy rule override state.

dim_policy_result_status

added in version 1.3.0

Description: Dimension for the possible statuses for a Policy Check result, such as Pass, Fail, or Not Applicable.

Type: normal

Columns

Column	Data type	Nullable	Description
status_id	character(1)	No	The identifier of the policy rule status.
description	text	No	The description of the policy rule status code.

dim_scan_engine

added in version 1.2.0

Description: Dimension for all scan engines that are defined. A record is present for each scan engine to which the owner of the report has access.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
scan_engine_id	integer	No	The unique identifier of the scan engine.	
name	text	No	The name of the scan engine.	
address	text	No	The address (either IP or host name) of the scan engine.	
port	integer	No	The port the scan engine is running on.	

dim_scan_template

added in version 1.2.0

Description: Dimension for all scan templates that are defined. A record is present for each scan template in the system.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
scan_ template_id	text	No	The identifier of the scan template.	
name	text	No	The short, human-readable name of the scan template.	
description	text	No	The verbose description of the scan template.	

dim_service

Description: Dimension that provides access to the name of a service detected on an asset in a scan. This dimension will contain a record for every service that was detected during any scan of any asset within the scope of the report.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
service_id	integer	No	The identifier of the service.	
name	text	No	The descriptive name of the service.	

dim_service_fingerprint

Description: Dimension that provides access to the detailed information of a service fingerprint. This dimension will contain a record for every service fingerprinted during any scan of any asset within the scope of the report.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
service_fingerprint_id	bigint	No	The identifier of the service fingerprint.	
vendor	text	No	The vendor name for the service. If the vendor was not detected, the value will be 'Unknown'.	
family	text	No	The family name or product line of the service. If the family was not detected, the value will be 'Unknown'.	
name	text	No	The name of the service. If the name was not detected, the value will be 'Unknown'.	
version	text	No	The version name or number of the service. If the version was not detected, the value will be 'Unknown'.	

dim_site

Description: Dimension that provides access to the textual information of all sites configured to be within the scope of the report. There will be one record in this dimension for every site which any asset in the scope of the report is associated to, including assets specified through configuring scans, sites, or asset groups.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
site_id	integer	No	The identifier of the site.	
name	text	No	The name of the site.	
description	text	Yes	The optional description of the site. If the site has no description, the value will be *null*.	

Column	Data type	Nullable	Description	Associated dimension
risk_factor	real	No	A numeric value that can be used to weight risk score computations. The default value is 1, but possible values from .33 to 3.0 to match the importance level.	
importance	text	No	The importance of the site. The site importance is one of the following values: 'Very Low', 'Low'' 'Normal', 'High', or 'Very High.'	
dynamic_ targets	boolean	No	Indicates whether the list of targets scanned by the site are dynamically configured (dynamic site).	
organization_ name	text	Yes	The optional name of the organization the site is associated to.	
organization_ url	text	Yes	The optional URL of the organization the site is associated to.	
organization_ contact	text	Yes	The optional contact name of the organization the site is associated to.	
organization_ job_title	text	Yes	The optional job title of the contact of the organization the site is associated to.	
organization_ email	text	Yes	The optional e-mail of the contact of the organization the site is associated to.	
organization_ phone	text	Yes	The optional phone number of the organization the site is associated to.	

Column	Data type	Nullable	Description	Associated dimension
organization_address	text	Yes	The optional postal address of the organization the site is associated to.	
organization_city	text	Yes	The optional city name of the organization the site is associated to.	
organization_state	text	Yes	The optional state name of the organization the site is associated to.	
organization_country	text	Yes	The optional country name of the organization the site is associated to.	
organization_zip	text	Yes	The optional zip code of the organization the site is associated to.	
last_scan_id	bigint	No	The identifier of the latest scan of the site that was run.	dim_scan

dim_site_asset

Description: Dimension that provides access to the relationship between a site and its associated assets. For each asset within the scope of the report, a record will be present in this table that links to its associated site. The values in this dimension will change whenever a scan of a site is completed.

Type: slowly changing (Type II)

Columns

Column	Data type	Nullable	Description	Associated dimension
site_id	integer	No	The identifier of the site.	dim_site
asset_id	bigint	No	The identifier of the asset.	dim_asset

dim_scan

Description: Dimension that provides access to the scans for any assets within the scope of the report.

Type: slowly changing (Type II)

Columns

Column	Data type	Nullable	Description	Associated dimension
scan_id	bigint	No	The identifier of the scan.	
started	timestamp without time zone	No	The date and time at which the scan started.	
finished	timestamp without time zone	Yes	The date and time at which the scan finished. If the scan did not complete normally, or is still in progress, this value will be *null*.	
status_id	character(1)	No	The current status of the scan.	dim_scan_status
type_id	character(1)	No	The type of scan, which indicates whether the scan was started manually by a user or on a schedule.	dim_scan_type

dim_site_scan

Description: Dimension that provides access to the relationship between a site and its associated scans. For each scan of a site within the scope of the report, a record will be present in this table.

Type: slowly changing (Type II)

Columns

Column	Data type	Nullable	Description	Associated dimension
site_id	integer	No	The identifier of the site.	dim_site
scan_id	bigint	No	The identifier of the scan.	dim_scan

dim_site_scan_config

added in version 1.2.0

Description: Dimension for the current scan configuration for a site.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
site_id	integer	No	The unique identifier of the site.	dim_site
scan_ template_id	text	No	The identifier of the currently configured scan template.	dim_scan_ template
scan_engine_ id	integer	No	The identifier of the currently configured scan engine.	dim_scan_engine

dim_site_target

added in version 1.2.0

Description: Dimension for all the included and excluded targets of a site. For all sites in the scope of the report, a record will be present for each unique IP range and/or host name defined as an included or excluded address in the site configuration. If any global exclusions are applied, these will also be provided at the site level.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
site_id	integer	No	The identifier of the site.	dim_site
type	text	No	Either *host* or *ip* to indicate the type of address.	
included	boolean	No	True if the target is included in the configuration, or false if it is excluded.	

Column	Data type	Nullable	Description	Associated dimension
target	text	No	The address of the target. If *host*, this is the host name. If *ip* type, this is the IP address in text form (result of running the HOST function).	

dim_software

Description: Dimension that provides access to all the software packages that have been enumerated across all assets within the scope of the report. Each record has detailed information for the fingerprint of the software package.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
software_id	bigint	No	The identifier of the software package.	
vendor	text	No	The vendor that produced or published the software package.	
family	text	No	The family or product line of the software package.	
name	text	No	The name of the software.	
version	text	No	The version of the software.	
software_class_id	integer	No	The identifier of the class of software.	dim_software_class
cpe	text	Yes	The Common Platform Enumeration (CPE) value that corresponds to the software.	

dim_software_class

Description: Dimension for the types of classes of software that can be used to classify or group the purpose of the software.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
software_class_id	integer	No	The identifier of the software class.	
description	text	No	The description of the software class, which may be 'Unknown'.	

dim_solution

added in version 1.1.0

Description: Dimension that provides access to all solutions defined.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
solution_id	integer	No	The identifier of the solution.	
nexpose_id	text	No	The identifier of the solution within the application.	
estimate	interval (0)	No	The amount of required time estimated to implement this solution on a single asset. The minimum value is 0 minutes, and the precision is measured in seconds.	
url	text	Yes	An optional URL link defined for getting more information about the solution. When defined, this may be a web page defined by the vendor that provides more details on the solution, or it may be a download link to a patch.	

Column	Data type	Nullable	Description	Associated dimension
solution_type	solution_type	No	Type of the solution, can be PATCH, ROLLUP or WORKAROUND. A patch type indicates that the solution involves applying a patch to a product or operating system. A rollup patch type indicates that the solution supercedes other vulnerabilities and rolls up many workaround or patch type solutions into one step.	
fix	text	Yes	The steps that are a part of the fix this solution prescribes. The fix will usually contain a list of procedures that must be followed to remediate the vulnerability. The fix will be provided in an HTML format.	
summary	text	No	A short summary of solution which describes the purpose of the solution at a high level and is suitable for use as a summarization of the solution.	
additional_data	text	Yes	Additional information about the solution, in an HTML format.	
applies_to	text	Yes	Textual representation of the types of system, software, and/or services that the solution can be applied to. If the solution is not restricted to a certain type of system, software or service, this field will be null.	

dim_solution_supercedence

added in version 1.1.0

Description: Dimension that provides all superceding associations between solutions. Unlike *dim_solution_highest_supercedence* , this dimension provides access to the entire graph of

superceding relationships. If a solution does not supercede any other solution, it will not have any records in this dimension.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
solution_id	integer	No	The identifier of the solution.	dim_solution
superceding_ solution_id	integer	No	The identifier of the superceding solution .	dim_solution

dim_solution_highest_supercedence

added in version 1.1.0

Description: Dimension that provides access to the highest level superceding solution for every solution. If a solution has multiple superceding solutions that themselves are not superceded, all will be returned. Therefore a single solution may have multiple records returned. If a solution is not superceded by any other solution, it will be marked as being superceded by itself (to allow natural joining behavior).

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
solution_id	integer	No	The identifier of the solution.	dim_ solution
superceding_ solution_id	integer	No	The surrogate identifier of a solution that is known to supercede the solution, and which itself is not superceded (the highest level of supercedence). If the solution is not superceded, this is the same identifier as *solution_id* .	dim_ solution

dim_solution_prerequisite

added in version 1.1.0

Description: Dimension that provides an association between a solution and all the prerequisite solutions that must be applied before it. If a solution has no prerequisites, it will have no records in this dimension.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
solution_id	integer	No	The identifier of the solution.	dim_solution
required_ solution_id	integer	No	The identifier of the solution that is required to be applied before the solution can be applied.	dim_solution

dim_tag

added in version 1.2.0

Description: Dimension for all tags that any assets within the scope of the report belong to. Each tag has either a direct association or indirection association to an asset based off site or asset group association or off dynamic membership criteria.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
tag_id	integer	No	The identifier of the tag.	
tag_ name	text	No	The name of the tag. Names are unique for tags within a type.	
tag_type	text	No	The type of the tag. The supported types are CRITICALITY, LOCATION, OWNER, and CUSTOM.	
source	text	No	The original application that created the tag.	

Column	Data type	Nullable	Description	Associated dimension
creation_date	timestamp	No	The date and time at which the tag was created.	
risk_modifier	float	Yes	The risk modifier for a CRITICALITY typed tag.	
color	text	Yes	The optional color that can be configured for a custom tag.	

dim_tag_asset

added in version 1.2.0

Description: Dimension for the association between an asset and a tag. For each asset there will be one record with an association to only one tag. This dimension only provides current associations. It does not indicate whether an asset was previously associated with a tag.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
tag_id	integer	No	The unique identifier of the tag.	dim_tag
asset_id	bigint	No	The unique identifier of the asset.	dim_asset
association	text	No	TThe association that the tag has with the asset. It can be a direct association (tag) or an indirect association through a site (site), a group (group) or the tag dynamic search criteria (criteria).	
site_id	integer	Yes	The site identifier by which an asset indirectly associates with the tag.	dim_site

Column	Data type	Nullable	Description	Associated dimension
group_id	integer	Yes	The asset group identifier by which an asset indirectly associates with the tag.	dim_asset_group

dim_vulnerability_solution

added in version 1.1.0

Description: Dimension that provides access to the relationship between a vulnerability and its (direct) solutions. These solutions are only those which are directly known to remediate the vulnerability, and does not include rollups or superceding solutions. If a vulnerability has more than one solution, multiple associated records will be present. If a vulnerability has no solutions, it will have no records in this dimension.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
vulnerability_id	integer	No	The identifier of the vulnerability.	dim_vulnerability
solution_id	integer	No	The identifier of the solution that vulnerability may be remediated with.	dim_solution

dim_vulnerability

Description: Dimension for all the metadata related to a vulnerability. This dimension will contain one record for every vulnerability included within the scope of the report. The values in this dimension will change whenever the risk model of the Security Console is modified.

Type: slowly changing (Type I)

Columns

Column	Data type	Nullable	Description	Associated dimension
vulnerability_id	integer	No	The identifier of the vulnerability.	
description	text	No	Long description for the vulnerability.	
nexpose_id	text	No	A textual identifier of a vulnerability unique to the application.	
title	text	No	The short, succinct title of the vulnerability.	
date_published	date	No	The date that the vulnerability was published by the source of the vulnerability (third-party, software vendor, or another authoring source).	
date_added	date	No	The date that the vulnerability was first checked by the application.	
severity_score	smallint	No	The numerical severity of the vulnerability, measured on a scale of 0 to 10 using whole numbers. A value of zero indicates low severity, and a value of 10 indicates high severity.	
severity	text	No	A human-readable description of the severity_score value. Possible values are 'Critical' , 'Severe' , and 'Moderate' .	

Column	Data type	Nullable	Description	Associated dimension
pci_severity_score	smallint	No	The numerical PCI severity score of the vulnerability, measured on a scale of 1 to 5 using whole numbers.	
pci_status	text	No	A human-readable description as to whether if the vulnerability was detected on an asset in a scan it would cause a PCI failure. Possible values are ' Pass ' or ' Fail '.	
riskscore	double precision	No	The risk score of the vulnerability as computed by the risk model currently configured on the Security Console.	
cvss_vector	text	No	A full CVSS vector in the CVSSv2 notation.	
cvss_access_vector_id	character (1)	No	The access vector (AV) code that represents the CVSS access vector value of the vulnerability.	dim_cvss_access_vector_type
cvss_access_complexity_id	character (1)	No	The access complexity (AC) code that represents the CVSS access complexity value of the vulnerability.	dim_cvss_access_complexity_type
cvss_authentication_id	character (1)	No	The authentication (Au) code that represents the CVSS authentication value of the vulnerability.	dim_cvss_access_authentication_type

Column	Data type	Nullable	Description	Associated dimension
cvss_confidentiality_impact_id	character (1)	No	The confidentiality impact (C) code that represents the CVSS confidentiality impact value of the vulnerability.	dim_cvss_confidentiality_impact_type
cvss_integrity_impact_id	character (1)	No	The integrity impact (I) code that represents the CVSS integrity impact value of the vulnerability.	dim_cvss_integrity_impact_type
cvss_availability_impact_id	character (1)	No	The availability impact (A) code that represents the CVSS availability impact value of the vulnerability.	dim_cvss_availability_impact_type
cvss_score	real	No	The CVSS score of the vulnerability, on a scale of 0 to 10.	
pci_adjusted_cvscore	real	No	Value between 0 and 10 representing the CVSS score of the vulnerability, adjusted if necessary according to PCI rules.	s_s
cvss_exploit_score	real	No	The base exploit score contribution to the CVSS score.	
cvss_impact_score	real	No	The base impact score contribution to the CVSS score.	
pci_special_notes	text	Yes	Notes attached to the vulnerability according to PCI rules.	
denial_of_service	boolean	No	Indicates whether the vulnerability is classified as a denial-of-service vulnerability.	

Column	Data type	Nullable	Description	Associated dimension
exploits	bigint	No	The number of distinct exploits that are associated with the vulnerability. If no exploits are associated to this vulnerability, the value will be zero.	
malware_kits	bigint	No	The number of malware kits that are associated with the vulnerability. If no malware kits are associated to this vulnerability, the value will be zero.	
date_modified	date	No	The date the vulnerability was last modified in a content release. The granularity of the date is a day.	

dim_vulnerability_category

Description: Dimension that provides the relationship between a vulnerability and a vulnerability category.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
category_id	integer	No	The identifier of the vulnerability category.	
vulnerability_id	integer	No	The identifier of the vulnerability the category applies to.	dim_vulnerability
category_name	text	No	The descriptive name of the category.	

dim_vulnerability_exception

Description: Dimension that provides access to all vulnerability exceptions in any state (including deleted) that may apply to any assets within the scope of the report. The exceptions available in this dimension will change as the their state changes, or any new exceptions are created over time.

Type: slowly changing (Type II)

Columns

Column	Data type	Nullable	Description	Associated dimension
vulnerability_exception_id	integer	No	The identifier of the vulnerability exception.	
vulnerability_id	integer	No	The identifier of the vulnerability.	dim_vulnerability
scope_id	character (1)	No	The scope of the vulnerability exception, which dictates what assets the exception applies to.	dim_exception_scope
reason_id	character (1)	No	The reason that the vulnerability exception was submitted.	dim_exception_reason
additional_comments	text	Yes	Optional comments associated with the last state change of the vulnerability exception.	
submitted_date	timestamp without time zone	No	The date the vulnerability was originally created and submitted, in the time zone specified by the report configuration.	
submitted_by	text	No	The login name of the user that submitted the vulnerability exception.	

Column	Data type	Nullable	Description	Associated dimension
review_date	timestamp without time zone	Yes	The date the vulnerability exception was reviewed, in the time zone specified by the report configuration. If the exception was rejected, approved, or recalled, this is the date of the last state transition made on the exception. If an exception is submitted and has not been reviewed, the value will be *null*.	
reviewed_by	text	Yes	The login name of the user that reviewed the vulnerability exception. If the exception is submitted and has not been reviewed, the value will be *null*.	
review_comment	text	Yes	The comment that accompanies the latest review action. If the exception is submitted and has not been reviewed, the value will be *null*.	
expiration_date	date	Yes	The date at which the vulnerability exception will expire. If the exception has no expiration date set, the value is will be *null*.	
status_id	character (1)	No	The status (state) of the vulnerability exception.	dim_exception_status
site_id	integer	Yes	The identifier of the site that the exception applies to. If this is not a site-level exception, the value will be *null.*	dim_site
asset_id	bigint	Yes	The identifier of the asset that the exception applies to. If this is not an asset-level or instance-level exception, the value will be *null*.	dim_asset
port	integer	Yes	The port that the exception applies to. If this is not an instance-level exception, the value will be *null*.	

Column	Data type	Nullable	Description	Associated dimension
key	text	Yes	The secondary identifier of the vulnerability the exception applies to. If this is not an instance-level exception, the value will be *null*.	

dim_vulnerability_exploit

Description: Dimension that provides the relationship between a vulnerability and an exploit.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
exploit_id	integer	No	The identifier of the exploit.	
vulnerability_id	integer	No	The identifier of the vulnerability.	dim_vulnerability
title	text	No	The short, succinct title of the exploit.	
description	text	Yes	The optional verbose description of the exploit. If there is no description, the value is *null*.	
skill_level	text	No	The skill level required to perform the exploit. Possible values include 'Expert', 'Novice', and 'Intermediate'.	
source_id	text	No	The source which defined and published the exploit. Possible values include 'Exploit DB' and 'Metasploit Module'.	
source_key	text	No	The identifier of the exploit in the source system, used as a key to index into the publisher's repository of metadata for the exploit.	

dim_vulnerability_malware_kit

Description: Dimension that provides the relationship between a vulnerability and a malware kit.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
vulnerability_id	integer	No	The identifier of the vulnerability the malware kit is associated to.	dim_vulnerability
name	text	No	The name of the malware kit.	
popularity	text	No	The popularity of the malware kit, which signifies how common or accessible it is. Possible values include 'Uncommon', 'Occasional' , 'Rare' , 'Common' , 'Favored' , 'Popular' , and 'Unknown' .	

dim_vulnerability_reference

Description: Dimension that provides the references associated to a vulnerability, which provide links to external sources of data and information related to a vulnerability.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
vulnerability_id	integer	No	The identifier of the vulnerability .	dim_vulnerability
source	text	No	The name of the source of the vulnerability information. The value is guaranteed to be provided in all upper-case characters.	

Column	Data type	Nullable	Description	Associated dimension
reference	text	No	The reference that keys or links into the source of the vulnerability information. If the source is 'URL', the reference is 'URL'. Otherwise, the value is typically a key or identifier that indexes into the source repository.	

Enumerated and Constant Dimensions

The following dimensions are static in nature and all represent mappings of codes, identifiers, and other constant values to human readable descriptions.

dim_access_type

Description: Dimension for the possible CVSS access vector values.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
type_id	character (1)	No	The identifier of the access vector type.	
description	text	No	The description of the access vector type.	

Values

Columns

Notes & Detailed Description	status_id	Description
'L'	'Local'	A vulnerability exploitable with only local access requires the attacker to have either physical access to the vulnerable system or a local (shell) account.
'A'	'Adjacent Network'	A vulnerability exploitable with adjacent network access requires the attacker to have access to either the broadcast or collision domain of the vulnerable software.
'N'	'Network'	A vulnerability exploitable with network access means the vulnerable software is bound to the network stack and the attacker does not require local network access or local access.

dim_aggregated_credential_status

added in version 1.3.1

Description: Dimension the containing the status aggregated across all available services for the given asset in the given scan.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
aggregated_credential_status_id	smallint	No	The credential status ID associated with the fact_asset_scan_service.	No

Column	Data type	Nullable	Description	Associated dimension
aggregated_credential_status_description	text	No	The human-readable description of the credential status.	No

Values

Columns

Notes & Detailed Description	status_id	Description
'No credentials supplied'	1	One or more services for which credential status is reported were detected in the scan, but there were no credentials supplied for any of them.
'All credentials failed'	2	One or more services for which credential status is reported were detected in the scan, and all credentials supplied for these services failed to authenticate.
'Credentials partially successful'	3	At least two of the four services for which credential status is reported were detected in the scan, and for some services the provided credentials failed to authenticate, but for at least one there was a successful authentication.
'All credentials successful'	4	One or more services for which credential status is reported were detected in the scan, and for all of these services for which credentials were supplied authentication with provided credentials was successful.
'N/A'	-1	None of the four applicable services (SNMP, SSH, Telnet, CIFS) was discovered in the scan.

dim_credential_status

added in version 1.3.1

Description: Dimension for the scan service credential status in human-readable form.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
credential_status_id	smallint	No	The credential status ID associated with the fact_asset_scan_service.	
credential_status_description	text	No	The human-readable description of the credential status.	

Values

Columns

Notes & Detailed Description	status_id	Description
'No credentials supplied'	1	No credentials were supplied. Applicable to all four services (SNMP, SSH, Telnet, or CIFS).
'Login failed'	2	The login failed. Applicable to all four services (SNMP, SSH, Telnet, or CIFS).
'Login successful'	3	The login succeeded. The login failed. Applicable to all four services (SNMP, SSH, Telnet, or CIFS).
'Allowed elevation of privileges'	4	Elevation of privileges was allowed. Applicable to SSH only.
'Root'	5	The credentials allowed login as root. Applicable to SSH and Telnet only.
'Login as local admin'	6	The credentials allowed login as local admin. Applicable to CIFS only.

Notes & Detailed Description	status_id	Description
'N/A'	-1	This status is listed for all the services that are not SNMP, SSH, Telnet, or CIFS.

dim_cvss_access_complexity_type

Description: Dimension for the possible CVSS access complexity values.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
type_id	character (1)	No	The identifier of the access complexity type.	
description	text	No	The description of the access complexity type.	

Values

Columns

Notes & Detailed Description	status_id	Description
'H'	'High'	Specialized access conditions exist.
'M'	'Medium'	The access conditions are somewhat specialized.
'L'	'Low'	Specialized access conditions or extenuating circumstances do not exist.

dim_cvss_authentication_type

Description: Dimension for the possible CVSS authentication values.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
type_id	character (1)	No	The identifier of the authentication type.	
description	text	No	The description of the authentication type.	

Values

Columns

Notes & Detailed Description	status_id	Description
'M'	'Multiple'	Exploiting the vulnerability requires that the attacker authenticate two or more times, even if the same credentials are used each time.
'S'	'Single'	The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).
'N'	'None'	Authentication is not required to exploit the vulnerability.

dim_cvss_confidentiality_impact_type

Description: Dimension for the possible CVSS confidentiality impact values.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
type_id	character (1)	No	The identifier of the confidentiality impact type.	
description	text	No	The description of the confidentiality impact type.	

Values

Columns

Notes & Detailed Description	status_id	Description
'P'	'Partial'	There is considerable informational disclosure. Access to some system files is possible, but the attacker does not have control over what is obtained, or the scope of the loss is constrained.
'C'	'Complete'	There is total information disclosure, resulting in all system files being revealed. The attacker is able to read all of the system's data (memory, files, etc.).
'N'	'None'	There is no impact to the confidentiality of the system.

dim_cvss_integrity_impact_type

Description: Dimension for the possible CVSS integrity impact values.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
type_id	character (1)	No	The identifier of the confidentiality impact type.	
description	text	No	The description of the confidentiality impact type.	

Values

Columns

Notes & Detailed Description	status_id	Description
'P'	'Partial'	Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.
'C'	'Complete'	There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised. The attacker is able to modify any files on the target system.
'N'	'None'	There is no impact to the integrity of the system.

dim_cvss_availability_impact_type

Description: Dimension for the possible CVSS availability impact values.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
type_id	character (1)	No	The identifier of the availability impact type.	
description	text	No	The description of the availability impact type.	

Values

Columns

Notes & Detailed Description	status_id	Description
'P'	'Partial'	There is reduced performance or interruptions in resource availability.

Notes & Detailed Description	status_id	Description
'C'	'Complete'	There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.
'N'	'None'	There is no impact to the availability of the system.

dim_exception_scope

Description: Dimension that provides all scopes a vulnerability exception can be defined on.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
scope_id	character (1)	No	The identifier of the scope of a vulnerability exception.	
short_ description	text	No	A succinct, one-word description of the scope.	
description	text	No	A verbose description of the scope.	

Values

Columns

Notes & Detailed Description	scope_ id	short_ description	Description
'G'	'Global'	'All instances (all assets)'	The vulnerability exception is applied to all assets in every site.
'S'	'Site'	'All instances in this site'	The vulnerability exception is applied to only assets within a specific site.

Notes & Detailed Description	scope_ id	short_ description	Description
'A'	'Asset'	'All instances on this asset'	The vulnerability exception is applied to all instances of the vulnerability on an asset.
'I'	'Instance'	'Specific instance on this asset'	The vulnerability exception is applied to a specific instances of the vulnerability on an asset (either all instances without a port, or instances sharing the same port and key).

dim_exception_reason

Description: Dimension for all possible reasons that can be used within a vulnerability exception.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
reason_id	character (1)	No	The identifier for the reason of the vulnerability exception.	
description	text	No		

Values

Columns

Notes & Detailed Description	reason_id	Description
'F'	'False positive'	The vulnerability is a false-positive and was confirmed to be an inaccurate result.
'C'	'Compensating control'	There is a compensating control in place unique to the site or environment that mitigates the vulnerability.

Notes & Detailed Description	reason_id	Description
'R'	'Acceptable risk'	The vulnerability is deemed an acceptable risk to the organization.
'U'	'Acceptable use'	The vulnerability is deemed to be acceptable with normal use (not a vulnerability to the organization).
'O'	'Other'	Any other reason not covered in a build-in reason.

dim_exception_status

Description: Dimension for the possible statuses (states) of a vulnerability exception.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
status_id	character (1)	No	The identifier of the exception status.	
description	text	No	The description or name of the exception status.	

Values

Columns

Notes & Detailed Description	status_id	Description
'U'	'Under review'	The exception was submitted and is waiting for review from an approver.
'A'	'Approved'	The exception was approved by a reviewer and is actively applied.
'R'	'Rejected'	The exception was rejected by the reviewer and requires further action by the submitter.

Notes & Detailed Description	status_id	Description
'D'	'Recalled'	The exception was deleted by the reviewer or recalled by the submitted.
'E'	'Expired'	The exception has expired due to an expiration date.

dim_host_name_source_type

Description: Dimension for the types of sources used to detect a host name on an asset.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
type_id	character (1)	No	The identifier of the source type.	
description	text	No	The description of the source type code.	

Values

Columns

Notes & Detailed Description	type_id	Description
'T'	'User Defined'	The host name of the asset was acquired as a result of being specified as a target within the scan (in the site configuration).
'D'	'DNS'	The host name discovered during a scan using the domain name system (DNS).
'N'	'NetBIOS'	The host name was discovered during a scan using the NetBios protocol.
'-'	'N/A'	The source of the host name could not be determined or is unknown.

dim_host_type

Description: Dimension for the types of hosts that an asset can be classified as.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
host_type_id	integer	No	The identifier of the host type.	
description	text	No	The description of the host type code.	

Values

Columns

Notes & Detailed Description	host_type_id	Description
1	'Virtual Machine'	The asset is a generic virtualized asset resident within a virtual machine.
2	'Hypervisor'	The asset is a virtualized asset within Hypervisor.
3	'Bare Metal'	The asset is a physical machine.
-1	'Unknown'	The asset type is unknown or could not be determined.

dim_scan_status

Description: Dimension for all possible statuses of a scan.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
status_id	character (1)	No	The identifier of the status a scan can have.	

Column	Data type	Nullable	Description	Associated dimension
description	text	No	The description of the status code.	

Values

Columns

Notes & Detailed Description	Status_id	Description
'A'	'Aborted'	The scan was either manually or automatically aborted by the system. If a scan is marked as aborted, it usually terminated abnormally. Aborted scans can occur when an engine is interrupted (terminated) while a scan is actively running.
'C'	'Successful'	The scan was successfully completed and no errors were encountered (this includes scans that were manually or automatically resumed).
'U'	'Running'	The scan is actively running and is in a non-paused state.
'S'	'Stopped'	The scan was manually stopped by the user.
'E'	'Failed'	The scan failed to launch or run successfully.
'P'	'Paused'	The scan is halted because a user manually paused the scan or the scan has met its maximum scan duration.
'-'	'Unknown'	The status of the scan cannot be determined.

dim_scan_type

Description: Dimension for all possible types of scans.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
type_id	character (1)	No	The identifier of the type a scan can be.	
description	text	No	The description of the type code.	

Values

Columns

Notes & Detailed Description	type_id	Description
'A'	'Manual'	The scan was manually launched by a user.
'S'	'Scheduled'	The scan was launched automatically by the Security Console on a schedule.
'-'	'Unknown'	The scan type could not be determined or is unknown.

dim_vulnerability_status

Description: Dimension for the statuses a vulnerability finding result can be classified as.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
status_id	character (1)	No	The identifier of the vulnerability status.	
description	text	No	The description of the vulnerability status.	

Values

Columns

Notes & Detailed Description	status_id	Description
'2'	'Confirmed vulnerability'	The vulnerability was discovered and either exploited or confirmed.
'3'	'Vulnerable version'	The vulnerability was discovered within a version of the installed software or operating system.
'9'	'Potential vulnerability'	The vulnerability was discovered, but not exploited or confirmed.

dim_protocol

Description: Dimension that provides all possible protocols that a service can be utilizing on an asset.

Type: normal

Columns

Column	Data type	Nullable	Description	Associated dimension
protocol_id	integer	No	The identifier of the protocol.	
name	text	No	The name of the protocol.	
description	text	No	The non-abbreviated description of the protocol.	

Values

Columns

protocol_id	Name	Description
0	'IP'	'Internet Protocol'
1	'ICMP'	'Internet Control Message Protocol'
2	'IGMP'	'Internet Group Management Protocol'

protocol_id	Name	Description
3	'GGP'	'Gateway-to-Gateway Protocol'
6	'TCP'	'Transmission Control Protocol'
12	'PUP'	'PARC Universal Protocol'
17	'UDP'	'User Datagram Protocol'
22	'IDP'	'Internet Datagram Protocol'
50	'ESP'	'Encapsulating Security Payload'
77	'ND'	'Network Disk Protocol'
255	‘RAW'	'Raw Packet'
-1	''	'N/A'

Understanding the reporting data model: Functions

See related sections:

- *Creating reports based on SQL queries* on page 383
- *Understanding the reporting data model: Overview and query design* on page 387
- *Understanding the reporting data model: Facts* on page 394
- *Understanding the reporting data model: Dimensions* on page 462

To ease the development and design of queries against the Reporting Data Model, several utility functions are provided to the report designer.

Note: Data model 2.0.0 exposes information about linking assets across sites. All previous information is still available, and in the same format. As of data model 2.0.0, there is a *sites* column in the dim_asset dimension that lists the sites to which an asset belongs.

age

added in version 1.2.0

Description: Computes the difference in time between the specified date and now. Unlike the built-in age function, this function takes as an argument the unit to calculate in. This function will compute the age and round based on the specified unit. Valid unit values are (precision of the output):

- *years* (2 digit precision)
- *months* (2 digit precision)
- *weeks* (2 digit precision)
- *days* (1 digit precision)
- *hours* (1 digit precision)
- *minutes* (0 digit precision)

The computation of age is not timezone aware, and uses heuristic values for time. In other words, the age is computed as the elapsed time between the date and now, not the calendar time. For example, a year is assumed to comprise 365.25 days, and a month 30.4 days.

Input: (timestamp, text) The date to compute the age for, and the unit of the computation.

Output: (numeric) The value of the age, in the unit specified, with a precision based on the input unit.

baselineComparison

Description: A custom aggregate function that performs a comparison between a set of identifiers from two snapshots in time within a grouping expression to return a baseline evaluation result, either 'New', 'Old', or 'Same'. This result indicates whether the entity being grouped appeared in only the most recent state ('New'), in only the previous state ('Old'), or in both states ('Same'). This aggregate can aggregate over the identifiers of objects that are temporal in nature (such as scan identifiers).

Input: (bigint, bigint) The identifier of any value in either the new or old state, followed by the identifier of the most recent state.

Output: (text) A value indicating whether the baseline evaluates to 'New', 'Old', or 'Same'.

csv

added in version 1.2.0

Description: Returns a comma-separated list of values defined within an aggregated group. This function can be used as a replacement for the syntax array_to_string(array_agg(column), ','). When creating the list of values, the order is defined as the order observed in the aggregate.

Input: (text) The textual value to place in the output list.

Output: (text) A comma-separated list of all the values in the aggregate.

htmlToText

added in version 1.2.0

Description: Formats HTML content and structure into a flattened, plain-text format. This function can be used to translate fields with content metadata, such as vulnerability proofs, vulnerability descriptions, solution fixes, etc.

Input: (text) The value containing embedded HTML content to format.

Output: (text) The plain-text representation.

lastScan

Description: Returns the identifier of the most recent scan of an asset.

Input: (bigint) The identifier of the asset.

Output: (bigint) The identifier of the scan that successfully completed most recently on the asset. As every asset must have had one scan completed, this is guaranteed to not return null.

maximumSeverity

added in version 1.2.0

Description: Returns the maximum severity value within an aggregated group. When used across a grouping that contains multiple vulnerabilities with varying severities, this aggregate can be used to select the highest severity of them all. For example, the aggregate of *Severe* and *Moderate* is *Severe*. This aggregate should only be used on columns containing severity rankings for a vulnerability.

Input: (text) A severity value to select from.

Output: (text) The maximum severity value found within a group: *Critical*, *Moderate*, or *Severe*.

previousScan

Description: Returns the identifier of the scan that took place prior to the most recent scan of the asset (see the function lastScan).

Input: (bigint) The identifier of the asset.

Output: (bigint) The identifier of the scan that occurred prior to the most recent scan of the asset. If an asset was only scanned once, this will return null.

proofAsText

Deprecated as of version 1.2.0. Use htmlToText() instead.

Description: Formats the proof of a vulnerability instance to be output into a flattened, plain-text format. This function is an alias for the htmlToText() function.

Input: (text) The proof value to format, which may be null.

Output: (text) The proof value formatted for display as plain text.

scanAsOf

Description: Returns the identifier of the scan that took place on an asset prior to the specified date (exclusive).

Input: (bigint, timestamp) The identifier of the asset and the date to search before.

Output: (bigint) The identifier of the scan that occurred prior to the specified date on the asset, or null if no scan took place on the asset prior to the date.

scanAsOfDate

added in version 1.2.0

Description: Returns the identifier of the scan that took place on an asset prior to the specified date. See *scanAsOf()* if you are using a timestamp field.

Input: (bigint, date) The identifier of the asset and the date to search before.

Output: (bigint) The identifier of the scan that occurred prior to the specified date on the asset, or null if no scan took place on the asset prior to the date.

Distributing, sharing, and exporting reports

When configuring a report, you have a number of options related to how the information will be consumed and by whom. You can restrict report access to one user or a group of users. You can restrict sections of reports that contain sensitive information so that only specific users see these sections. You can control how reports are distributed to users, whether they are sent in e-mails or stored in certain directories. If you are exporting report information to external databases, you can specify certain properties related to the data export.

See the following sections for more information:

- *Working with report owners* on page 525
- *Managing the sharing of reports* on page 527
- *Granting users the report-sharing permission* on page 529
- *Restricting report sections* on page 534
- *Exporting scan data to external databases* on page 537
- *Configuring data warehousing settings* on page 538

Working with report owners

After a report is generated, only a Global Administrator and the designated report owner can see that report on the *Reports* page. You also can have a copy of the report stored in the report owner's directory. See *Storing reports in report owner directories* on page 525.

If you are a Global Administrator, you can assign ownership of the report one of a list of users.

If you are not a Global Administrator, you will automatically become the report owner.

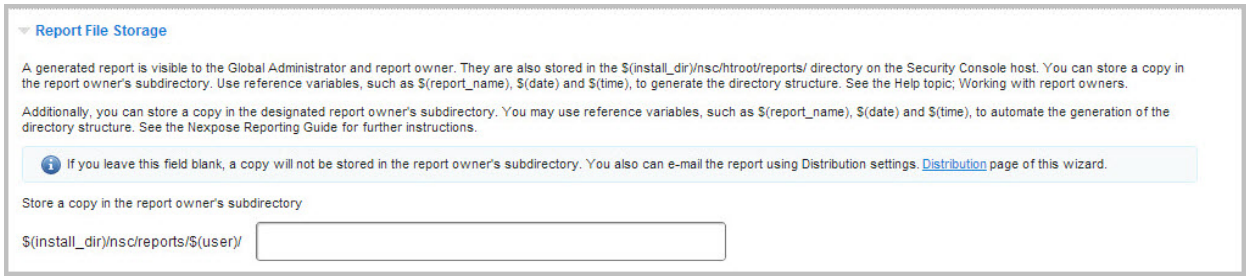
Storing reports in report owner directories

When the application generates a report, it stores it in the reports directory on the Security Console host:

```
[installation_directory]/nsc/reports/[user_name]/
```

You can configure the application to also store a copy of the report in a user directory for the report owner. It is a subdirectory of the reports folder, and it is given the report owner's user name.

1. Click **Configure advanced settings...**on the *Create a report* panel.
2. Click **Report File Storage**.



Report File Storage

3. Enter the report owner's name in the directory field `$(install_dir)/nsc/reports/$(user)`. Replace (`user`) with the report owner's name.

You can use string literals, variables, or a combination of these to create a directory path.

Available variables include:

- `$(date)`: the date that the report is created; format is yyyy-MM-dd
- `$(time)`: the time that the report is created; format is HH-mm-ss
- `$(user)`: the report owner's user name
- `$(report_name)`: the name of the report, which was created on the *General* section of the *Create a Report* panel

After you create the path and run the report, the application creates the report owner's user directory and the subdirectory path that you specified on the *Output* page. Within this subdirectory will be another directory with a hexadecimal identifier containing the report copy.

For example, if you specify the path `windows_scans/$(date)`, you can access the newly created report at:

`reports/[report_owner]/windows_scans/$(date)/[hex_number]/[report_file_name]`

Consider designing a path naming convention that will be useful for classifying and organizing reports. This will become especially useful if you store copies of many reports.

Another option for sharing reports is to distribute them via e-mail. Click the **Distribution** link in the left navigation column to go the *Distribution* page. See *Managing the sharing of reports* on page 527.

Managing the sharing of reports

Every report has a designated owner. When a Global Administrator creates a report, he or she can select a report owner. When any other user creates a report, he or she automatically becomes the owner of the new report.

In the console Web interface, a report and any generated instance of that report, is visible only to the report owner or a Global Administrator. However, it is possible to give a report owner the ability to share instances of a report with other individuals via e-mail or a distributed URL. This expands a report owner's ability to provide important security-related updates to a targeted group of stakeholders. For example, a report owner may want members of an internal IT department to view vulnerability data about a specific set of servers in order to prioritize and then verify remediation tasks.

Note: The granting of this report-sharing permission potentially means that individuals will be able to view asset data to which they would otherwise not have access.

Administering the sharing of reports involves two procedures for administrators:

- configuring the application to redirect users who click the distributed report URL link to the appropriate portal
- granting users the report-sharing permission

Note: If a report owner creates an access list for a report and then copies that report, the copy will not retain the access list of the original report. The owner would need to create a new access list for the copied report.

Report owners who have been granted report-sharing permission can then create a report access list of recipients and configure report-sharing settings.

Configuring URL redirection

By default, URLs of shared reports are directed to the Security Console. To redirect users who click the distributed report URL link to the appropriate portal, you have to add an element to the oem.xml configuration file.

The element reportLinkURL includes an attribute called altURL, with which you can specify the redirect destination.

To specify a redirected URL:

1. Open the oem.xml file, which is located in `[product_installation-directory]/nsc/conf`. If the file does not exist, you can create the file. See the branding guide, which you can request from Technical Support.

   Note: If you are creating the oem.xml file, make sure to specify the tag at the beginning and the tag at the end.

2. Add or edit the reports sub-element to include the reportLinkURL element with the altURL attribute set to the appropriate destination, as in the following example:

```
<reports>

<reportEmail>

<reportSender>account@exampleinc.com</reportSender>

<reportSubject>${report-name}

</reportSubject>

<reportMessage type="link">Your report (${report-name}) was generated
on ${report-date}: ${report-url}

</reportMessage>

<reportMessage type="file">Your report (${report-name}) was generated
on ${report-date}. See attached files.

</reportMessage>

<reportMessage type="zip">Your (${report-name}) was generated on
${report-date}. See attached zip file.

</reportMessage>

</reportEmail>

<reportLinkURL altURL="base_url.net/directory_
path${variable}?loginRedir="/>

</reports>
```

3. Save and close the oem.xml file.
4. Restart the application.

Granting users the report-sharing permission

Global Administrators automatically have permission to share reports. They can also assign this permission to others users or roles.

Assigning the permission to a new user involves the following steps.

1. Go to the *Administration* page, and click the **Create** link next to *Users*.

   (*Optional*) Go to the *Users* page and click **New user**.
2. Configure the new user's account settings as desired.
3. Click the **Roles** link in the *User Configuration* panel.
4. Select the **Custom** role from the drop-down list on the *Roles* page.
5. Select the permission **Add Users to Report**.

   Select any other permissions as desired.
6. Click **Save** when you have finished configuring the account settings.

To assign the permission to an existing user use the following procedure:

1. Go to the *Administration* page, and click the **manage** link next to *Users*.

   (*Optional*) Go to the *Users* page and click the **Edit** icon for one of the listed accounts.
2. Click the **Roles** link in the *User Configuration* panel.
3. Select the **Custom** role from the drop-down list on the *Roles* page.
4. Select the check box labeled **Add Users to Report**.

   Select any other permissions as desired.

   Note: You also can grant this permission by making the user a Global Administrator.
5. Click **Save** when you have finished configuring the account settings.

Creating a report access list

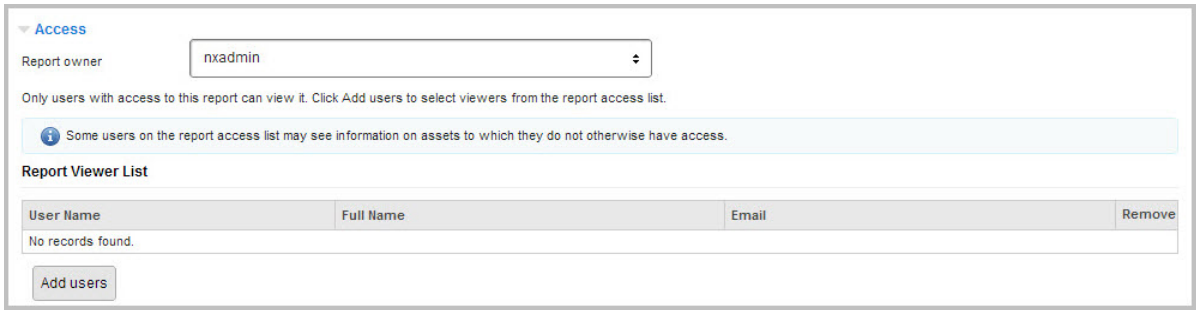
If you are a Global Administrator, or if you have been granted permission to share reports, you can create an access list of users when configuring a report. These users will only be able to view the report. They will not be able to edit or copy it.

Using the Web-based interface to create a report access list

To create a report access list with the Web-based interface, take the following steps:

1. Click **Configure advanced settings...** on the *Create a report* panel.
2. Click **Access**.

   If you are a Global Administrator or have Super-User permissions, you can select a report owner. Otherwise, you are automatically the report owner.



Report Access

3. Click **Add User** to select users for the report access list.

   A list of user accounts appears.
4. Select the check box for each desired user, or select the check box in the top row to select all users.
5. Click **Done**.

   The selected users appear in the report access list.

   Note: Adding a user to a report access list potentially means that individuals will be able to view asset data to which they would otherwise not have access.
6. Click **Run the report** when you have finished configuring the report, including the settings for sharing it.

Using the Web-based interface to configure report-sharing settings

Note: Before you distribute the URL, you must configure URL redirection.

You can share a report with your access list either by sending it in an e-mail or by distributing a URL for viewing it.

To share a report, use the following procedure:

1. Click **Configure advanced settings...**on the *Create a report* panel.
2. Click **Distribution**.



Report Distribution

3. Enter the sender's e-mail address and SMTP relay server. For example, **E-mail sender address**: j_smith@example.com and **SMTP relay server**: mail.server.com.

   You may require an SMTP relay server for one of several reasons. For example, a firewall may prevent the application from accessing your network's mail server. If you leave the SMTP relay server field blank, the application searches for a suitable mail server for sending reports. If no SMTP server is available, the Security Console does not send the e-mails and will report an error in the log files.

4. Select the check box to send the report to the report owner.
5. Select the check box to send the report to users on a report access list.
6. Select the method to send the report as: **URL**, **File**, or **Zip Archive**.
7. (*Optional*) Select the check box to send the report to users that are not part of an access list.



Additional Report Recipients

8. (*Optional*) Select the check box to send the report to all users with access to assets in the report.

   Adding a user to a report access list potentially means that individuals will be able to view asset data to which they would otherwise not have access.

9. Enter the recipient's e-mail addresses in the **Other recipients** field.

   Note: You cannot distribute a URL to users who are not on the report access list.

10. Select the method to send the report as: **File** or **Zip Archive**.
11. Click **Run the report** when you have finished configuring the report, including the settings for sharing it.

Creating a report access list and configuring report-sharing settings with the API

Note: This topic identifies the API elements that are relevant to creating report access lists and configuring report sharing. For specific instructions on using API v1.1 and Extended API v1.2, see the API guide, which you can download from the *Support* page in Help.

The elements for creating an access list are part of the ReportSave API, which is part of the API v1.1:

- With the `Users` sub-element of `ReportConfig`, you can specify the IDs of the users whom you want add to the report access list.

  Enter the addresses of e-mail recipients, one per line.

- With the `Delivery` sub-element of `ReportConfig`, you can use the `sendToAclAs` attribute to specify how to distribute reports to your selected users.

  Possible values include `file`, `zip`, or `url`.

To create a report access list:

Note: To obtain a list of users and their IDs, use the MultiTenantUserListing API, which is part of the Extended API v1.2.

1. Log on to the application.

   For general information on accessing the API and a sample LoginRequest, see the section API overview in the API guide, which you can download from the *Support* page in Help.

2. Specify the user IDs you want to add to the report access list and the manner of report distribution using the ReportSave API, as in the following XML example:

```
<ReportSaveRequest generate-now="1" sync-id="String"
session-id="48D86A19D786361DE4B862C69EE0768BCC69396B">
     <ReportConfig name="r6" timezone="" owner="15" template-id="baseline-comparison" id="11"
format="pdf">
            <description>
                    <a href="String"> <p>text</p> </a>
            </description>
            <Filters>
                        <filter id="1" type="site">
                        </filter>
            </Filters>
            <Users>
               <user id="16"/>
               <user id="17"/>
            </Users>
            <Baseline compareTo=""/>
            <Delivery>
                        <Storage storeOnServer="1">
                        </Storage>
```

3. If you have no other tasks to perform, log off.

For a LogoutRequest example, see the *API guide*.

For additional, detailed information about the ReportSave API, see the *API guide*.

Restricting report sections

Every report is based on a template, whether it is one of the preset templates that ship with the product or a customized template created by a user in your organization. A template consists of one or more sections. Each section contains a subset of information, allowing you to look at scan data in a specific way.

Security policies in your organization may make it necessary to control which users can view certain report sections, or which users can create reports with certain sections. For example, if your company is an Approved Scanning Vendor (ASV), you may only want a designated group of users to be able to create reports with sections that capture Payment Card Industry (PCI)-related scan data. You can find out which sections in a report are restricted by using the API (see the section *SiloProfileConfig* in the *API guide*.)

Restricting report sections involves two procedures:

- setting the restriction in the API

  Note: Only a Global Administrator can perform these procedures.

- granting users access to restricted sections

Setting the restriction for a report section in the API

The sub-element RestrictedReportSections is part of the SiloProfileCreate API for new silos and SiloProfileUpdate API for existing silos. It contains the sub-element RestrictedReportSection for which the value string is the name of the report section that you want to restrict.

In the following example, the Baseline Comparison report section will become restricted.

1. Log on to the application.

   For general information on accessing the API and a sample LoginRequest, see the section API overview in the *API v1.1 guide*, which you can download from the *Support* page in Help.

2. Identify the report section you want to restrict. This XML example of SiloProfileUpdateRequest includes the RestrictedReportSections element.

```
<SiloProfileUpdateRequest session-id="E6B508C469F4EE1988985C49BE36D1CD0FACAEE6"
sync-id="SILO-PROFILE-CREATE-0001-004">
    <SiloProfileConfig all-global-report-templates="1" all-global-engines="1"
all-global-scan-templates="1" all-licensed-modules="1" description="silo profile description"
id="myprofile-10" name="My SiloProfile Name 10">
       <RestrictedReportSections>
           <RestrictedReportSection name="BaselineComparison"/>
       </RestrictedReportSections>
```

3. If you have no other tasks to perform, log off.

Note: To verify restricted report sections, use the SiloProfileConfig API. See the *API guide*.

For a LogoutRequest example, see the *API guide*.

The Baseline Comparison section is now restricted. This has the following implications for users who have permission to generate reports with restricted sections:

- They can see Baseline Comparison as one of the sections they can include when creating custom report templates.
- They can generate reports that include the Baseline Comparison section.

The restriction has the following implications for users who *do not* have permission to generate reports with restricted sections:

- These users will not see Baseline Comparison as one of the sections they can include when creating custom report templates.
- If these users attempt to generate reports that include the Baseline Comparison section, they will see an error message indicating that they do not have permission to do so.

For additional, detailed information about the SiloProfile API, see *API guide*.

Permitting users to generate restricted reports

Global Administrators automatically have permission to generate restricted reports. They can also assign this permission to others users.

To assign the permission to a new user:

1. Go to the *Administration* page, and click the **Create** link next to *Users*.

   (*Optional*) Go to the *Users* page and click **New user**.

2. Configure the new user's account settings as desired.
3. Click **Roles** in the *User Configuration* panel.

   The console displays the *Roles* page.

4. Select the **Custom** role from the drop-down list.
5. Select the check box labeled **Generate Restricted Reports**.
6. Select any other permissions as desired.
7. Click **Save** when you have finished configuring the account settings.

Note: You also can grant this permission by making the user a Global Administrator.

Assigning the permission to an existing user involves the following steps.

1. Go to the *Administration* page, and click the **manage** link next to *Users*.

   OR

2. (Optional) Go to the *Users* page and click the **Edit** icon for one of the listed accounts.
3. Click the **Roles** link in the *User Configuration* panel.

   The console displays the *Roles* page.
4. Select the **Custom** role from the drop-down list.
5. Select the check box labeled **Generate Restricted Reports**.
6. Select any other permissions as desired.
7. Click **Save** when you have finished configuring the account settings.

Exporting scan data to external databases

If you selected *Database Export* as your report format, the *Report Configuration–Output* page contains fields specifically for transferring scan data to a database.

Before you type information in these fields, you must set up a JDBC-compliant database. In Oracle, MySQL, or Microsoft SQL Server, create a new database called `nexpose` with administrative rights.

1. Go to the *Database Configuration* section that appears when you select the **Database Export** template on the *Create a Report* panel.
2. Enter the IP address and port of the database server.
3. Enter the IP address of the database server.
4. Enter a server port if you want to specify one other than the default.
5. Enter a name for the database.
6. Enter the administrative user ID and password for logging on to that database.
7. Check the database to make sure that the scan data has populated the tables after the application completes a scan.

Configuring data warehousing settings

Note: Currently, this warehousing feature only supports PostgreSQL databases.

You can configure warehousing settings to store scan data or to export it to a PostgreSQL database. You can use this feature to obtain a richer set of scan data for integration with your own internal reporting systems.

Note: Due to the amount of data that can be exported, the warehousing process may take a long time to complete.

This is a technology preview of a feature that is undergoing expansion.

To configure data warehouse settings:

1. Click **manage** next to *Data Warehousing* on the *Administration* page.
2. Enter database server settings on the **Database** page.
3. Go to the *Schedule* page, and select the check box to enable data export.

   You can also disable this feature at any time.
4. Select a date and time to start automatic exports.
5. Select an interval to repeat exports.
6. Click **Save.**

For ASVs: Consolidating three report templates into one custom template

If you are an approved scan vendor (ASV), you must use the following PCI-mandated report templates for PCI scans as of September 1, 2010:

- Attestation of Compliance
- PCI Executive Summary
- Vulnerability Details

You may find it useful and convenient to combine multiple reports into one template. For example you can create a template that combines sections from the Executive Summary, Vulnerability Details, and Host Details templates into one report that you can present to the customer for the initial review. Afterward, when the post-scan phase is completed, you can create another template that includes the PCI Attestation of Compliance with the other two templates for final delivery of the complete report set.

Note: PCI Attestation of Scan Compliance is one self-contained section.

PCI Executive Summary includes the following sections:

- Cover Page
- Payment Card Industry (PCI) Scan Information
- Payment Card Industry (PCI) Component Compliance Summary
- Payment Card Industry (PCI) Vulnerabilities Noted
- Payment Card Industry (PCI) Special Notes

PCI Vulnerability Details includes the following sections:

- Cover Page
- Table of Contents
- Payment Card Industry (PCI) Scan Information
- Payment Card Industry (PCI) Vulnerability Details

PCI Host Detail contains the following sections:

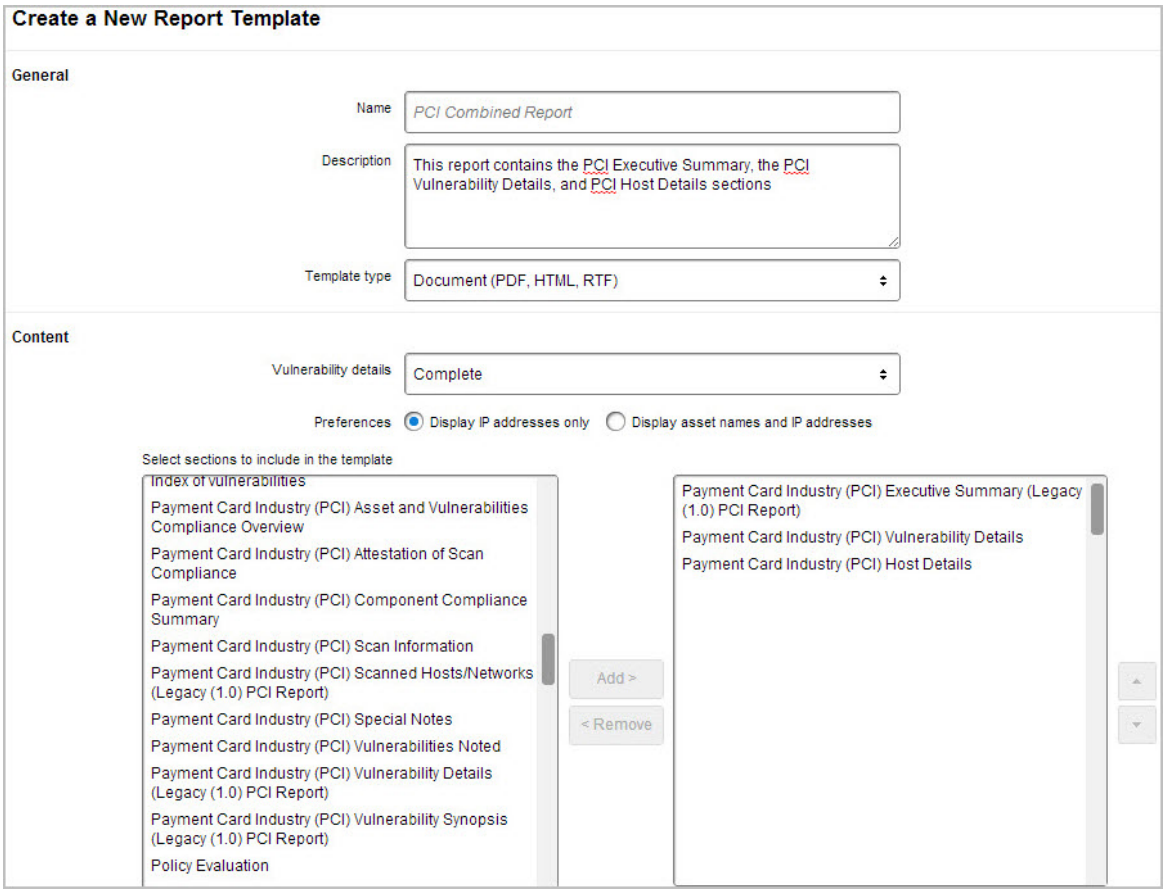
- Table of Contents
- Payment Card Industry (PCI) Scan Information
- Payment Card Industry (PCI) Host Details

To consolidate reports into one custom template:

Note: Due to PCI Council restrictions, section numbers of PCI reports are static and cannot change to reflect the section structure of a customized report. Therefore, a customized report that mixes PCI report sections with non-PCI report sections may have section numbers that appear out of sequence.

1. Select the **Manage report templates** tab on the *Reports* page.
2. Click **New** to create a new report template.

   The console displays the *Create a New Report Template* panel.



Consolidated report template for ASVs.

3. Enter a name and description for your custom report on the *View Reports* page.

   The report name is unique.

4. Select the document template type from the drop-down list.

5. Select a level of vulnerability detail to be included in the report from the drop-down list.

6. Specify if you want to display **IP addresses** or **asset names and IP addresses** on the template.

7. Locate the PCI report sections and click **Add>**.

Note: Do not use sections related to “legacy” reports. These are deprecated and no longer sanctioned by PCI as of September 1, 2010.

8. Click **Save**.

The Security Console displays the *Manage report templates* page with the new report template.

Note: If you use sections from PCI Executive Summary or PCI Attestation of Compliance templates, you will only be able to use the RTF format. If you attempt to select a different format, an error message is displayed.

Configuring custom report templates

The application includes a variety of built-in templates for creating reports. These templates organize and emphasize asset and vulnerability data in different ways to provide multiple looks at the state of your environment's security. Each template includes a specific set of information sections.

If you are new to the application, you will find built-in templates especially convenient for creating reports. To learn about built-in report templates and the information they include, see *Report templates and sections* on page 689.

As you become more experienced with the application and want to tailor reports to your unique informational needs, you may find it useful to create or upload custom report templates.

Fine-tuning information with custom report templates

Creating custom report templates enables you to include as much, or as little, scan information in your reports as your needs dictate. For example, if you want a report that lists assets organized by risk level, a custom report might be the best solution. This template would include only the Discovered System Information section. Or, if you want a report that only lists vulnerabilities, you may create a document template with the Discovered Vulnerabilities section or create a data export template with vulnerability-related attributes.

You can also upload a custom report template that has been created by Rapid7at your request to suit your specific needs. For example, custom report templates can be designed to provide high-level information presented in a dashboard format with charts for quick reference that include asset or vulnerability information that can be tailored to your requirements.Contact your account representative for information about having custom report templates designed for your needs. Templates that have been created for you will be provided to you. Otherwise, you can download additional report templates in the Rapid7Community Web site at *https://community.rapid7.com/* .

After you create or upload a custom report template, it appears in the list of available templates on the *Template* section of the *Create a report* panel. See *Working with externally created report templates* on page 549.

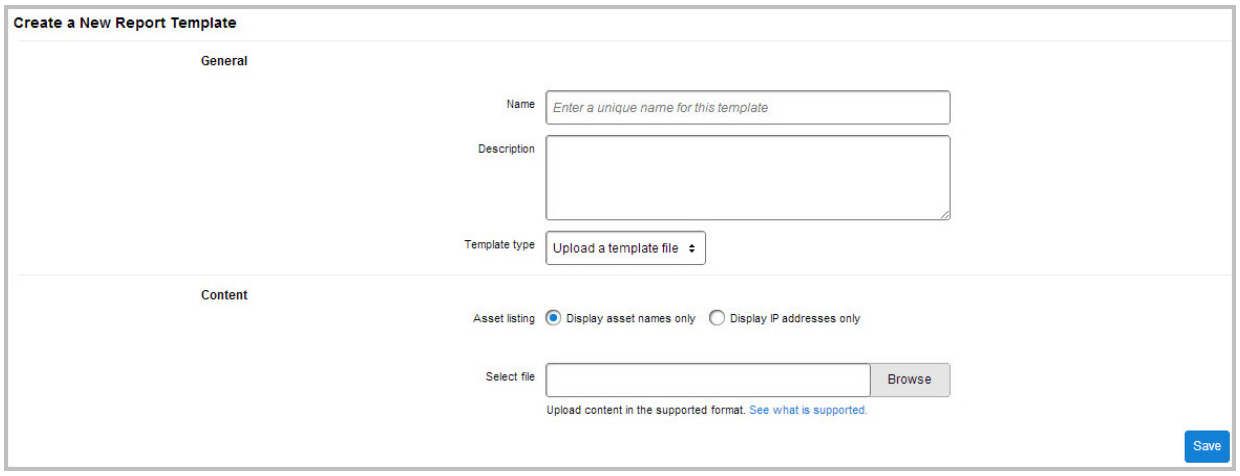
You must have permission to create a custom report template. To find out if you do, consult your Global Administrator. To create a custom report template, take the following steps:

1. Click the **Reports** tab in the Web interface.
2. Click *Manage report templates.*

   The *Manage report templates* panel appears.

3. Click **New**.

   The Security Console displays the *Create a New Report Template* panel.



The Create a New Report Template panel

Editing report template settings

1. Enter a name and description for the new template on the *General* section of the *Create a New Report Template* panel.

   Tip: If you are a Global Administrator, you can find out if your license enables a specific feature. Click the **Administration** tab and then the **Manage** link for the Security Console. In the *Security Console Configuration* panel, click the **Licensing** link.

2. Select the template type from the **Template type** drop-down list:
   - With a *Document* template you will generate section-based, human-readable reports that contain asset and vulnerability information. Some of the formats available for this template type—Text, PDF, RTF, and HTML—are convenient for sharing information to be read by stakeholders in your organization, such as executives or security team members tasked with performing remediation.
   - With an *export* template, the format is identified in the template name, either comma-separated-value (CSV) or XML files. CSV format is useful for integrating check results into spreadsheets, that you can share with stakeholders in your organization. Because the output is CSV, you can further manipulate the data using pivot tables or other spreadsheet features. See *Using Excel pivot tables to create custom reports from a CSV file* on page 554. To use this template type, you must have the *Customizable CSV export* featured enabled. If it is not, contact your account representative for license options.
   - With the *Upload a template file* option you can select a template file from a library. You will select the file to upload in the *Content* section of the *Create a New Report Template* panel. See *Working with externally created report templates* on page 549.

   Note: The **Vulnerability details** setting only affects document report templates. It does not affect data export templates.

3. Select a level of vulnerability details from the drop-down list in the *Content* section of the *Create a New Report Template* panel.

   Vulnerability details filter the amount of information included in document report templates:

   - *None* excludes all vulnerability-related data.
   - *Minimal (title and risk metrics)* excludes vulnerability solutions.
   - *Complete except for solutions* includes basic information about vulnerabilities, such as title, severity level, CVSS score, and date published.
   - *Complete* includes all vulnerability-related data.

4. Select your display preference:
   - *Display asset names only*
   - *Display asset names and IP addresses*

5. Select the sections to include in your template and click **Add>**. See *Report templates and sections* on page 689.

   Set the order for the sections to appear by clicking the up or down arrows.

6. (*Optional*)Click **<Remove** to take sections out of the report.

7. (*Optional*) Add the *Cover Page* section to include a cover page, logo, scan date, report date, and headers and footers. See *Adding a custom logo to your report* on page 547 for information on file formats and directory location for adding a custom logo.

8. (*Optional*) Clear the check boxes to *Include scan data* and *Include report date* if you do not want the information in your report.

9. (*Optional*) Add the *Baseline Comparison* section to select the scan date to use as a baseline. See *Selecting a scan as a baseline* on page 376 for information about designating a scan as a baseline.

10. (*Optional*) Add the *Executive Summary* section to enter an introduction to begin the report.

11. Click **Save**.

Creating a custom report template based on an existing template

You can create a new custom report template based on any built-in or existing custom report template. This allows you to take advantage of some of a template's useful features without having to recreate them as you tailor a template to your needs.

To create a custom template based on an existing template, take the following steps:

1. Click the **Reports** tab in the Web interface.

2. Click **Manage report templates.**

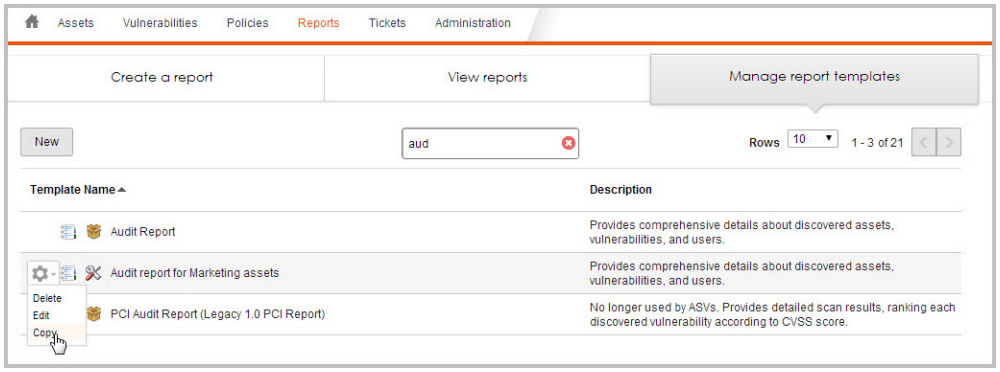
   The *Manage report templates* panel appears.

3. From the table, select a template that you want to base a new template on.

   OR

   If you have a large number of templates and don't want to scroll through all of them, start typing the name of a template in the *Find a report template* text box. The Security Console displays any matches. The search is not case-sensitive.

4. Hover over the tool icon of the desired template. If it is a built-in template, you will have the option to copy and then edit it. If it is a custom template, you can edit it directly unless you prefer to edit a copy. Select an option.



Selecting a report template to edit

   The Security Console displays the **Create a New Report Template** panel.

5. Edit settings as described in *Editing report template settings* on page 544. If you are editing a copy of a template, give the template a new name.

6. Click **Save**.

   The new template appears in the template table.

Adding a custom logo to your report

By default, a document report cover page includes a generic title, the name of the report, the date of the scan that provided the data for the report, and the date that the report was generated. It also may include the Rapid7 logo or no logo at all, depending on the report template. See *Cover Page* on page 706. You can easily customize a cover page to include your own title and logo.

Note: Logos can be JPEG and PNG logo formats.

To display your own logo on the cover page:

1. Copy the logo file to the designated directory of your installation.

   - In Windows: C:\Program Files\[installation_directory]\shared\reportImages\custom\silo\default.
     - In Windows: C:\Program Files\[installation_directory]\shared\reportImages\custom\silo\default.

2. Go to the *Cover Page Settings* section of the *Create a New Report Template* panel.
3. Enter the name of the file for your own logo, preceded by the word “image:” in the **Add logo** field.

   Example: image:file_name.png. Do not insert a space between the word “image:” and the file name.

4. Enter a title in the **Add title** field.
5. Click **Save**.
6. Restart the Security Console. *Make sure to restart before you attempt to create a report with the custom logo.*

Working with externally created report templates

The application provides built-in report templates and the ability to create custom templates based on those built-in templates. Beyond these options, you may want to use compatible templates that have been created outside of the application for your specific business needs. These templates may have been provided directly to your organization or they may have been posted in the Rapid7 Community at https://community.rapid7.com/community/nexpose/report-templates.

See *Fine-tuning information with custom report templates* on page 543 for information about requesting custom report templates.

Making one of these externally created templates available in the Security Console involves two actions:

1. downloading the template to the workstation that you use to access the Security Console
2. uploading the template to the Security Console using the *Reports* configuration panel

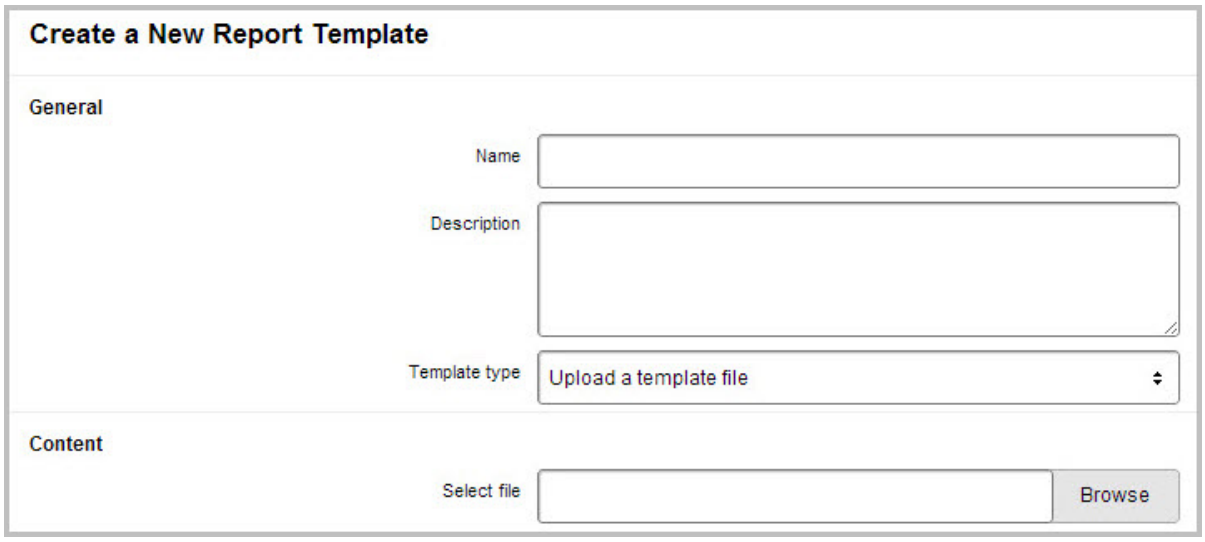
Note: Your license must enable custom reporting for the template upload option to be available. Also, externally created custom template files must be approved by Rapid7 and archived in the .JAR format.

After you have downloaded a template archive, take the following steps:

1. Click the **Reports** tab in the Security Console Web interface.
2. Click *Manage report templates.*

   The *Manage report templates* panel appears.
3. Click **New**.

   The Security Console displays the *Create a New Report Template* panel.
4. Enter a name and description for the new template on the *General* section of the *Create a New Report Template* panel.
5. Select *Upload a template file* from the **Template type** drop-down list.



Upload a report template file

6. Click **Browse** in the **Select file** field to display a directory for you to search for custom templates.
7. Select the report template file and click **Open**.

   The report template file appears in the *Select file* field in the *Content* section.

   Note: Contact Technical Support if you see errors during the upload process.
8. Click **Save**.

   The custom report template file will now appear in the list of available report templates on the *Manage report templates* panel.

Working with report formats

The choice of a format is important in report creation. Formats not only affect how reports appear and are consumed, but they also can have some influence on what information appears in reports.

Working with human-readable formats

Several formats make report data easy to distribute, open, and read immediately:

- *PDF* can be opened and viewed in Adobe Reader.
- *HTML* can be opened and viewed in a Web browser.
- *RTF* can be opened, viewed, and edited in Microsoft Word. This format is preferable if you need to edit or annotate the report.
- *Text* can be opened, viewed, and edited in any text editing program.

Note: If you wish to generate PDF reports with Asian-language characters, make sure that UTF-8 fonts are properly installed on your host computer. PDF reports with UTF-8 fonts tend to be slightly larger in file size.

If you are using one of the three report templates mandated for PCI scans as of September 1, 2010 *(Attestation of Compliance, PCI Executive Summary, or Vulnerability Details)*, or a custom template made with sections from these templates, you can only use the RTF format. These three templates require ASVs to fill in certain sections manually.

Working with XML formats

Tip: For information about XML export attributes, see *Export template attributes* on page 712. That section describes similar attributes in the CSV export template, some of which have slightly different names.

Various XML formats make it possible to integrate reports with third-party systems.

- *Asset Report Format (ARF)* provides asset information based on connection type, host name, and IP address. This template is required for submitting reports of policy scan results to the U.S. government for SCAP certification.
- *XML Export*, also known as "raw XML," contains a comprehensive set of scan data with minimal structure. Its contents must be parsed so that other systems can use its information.
- *XML Export 2.0* is similar to *XML Export*, but contains additional attributes:

Asset Risk	Exploit Title	Site Name
Exploit IDs	Malware Kit Name(s)	Site Importance
Exploit Skill Needed	PCI Compliance Status	Vulnerability Risk
Exploit Source Link	Scan ID	Vulnerability Since
Exploit Type	Scan Template	

- *Nexpose* TM *Simple XML is also a "raw XML" format. It is ideal for integration of scan data with the Metasploit vulnerability exploit framework. It contains a subset of the data available in the XML Export format:*
  - hosts scanned
  - vulnerabilities found on those hosts
  - services scanned
  - vulnerabilities found in those services
- *SCAP Compatible XML* is also a "raw XML" format that includes Common Platform Enumeration (CPE) names for fingerprinted platforms. This format supports compliance with Security Content Automation Protocol (SCAP) criteria for an Unauthenticated Scanner product.
- *XML* arranges data in clearly organized, human-readable XML and is ideal for exporting to other document formats.
- *XCCDF Results XML Report* provides information about compliance tests for individual USGCB or FDCC configuration policy rules. Each report is dedicated to one rule. The XML output includes details about the rule itself followed by data about the scan results. If any results were overridden, the output identifies the most recent override as of the time the report was run. See *Overriding rule test results*.
- *XCCDF Results XML Report* provides information about compliance tests for individual USGCB or FDCC configuration policy rules. Each report is dedicated to one rule. The XML output includes details about the rule itself followed by data about the scan results. If any results were overridden, the output identifies the most recent override as of the time the report was run. See *Overriding rule test results*.
- *CyberScope XML Export* organizes scan data for submission to the CyberScope application. Certain entities are required by the U.S. Office of Management and Budget to submit CyberScope-formatted data as part of a monthly program of reporting threats.
- *Qualys* XML Export* is intended for integration with the Qualys reporting framework.

  ** Qualys is a trademark of Qualys, Inc.*

XML Export 2.0 contains the most information. In fact, it contains all the information captured during a scan. Its schema can be downloaded from the *Support* page in Help. Use it to help you understand how the data is organized and how you can customize it for your own needs.

Working with CSV export

You can open a *CSV* (comma separated value) report in Microsoft Excel. It is a powerful and versatile format. Not only does it contain a significantly greater amount of scan information than is available in report templates, but you can easily use macros and other Excel tools to manipulate this data and provide multiple views of it. Two CSV formats are available:

- *CSV Export* includes comprehensive scan data
- *XCCDF Human Readable CSV Report* provides test results on individual assets for compliance with individual USGCB or FDCC configuration policy rules. If any results were overridden, the output lists results based on the most recent overrides as of the time the output was generated. However, the output does not identify overrides as such or include the override history. See *Overriding rule test results* on page 303.

The CSV Export format works only with the Basic Vulnerability Check Results template and any *Data*-type custom templates. See *Fine-tuning information with custom report templates* on page 543.

Using Excel pivot tables to create custom reports from a CSV file

The pivot table feature in Microsoft Excel allows you to process report data in many different ways, essentially creating multiple reports one exported CSV file. Following are instructions for using pivot tables. These instructions reflect Excel 2007. Other versions of Excel provide similar workflows.

If you have Microsoft Excel installed on the computer with which you are connecting to the Security Console, click the link for the CSV file on the *Reports* page. This will start Microsoft Excel and open the file. If you do not have Excel installed on the computer with which you are connecting to the console, download the CSV file from the *Reports* page, and transfer it to a computer that has Excel installed. Then, use the following procedure.

To create a custom report from a CSV file:

1. Start the process for creating a pivot table.
2. Select all the data.
3. Click the **Insert** tab, and then select the **PivotTable** icon.

   The *Create Pivot Table* dialog box, appears.
4. Click **OK** to accept the default settings.

   Excel opens a new, blank sheet. To the right of this sheet is a bar with the title *PivotTable Field List*, which you will use to create reports. In the top pane of this bar is a list of fields that you can add to a report. Most of these fields re self-explanatory.

   The **result-code** field provides the results of vulnerability checks. See *How vulnerability exceptions appear in XML and CSV formats* on page 558 for a list of result codes and their descriptions.

   The **severity** field provides numeric severity ratings. The application assigns each vulnerability a severity level, which is listed in the Severity column. The three severity levels—Critical, Severe, and Moderate—reflect how much risk a given vulnerability poses to your network security. The application uses various factors to rate severity, including CVSS scores, vulnerability age and prevalence, and whether exploits are available.

   Note: The severity field is not related to the severity score in PCI reports.

   - 8 to 10 = Critical
   - 4 to 7 = Severe
   - 1 to 3 = Moderate

The next steps involve choosing fields for the type of report that you want to create, as in the three following examples.

Example 1: Creating a report that lists the five most numerous exploited vulnerabilities

1. Drag **result-code** to the *Report Filter* pane.
2. Click drop-down arrow in column B to display result codes that you can include in the report.
3. Select the option for multiple items.
4. Select *ve* for exploited vulnerabilities.
5. Click **OK**.
6. Drag **vuln-id** to the *Row Labels* pane.

   Row labels appear in column A.
7. Drag **vuln-id** to the *Values* pane.

   A count of vulnerability IDs appears in column B.
8. Click the drop-down arrow in column A to change the number of listed vulnerabilities to five.
9. Select Value Filters, and then Top 10...
10. Enter 5 in the Top 10 Filter dialog box and click **OK**.

The resulting report lists the five most numerous exploited vulnerabilities.

Example 2: Creating a report that lists required Microsoft hot-fixes for each asset

1. Drag result-code to the *Report Filter* pane.
2. Click the drop-down arrow in column B of the sheet it to display result codes that you can include in the report.
3. Select the option for multiple items.
4. Select *ve* for exploited vulnerabilities and *vv* for vulnerable versions.
5. Click **OK**.
6. Drag **host** to the *Row Labels* pane.
7. Drag **vuln-id** to the *Row Labels p*ane.
8. Click **vuln-id** once in the pane for choosing fields in the *PivotTable Field List* bar.
9. Click the drop-down arrow that appears next to it and select **Label Filters**.
10. Select **Contains...** in the *Label Filter* dialog box.
11. Enter the value windows-hotfix.
12. Click **OK**.

The resulting report lists required Microsoft hot-fixes for each asset.

Example 3: Creating a report that lists the most critical vulnerabilities and the systems that are at risk

1. Drag **result-code** to the *Report Filter* pane.
2. Click the drop-down arrow that appears in column B to display result codes that you can include in the report.
3. Select the option for multiple items.
4. Select *ve* for exploited vulnerabilities.
5. Click **OK**.
6. Drag **severity** to the *Report Filter* pane.

Another of the sheet.

7. Click the drop-down arrow appears that column B to display ratings that you can include in the report.
8. Select the option for multiple items.
9. Select **8**, **9**, and **10**, for critical vulnerabilities.
10. Click **OK**.
11. Drag **vuln-titles** to the *Row Labels* pane.
12. Drag **vuln-titles** to the *Values* pane.
13. Click the drop-down arrow that appears in column A and select **Value Filters.**
14. Select **Top 10...** in the *Top 10 Filter* dialog box, confirm that the value is 10.
15. Click **OK**.
16. Drag **host** to the *Column Labels* pane.
17. Another of the sheet.
18. Click the drop-down arrow appears in column B and select **Label Filters**.
19. Select **Greater Than...** in the Label Filter dialog box, enter a value of 1.
20. Click **OK**.

The resulting report lists the most critical vulnerabilities and the assets that are at risk.

How vulnerability exceptions appear in XML and CSV formats

Vulnerability exceptions can be important for the prioritization of remediation projects and for compliance audits. Report templates include a section dedicated to exceptions. See *Vulnerability Exceptions* on page 711. In XML and CSV reports, exception information is also available.

XML: The vulnerability test status attribute will be set to one of the following values for vulnerabilities suppressed due to an exception:

```
exception-vulnerable-exploited - Exception suppressed exploited
vulnerability
```

`exception-vulnerable-version - Exception suppressed version-checked vulnerability`

`exception-vulnerable-potential - Exception suppressed potential vulnerability`

CSV: The vulnerability result-code column will be set to one of the following values for vulnerabilities suppressed due to an exception.

Vulnerability result codes

Each code corresponds to results of a vulnerability check:

- *ds* (skipped, disabled): A check was not performed because it was disabled in the scan template.
- *ee* (excluded, exploited): A check for an exploitable vulnerability was excluded.
- *ep* (excluded, potential): A check for a potential vulnerability was excluded.
- er (error during check): An error occurred during the vulnerability check.
- *ev* (excluded, version check): A check was excluded. It is for a vulnerability that can be identified because the version of the scanned service or application is associated with known vulnerabilities.
- *nt* (no tests): There were no checks to perform.
- *nv* (not vulnerable): The check was negative.
- *ov* (overridden, version check): A check for a vulnerability that would ordinarily be positive because the version of the target service or application is associated with known vulnerabilities was negative due to information from other checks.
- *sd* (skipped because of DoS settings): sd (skipped because of DOS settings)—If unsafe checks were not enabled in the scan template, the application skipped the check because of the risk of causing denial of service (DOS). See *Configuration steps for vulnerability check settings* on page 603.
- *sv* (skipped because of inapplicable version): the application did not perform a check because the version of the scanned item is not included in the list of checks.
- *uk* (unknown): An internal issue prevented the application from reporting a scan result.
- *ve* (vulnerable, exploited): The check was positive as indicated by asset-specific vulnerability tests. Vulnerabilities with this result appear in the CSV report if the *Vulnerabilities found* result type was selected in the report configuration. See *Filtering report scope with vulnerabilities* on page 365.
- *vp* (vulnerable, potential): The check for a potential vulnerability was positive.

- *vv* (vulnerable, version check): The check was positive. The version of the scanned service or software is associated with known vulnerabilities.

Working with the database export format

You can output the *Database Export* report format to Oracle, MySQL, and Microsoft SQL Server.

Like CSV and the XML formats, the Database Export format is fairly comprehensive in terms of the data it contains. It is not possible to configure what information is included in, or excluded from, the database export. Consider CSV or one of the XML formats as alternatives.

Nexpose provides a schema to help you understand what data is included in the report and how the data is arranged, which is helpful in helping you understand how to you can work with the data. You can request the database export schema from Technical Support.

Understanding report content

Reports contain a great deal of information. It's important to study them carefully for better understanding, so that they can help you make more informed security-related decisions.

The data in a report is a static snapshot in time. The data displayed in the Web interface changes with every scan. Variance between the two, such as in the number of discovered assets or vulnerabilities, is most likely attributable to changes in your environment since the last report.

For stakeholders in your organization who need fresh data but don't have access to the Web interface, run reports more frequently. Or use the report scheduling feature to automatically synchronize report schedules with scan schedules.

In environments that are constantly changing, Baseline Comparison reports an be very useful.

If your report data turns out to be much different from what you expected, consider several factors that may have skewed the data.

Scan settings can affect report data

Scan settings affect report data in several ways:

- Lack of credentials: If certain information is missing from a report, such as discovered files, spidered Web sites, or policy evaluations, check to see if the scan was configured with proper logon information. The application cannot perform many checks without being able to log onto target systems as a normal user would.
- Policy checks not enabled: Another reason that policy settings may not appear in a report is that policy checks were not enabled in the scan template.
- Discovery-only templates: If no vulnerability data appears in a report, check to see if the scan was preformed with a discovery-only scan template, which does not check for vulnerabilities.
- Certain vulnerability checks enabled or disabled: If your report shows vulnerabilities than you expected, check the scan template to see which checks have been enabled or disabled.
- Unsafe checks not enabled: If a report shows indicates that a check was skipped because of Denial of Service (DOS) settings, as with the *sd* result code in CSV reports, then unsafe checks were not enabled in the scan template.
- Manual scans: A manual scan performed under unusual conditions for a site can affect reports. For example, an automatically scheduled report that only includes recent scan data is related to a specific, multiple-asset site that has automatically scheduled scans. A user runs a manual scan of a single asset to verify a patch update. The report may include that scan data, showing only one asset, because it is from the most recent scan.

Different report formats can influence report data

If you are disseminating reports using multiple formats, keep in mind that different formats affect not only *how* data is presented, but *what* data is presented. The human-readable formats, such as PDF and HTML, are intended to display data that is organized by the document report templates. These templates are more “selective” about data to include. On the other hand, XML Export, XML Export 2.0, CSV, and export templates essentially include all possible data from scans.

Understanding how vulnerabilities are characterized according to certainty

Remediating confirmed vulnerabilities is a high security priority, so it's important to look for confirmed vulnerabilities in reports. However, don't get thrown off by listings of potential or unconfirmed vulnerabilities. And don't dismiss these as false positives.

The application will flag a vulnerability if it discovers certain conditions that make it probable that the vulnerability exists. If, for any reason, it cannot absolutely verify that the vulnerability is there, it will list the vulnerability as potential or unconfirmed. Or it may indicate that the *version* of the scanned operating system or application is vulnerable.

The fact that a vulnerability is a "potential" vulnerability or otherwise not officially confirmed does not diminish the probability that it exists or that some related security issue requires your attention. You can confirm a vulnerability by running an exploit if one is available. See *Working with vulnerabilities* on page 265. You also can examine the scan log for the certainty with which a potentially vulnerable item was fingerprinted. A high level of fingerprinting certainty may indicate a greater likelihood of vulnerability.

How to find out the certainty characteristics of a vulnerability

You can find out the certainty level of a reported vulnerability in different areas:

- The PCI Audit report includes a table that lists the status of each vulnerability. Status refers to the certainty characteristic, such as Exploited, Potential, or Vulnerable Version.
- The Report Card report includes a similar status column in one of its tables, which also lists information about the test that the application performed for each vulnerability on each asset.
- The XML Export and XML Export 2.0 reports include an attribute called test status, which includes certainty characteristics, such as vulnerable-exploited, and not-vulnerable.
- The CSV report includes result codes related to certainty characteristics.
- If you have access to the Web interface, you can view the certainty characteristics of a vulnerability on the page that lists details about the vulnerability.

Note that the Discovered and Potential Vulnerabilities section, which appears in the Audit report, potential and confirmed vulnerabilities are not differentiated.

Looking beyond vulnerabilities

When reviewing reports, look beyond vulnerabilities for other signs that may put your network at risk. For example, the application may discover a telnet service and list it in a report. A telnet service is not a vulnerability. However, telnet is an unencrypted protocol. If a server on your network is using this protocol to exchange information with a remote computer, it's easy for an uninvited party to monitor the transmission. You may want to consider using SSH instead.

In another example, it may discover a Cisco device that permits Web requests to go to an HTTP server, instead of redirecting them to an HTTPS server. Again, this is not technically a vulnerability, but this practice may be exposing sensitive data.

Study reports to help you manage risk proactively.

Using report data to prioritize remediation

A long list of vulnerabilities in a report can be a daunting sight, and you may wonder which problem to tackle first. The vulnerability database contains checks for over 12,000 vulnerabilities, and your scans may reveal more vulnerabilities than you have time to correct.

One effective way to prioritize vulnerabilities is to note which have real exploits associated with them. A vulnerability with known exploits poses a very concrete risk to your network. The Exploit ExposureTM feature flags vulnerabilities that have known exploits and provides exploit information links to Metasploit modules and the Exploit Database. It also uses the exploit ranking data from the Metasploit team to rank the skill level required for a given exploit. This information appears in vulnerability listings right in the Security Console Web interface, so you can see right away

Since you can’t predict the skill level of an attacker, it is a strongly recommend best practice to immediately remediate any vulnerability that has a live exploit, regardless of the skill level required for an exploit or the number of known exploits.

Report creation settings can affect report data

Report settings can affect report data in various ways:

- Using most recent scan data: If old assets that are no longer in use still appear in your reports, and if this is not desirable, make sure to enable the check box labeled **Use the last scan data only**.
- Report schedule out of sync with scan schedule: If a report is showing no change in the number of vulnerabilities despite the fact that you have performed substantial remediation since the last report was generated, check the report schedule against the scan schedule. Make sure that reports are automatically generated to follow scans if they are intended to show patch verification.
- Assets not included: If a report is not showing expected asset data, check the report configuration to see which sites and assets have been included and omitted.
- Vulnerabilities not included: If a report is not showing an expected vulnerability, check the report configuration to vulnerabilities that have been filtered from the report. On the *Scope* section of the *Create a report* panel, click **Filter report scope based on vulnerabilities** and verify the filters are set appropriately to include the categories and severity level you need.

Prioritize according to risk score

Another way to prioritize vulnerabilities is according to their risk scores. A higher score warrants higher priority.

The application calculates risk scores for every asset and vulnerability that it finds during a scan. The scores indicate the potential danger that the vulnerability poses to network and business security based on impact and likelihood of exploit.

Risk scores are calculated according to different risk strategies. See *Working with risk strategies to analyze threats* on page 652.

Using tickets

You can use the ticketing system to manage the remediation work flow and delegate remediation tasks. Each ticket is associated with an asset and contains information about one or more vulnerabilities discovered during the scanning process.

Viewing tickets

Click the **Tickets** tab to view all active tickets. The console displays the *Tickets* page.

Click a link for a ticket name to view or update the ticket. See the following section for details about editing tickets. From the *Tickets* page, you also can click the link for an asset's address to view information about that asset, and open a new ticket.

Creating and updating tickets

The process of creating a new ticket for an asset starts on the Security Console page that lists details about that asset. You can get to that page by selecting a view option on the *Assets* page and following the sequence of console pages that ends with asset. See *Locating and working with assets* on page 240.

Opening a ticket

When you want to create a ticket for a vulnerability, click the **Open a ticket** button, which appears at the bottom of the *Vulnerability Listings* pane on the detail page for each asset. See *Locating assets by sites* on page 243. The console displays the *General* page of the *Ticket Configuration* panel.

On the *Ticket Configuration-General* page, type name for the new ticket. These names are not unique. They appear in ticket notifications, reports, and the list of tickets on the *Tickets* page.

The status of the ticket appears in the *Ticket State* field. You cannot modify this field in the panel. The state changes as the ticket issue is addressed.

Note: If you need to assign the ticket to a user who does not appear on the drop down list, you must first add that user to the associated asset group.

Assign a priority to the ticket, ranging from *Critical* to *Low,* depending on factors such as the vulnerability level. The priority of a ticket is often associated with external ticketing systems.

Assign the ticket to a user who will be responsible for overseeing the remediation work flow. To do so, select a user name from the drop down list labeled *Assigned To*. Only accounts that have access to the affected asset appear in the list.

You can close the ticket to stop any further remediation action on the related issue. To do so, click the **Close Ticket** button on this page. The console displays a box with a drop down list of reasons for closing the ticket. Options include *Problem fixed*, *Problem not reproducible*, and *Problem not considered an issue (policy reasons)*. Add any other relevant information in the dialog box and click the Save button.

Adding vulnerabilities

Go to the *Ticket Configuration–Vulnerabilities* page.

Click the **Select Vulnerabilities...** button. The console displays a box that lists all reported vulnerabilities for the asset. You can click the link for any vulnerability to view details about it, including remediation guidance.

Select the check boxes for all the vulnerabilities you wish to include in the ticket, and click the **Save** button. The selected vulnerabilities appear on the *Vulnerabilities* page.

Updating ticket history

You can update coworkers on the status of a remediation project, or note impediments, questions, or other issues, by annotating the ticket history. As Nexpose users and administrators add comments related to the work flow, you can track the remediation progress.

1. Go to the *Ticket Configuration–History* page.
2. Click the **Add Comments...** button.

   The console displays a box, where you can type a comment.
3. Click **Save**.

   The console displays all comments on the *History* page.

Tune

As you use the application to gather, view, and share security information, you may want to adjust settings of features that these operations.

Tune provides guidance on adjusting or customizing settings for scans, risk calculation, and configuration assessment.

Working with scan templates and tuning scan performance on page 572: After familiarizing yourself with different built-in scan templates, you may want to customize your own scan templates for maximum speed or accuracy in your network environment. This section provides best practices for scan tuning and guides you through the steps of creating a custom scan template.

Working with risk strategies to analyze threats on page 652: The application provides several strategies for calculating risk. This section explains how each strategy emphasizes certain characteristics, allowing you to analyze risk according to your organization's unique security needs or objectives. It also provides guidance for changing risk strategies and supporting custom strategies.

Creating a custom policy on page 631: You can create custom configuration policies based an USGCB and FDCC policies, allowing you to check your environment for compliance with your organization's unique configuration policies. This section guides you through configuration steps.

Working with scan templates and tuning scan performance

You may want to improve scan performance. You may want to make scans faster or more accurate. Or you may want scans to use fewer network resources. The following section provides best practices for scan tuning and instructions for working with scan templates.

Tuning scans is a sensitive process. If you change one setting to attain a certain performance boost, you may find another aspect of performance diminished. Before you tweak any scan templates, it is important for you to know two things:

- What your goals or priorities for tuning scans?
- What aspects of scan performance are you willing to compromise on?

Identify your goals and how they're related to the performance "triangle." See *Keep the "triangle" in mind when you tune* on page 574. Doing so will help you look at scan template configuration in the more meaningful context of your environment. Make sure to familiarize yourself with scan template elements before changing any settings.

Also, keep in mind that tuning scan performance requires some experimentation, finesse, and familiarity with how the application works. Most importantly, you need to understand your unique network environment.

This introductory section talks about why you would tune scan performance and how different built-in scan templates address different scanning needs:

- *Defining your goals for tuning* on page 573
- *The primary tuning tool: the scan template* on page 578

See also the appendix that compares all of our built-in scan templates and their use cases:

- *Scan templates* on page 684

Familiarizing yourself with built-in templates is helpful for customizing your own templates. You can create a custom template that incorporates many of the desirable settings of a built-in template and just customize a few settings vs. creating a new template from scratch.

To create a custom scan template, go to the following section:

- *Configuring custom scan templates* on page 582

Defining your goals for tuning

Before you tune scan performance, make sure you know why you're doing it. What do you want to change? What do you need it to do better? Do you need scans to run more quickly? Do you need scans to be more accurate? Do you want to reduce resource overhead?

The following sections address these questions in detail.

You need to finish scanning more quickly

Your goal may be to increase overall scan speed, as in the following scenarios:

- Actual scan-time windows are widening and conflicting with your scan blackout periods. Your organization may schedule scans for non-business hours, but scans may still be in progress when employees in your organization need to use workstations, servers, or other network resources.
- A particular type of scan, such as for a site with 300 Windows workstations, is taking an especially long time with no end in sight. This could be a "scan hang" issue rather than simply a slow scan.

  Note: If a scan is taking an extraordinarily long time to finish, terminate the scan and contact Technical Support.
- You need to able to schedule more scans within the same time window.
- Policy or compliance rules have become more stringent for your organization, requiring you to perform "deeper" authenticated scans, but you don't have additional time to do this.
- You have to scan more assets in the same amount of time.
- You have to scan the same number of assets in less time.
- You have to scan *more* assets in *less* time.

You need to reduce consumption of network or system resources

Your goal may be to lower the hit on resources, as in the following scenarios:

- Your scans are taking up too much bandwidth and interfering with network performance for other important business processes.
- The computers that host your Scan Engines are maxing out their memory if they scan a certain number of ports.
- The security console runs out of memory if you perform too many simultaneous scans.

You need more accurate scan data

Scans may not be giving you enough information, as in the following scenarios:

- Scans are missing assets.
- Scans are missing services.
- The application is reporting too many false positives or false negatives.
- Vulnerability checks are not occurring at a sufficient depth.

Keep the “triangle” in mind when you tune

Any tuning adjustment that you make to scan settings will affect one or more main performance categories.

These categories reflect the general goals for tuning discussed in the preceding section:

- accuracy
- resources
- time

These three performance categories are interdependent. It is helpful to visualize them as a triangle.



If you lengthen one side of the triangle—that is, if you favor one performance category—you will shorten at least one of the other two sides. It is unrealistic to expect a tuning adjustment to lengthen all three sides of the triangle. However, you often can lengthen two of the three sides.

Increasing time availability

Providing more time to run scans typically means making scans run faster. One use case is that of a company that holds auctions in various locations around the world. Its asset inventory is slightly over 1,000. This company cannot run scans while auctions are in progress because time-sensitive data must traverse the network at these times without interruptions. The fact that the company holds auctions in various time zones complicates scan scheduling. Scan windows are extremely tight. The company's best solution is to use a lot of bandwidth so that scan can finish as quickly as possible.

In this case it's possible to reduce scan time without sacrificing accuracy. However, a high workload may tap resources to the point that the scanning mechanisms could become unstable. In this case, it may be necessary to reduce the level of accuracy by, for example, turning off credentialed scanning.

There are many various ways to increase scan speeds, including the following:

- Increase the number of assets that are scanned simultaneously. Be aware that this will tax RAM on Scan Engines and the Security Console.
- Allocate more scan threads. Doing so will impact network bandwidth.
- Use a less exhaustive scan template. Again, this will diminish the accuracy of the scan.

- Add Scan Engines, or position them in the network strategically. If you have one hour to scan 200 assets over low bandwidth, placing a Scan Engine on the same side of the firewall as those assets can speed up the process. When deploying a Scan Engine relative to target assets, choose a location that maximizes bandwidth and minimizes latency. For more information on Scan Engine placement, refer to the administrator's guide.

  Note: Deploying additional Scan Engines may lower bandwidth availability.

Increasing accuracy

Making scans more accurate means finding more security-related information.

There are many ways to this, each with its own "cost" according to the performance triangle:

Increase the number of discovered assets, services, or vulnerability checks. This will take more time.

"Deepen" scans with checks for policy compliance and hotfixes. These types of checks require credentials and can take considerably more time.

Scan assets more frequently. For example, peripheral network assets, such as Web servers or Virtual Private Network (VPN) concentrators, are more susceptible to attack because they are exposed to the Internet. It's advisable to scan them often. Doing so will either require more bandwidth or more time. The time issue especially applies to Web sites, which can have deep file structures.

Be aware of license limits when scanning network services. When the application attempts to connect to a service, it appears to that service as another "client," or user. The service may have a defined limit for how many simultaneous client connections it can support. If service has reached that client capacity when the application attempts a connection, the service will reject the attempt. This is often the case with telnet-based services. If the application cannot connect to a service to scan it, that service won't be included in the scan data, which means lower scan accuracy.

Increasing resource availability

Making more resources available primarily means reducing how much bandwidth a scan consumes. It can also involve lowering RAM use, especially on 32-bit operating systems.

Consider bandwidth availability in four major areas of your environment. Any one of or more of these can become bottlenecks:

- The computer that hosts the application can get bogged down processing responses from target assets.
- The network infrastructure that the application runs on, including firewalls and routers, can get bogged down with traffic.
- The network on which target assets run, including firewalls and routers, can get bogged down with traffic.
- The target assets can get bogged down processing requests from the application.

Of particular concern is the network on which target assets run, simply because some portion of total bandwidth is always in use for business purposes. This is especially true if you schedule scans to run during business hours, when workstations are running and laptops are plugged into the network. Bandwidth sharing also can be an issue during off hours, when backup processes are in progress.

Two related bandwidth metrics to keep an eye on are the number of data packets exchanged during the scan, and the correlating firewall states. If the application sends too many packets per second (pps), especially during the service discovery and vulnerability check phases of a scan, it can exceed a firewall's capacity to track connection states. The danger here is that the firewall will start dropping request packets, or the response packets from target assets, resulting in false negatives. So, taxing bandwidth can trigger a drop in accuracy.

There is no formula to determine how much bandwidth should be used. You have to know how much bandwidth your enterprise uses on average, as well as the maximum amount of bandwidth it can handle. You also have to monitor how much bandwidth the application consumes and then adjust the level accordingly.

For example, if your network can handle a maximum of 10,000 pps without service disruptions, and your normal business processes average about 3,000 pps at any given time, your goal is to have the application work within a window of 7,000 pps.

The primary scan template settings for controlling bandwidth are scan threads and maximum simultaneous ports scanned.

The cost of conserving bandwidth typically is time.

For example, a company operates full-service truck stops in one region of the United States. Its security team scans multiple remote locations from a central office. Bandwidth is considerably

low due to the types of network connections. Because the number of assets in each location is lower than 25, adding remote Scan Engines is not a very efficient solution. A viable solution in this situation is to reduce the number of scan threads to between two and five, which is well below the default value of 10.

There are various other ways to increase resource availability, including the following:

- Reduce the number of target assets, services, or vulnerability checks. The cost is accuracy.
- Reduce the number of assets that are scanned simultaneously. The cost is time.
- Perform less exhaustive scans. Doing so primarily reduces scan times, but it also frees up threads.

The primary tuning tool: the scan template

Scan templates contain a variety of parameters for defining how assets are scanned. Most tuning procedures involve editing scan template settings.

The built-in scan templates are designed for different use cases, such as PCI compliance, Microsoft Hotfix patch verification, Supervisory Control And Data Acquisition (SCADA) equipment audits, and Web site scans. You can find detailed information about scan templates in the section titled *Scan templates* on page 684. This section includes use cases and settings for each scan template.

Templates are best practices

Note: Until you are familiar with technical concepts related to scanning, such as port discovery and packet delays, it is recommended that you use built-in templates.

You can use built-in templates without altering them, or create custom templates based on built-in templates. You also can create new custom templates. If you opt for customization, keep in mind that built-in scan templates are themselves best practices. Not only do built-in templates address specific use cases, but they also reflect the delicate balance of factors in the performance triangle: time, resources, and accuracy.

You will notice that if you select the option to create a new template, many basic configuration settings have built-in values. It is recommended that you do not change these values unless you have a thorough working knowledge of what they are for. Use particular caution when changing any of these built-in values.

If you customize a template based on a built-in template, you may not need to change every single scan setting. You may, for example, only need to change a thread number or a range of ports and leave all other settings untouched.

For these reasons, it's a good idea to perform any customizations based on built-in templates. Start by familiarizing yourself with built-in scan templates and understanding what they have in common and how they differ. The following section is a comparison of four sample templates.

Understanding configurable phases of scanning

Understanding the phases of scanning is helpful in understanding how scan templates are structured.

Each scan occurs in three phases:

- asset discovery
- service discovery
- vulnerability checks

Note: The discovery phase in scanning is a different concept than that of *asset discovery*, which is a method for finding potential scan targets in your environment.

During the *asset discovery* phase, a Scan Engine sends out simple packets at high speed to target IP addresses in order to verify that network assets are live. You can configure timing intervals for these communication attempts, as well as other parameters, on the *Asset Discovery* and *Discovery Performance* pages of the *Scan Template Configuration* panel.

Upon locating the asset, the Scan Engine begins the *service discovery* phase, attempting to connect to various ports and to verify services for establishing valid connections. Because the application scans Web applications, databases, operating systems and network hardware, it has many opportunities for attempting access. You can configure attributes related to this phase on the *Service Discovery* and *Discovery Performance* pages of the *Scan Template Configuration* panel.

During the third phase, known as the *vulnerability check* phase, the application attempts to confirm vulnerabilities listed in the scan template. You can select which vulnerabilities to scan for in *Vulnerability Checking* page of the *Scan Template Configuration* panel.

Other configuration options include limiting the types of services that are scanned, searching for specific vulnerabilities, and adjusting network bandwidth usage.

In every phase of scanning, the application identifies as many details about the asset as possible through a set of methods called fingerprinting. By inspecting properties such as the specific bit settings in reserved areas of a buffer, the timing of a response, or a unique acknowledgement interchange, the application can identify indicators about the asset's hardware, operating system, and, perhaps, applications running under the system. A well-protected asset can mask its existence, its identity, and its components from a network scanner.

Do you need to alter templates or just alter-nate them?

When you become familiar with the built-in scan templates, you may find that they meet different performance needs at different times.

Tip: Use your variety of report templates to parse your scan results in many useful ways. Scans are a resource investment, especially “deeper” scans. Reports help you to reap the biggest possible returns from that investment.

You could, for example, schedule a Web audit to run on a weekly basis, or even more frequently, to monitor your Internet-facing assets. This is a faster scan and less of a drain on resources. You could also schedule a Microsoft hotfix scan on a monthly basis for patch verification. This scan requires credentials, so it takes longer. But the trade-off is that it doesn't have to occur as frequently. Finally, you could schedule an exhaustive scan on a quarterly basis do get a detailed, all-encompassing view of your environment. It will take time and bandwidth but, again, it's a less frequent scan that you can plan for in advance

Note: If you change templates regularly, you will sacrifice the conveniences of scheduling scans to run at automatic intervals with the same template.

Another way to maximize time and resources without compromising on accuracy is to alternate target assets. For example, instead of scanning all your workstations on a nightly basis, scan a third of them and then scan the other two thirds over the next 48 hours. Or, you could alternate target ports in a similar fashion.

Quick tuning: What can you turn off?

Sometimes, tuning scan performance is a simple matter of turning off one or two settings in a template. The fewer things you check for, the less time or bandwidth you'll need to complete a scan. However, your scan will be less comprehensive, and so, less accurate.

Note: Credentialed checks are critical for accuracy, as they make it possible to perform “deep” system scans. Be absolutely certain that you don't need credentialed checks before you turn them off.

If the scope of your scan does not include Web assets, turn off Web spidering, and disable Web-related vulnerability checks. If you don't have to verify hotfix patches, disable any hotfix checks. Turn off credentialed checks if you are not interested in running them. If you do run credentialed checks, make sure you are only running necessary ones.

An important note here is that you need to know exactly what's running on your network in order to know what to turn off. This is where discovery scans become so valuable. They provide you with a reliable, dynamic asset inventory. For example, if you learn, from a discovery scan, that you have no servers running Lotus Notes/Domino, you can exclude those policy checks from the scan.

Configuring custom scan templates

To begin modifying a default template go to the *Administration* page, and click **manage** for *Scan Templates*. The console displays the *Scan Templates* pages.

You cannot directly edit a built-in template. Instead, make a copy of the template and edit that copy. When you click **Copy** for any default template listed on the page, the console displays the *Scan Template Configuration* panel.

To create a custom scan template from scratch, go to the **Administration page,** and click **create** for *Scan Templates*.

Note: The PCI-related scanning and reporting templates are packaged with the application, but they require purchase of a license in order to be visible and available for use. The FDCC template is only available with a license that enables FDCC policy scanning.

The console displays the *Scan Template Configuration* panel. All attribute fields are blank.

Fine-tuning: What can you turn up or down?

Configuring templates to fine-tune scan performance involves trial and error and may include unexpected results at first. You can prevent some of these by knowing your network topology, your asset inventory, and your organization's schedule and business practices. And always keep the triangle in mind. For example, don't increase simultaneous scan tasks dramatically if you know that backup operations are in progress. The usage spike might impact bandwidth.

Familiarize yourself with built-in scan templates and how they work before changing any settings or customizing templates from scratch. See *Scan templates* on page 684.

Default and customized credential checking

Many products provide default login user IDs and passwords upon installation. Oracle ships with over 160 default user IDs. Windows users may not disable the guest account in their system. If you don't disable the default account vulnerability check type when creating a scan template, the application can perform checks for these items. See *Configuration steps for vulnerability check settings* on page 603 for information on enabling and disabling vulnerability check types.

The application performs checks against databases, applications, operating systems, and network hardware using the following protocols:

- CVS
- Sybase
- AS/400
- DB2
- SSH
- Oracle
- Telnet
- CIFS (Windows File Sharing)
- FTP
- POP
- HTTP
- SNMP
- SQL/Server
- SMTP

To specify users IDs and passwords for logon, you must enter appropriate credentials during site configuration See *Configuring scan credentials* on page 93. If a specific asset is not chosen to restrict credential attempts then the application will attempt to use these credentials on all assets. If a specific service is not selected then it will attempt to use the supplied credentials to access all services.

Starting a new custom scan template

If you are creating a new scan template from scratch, start with the following steps:

1. On the *Administration* page, click the **Create** link for *Scan templates*.
   OR
   If you are in the *Browse Scan Templates* window for a site configuration, click **Create**.
2. On the *Scan Template Configuration–General* page, enter a name and description for the new template.
3. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Selecting the type of scanning you want to do

You can configure your template to include all available types of scanning, or you can limit the scope of the scan to focus resources on specific security needs. To select the type of scanning you want to do, take the following steps.

1. Go to the *Scan Template Configuration–General* page.
2. Select one or more of the following options:

- **Asset Discovery**—Asset discovery occurs with every scan, so this option is always selected. If you select only **Asset Discovery**, the template will not include any vulnerability or policy checks. By default, all other options are selected, so you need to clear the other option check boxes to select asset discovery only.
- **Vulnerabilities**—Select this option if you want the scan to include vulnerability checks. To select or exclude specific checks, click the **Vulnerability Checks** link in the left navigation pane of the configuration panel. See *Configuration steps for vulnerability check settings* on page 603.
- **Web Spidering**—Select this option if you want the scan to include checks that are performed in the process of Web spidering. If you want to perform Web spidering checks only, you will need to click the Vulnerability Checks link in the left navigation pane of the configuration panel and disable non-Web spidering checks. See *Configuration steps for vulnerability check settings* on page 603. You must select the vulnerabilities option first in order to select Web spidering.
- **Policies**—Select this option if you want the scan to include policy checks, including Policy Manager. You will need to select individual checks and configure other settings, depending on the policy. See *Selecting Policy Manager checks* on page 608, *Configuring verification of standard policies* on page 611, and *Performing configuration assessment* on page 682.

3. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Tuning performance with simultaneous scan tasks

You may want to improve scan performance by tuning the number of scan processes or tasks that occur simultaneously.

Increasing the number of simultaneous scan processes against a host with an excessive number of ports can reduce scan time. In “tar pits,” or scan environments with targets that have a very high number of ports open, such as 60,000 or more, scanning multiple hosts simultaneously can help the scan complete more quickly without timing out.

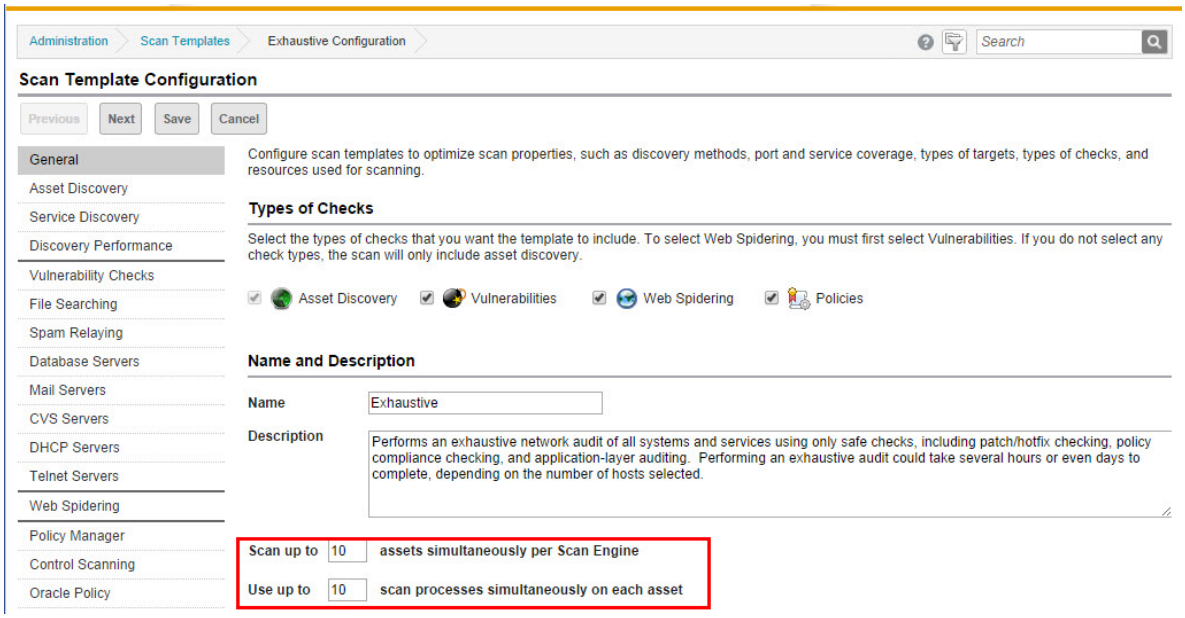
In another example, when your scan template allows for multiple scan processes to run on a single asset, performance improves for protocol fingerprinting and certain vulnerability checks, meaning that the scan can complete more quickly.

Note: If protocol fingerprinting exceeds one hour, it will stop and be reported as a timeout in the scan log.

You can configure these settings in your scan template:

- scanning multiple hosts simultaneously
- running multiple scan processes on an asset

To access these settings, click the **General** tab of the *Scan Template Configuration* panel. The settings appear at the bottom of the *General* page. To change the value for either default setting, enter a different value in the respective text box.



Scan template settings for simultaneous scan processes

For built-in scan templates, the default values depend on the scan template. For example, in the Discovery Scan - Aggressive template, the default number of hosts to scan simultaneously per Scan Engine is 25. This setting is higher than most built-in templates, because it is designed for higher-speed networks.

You can optimize scan performance by configuring the number of simultaneous scan processes against each host to match the average number of ports open per host in your environment.

You can optimize scan performance even more, but with less efficient use of Scan Engine resources, by setting the number of simultaneous scan processes against each host to match the highest number of ports open on any host in your environment.

Resource considerations

Scanning high numbers of assets simultaneously can be memory intensive. You can consider lowering them if you are encountering short-term memory issues. As a general rule, keep the setting for simultaneous host scanning to within 10 per 4 GB memory on the Scan Engine.

Certain scan operations, such as if policy scanning or Web spidering consume more memory per host. If such operations are enabled, you may need to reduce the number of hosts being scanned in parallel to compensate.

Configuring asset discovery

Asset discovery configuration involves three options:

- determining if target assets are live
- collecting information about discovered assets
- reporting any assets with unauthorized MAC addresses

If you choose not to configure asset discovery in a custom scan template, the scan will begin with service discovery.

Determining if target assets are live

Determining whether target assets are live can be useful in environments that contain large numbers of assets, which can be difficult to keep track of. Filtering out dead assets from the scan job helps reduce scan time and resource consumption.

Three methods are available to contact assets:

- ICMP echo requests (also known as “pings”)
- TCP packets
- UDP packets

The potential downside is that firewalls or other protective devices may block discovery connection requests, causing target assets to appear dead even if they are live. If a firewall is on the network, it may block the requests, either because it is configured to block network access for any packets that meet certain criteria, or because it regards any scan as a potential attack. In either case, the application reports the asset to be *DEAD* in the scan log. This can reduce the overall accuracy of your scans. Be mindful of where you deploy Scan Engines and how Scan Engines interact with firewalls. See *Make your environment “scan-friendly”* on page 626.

Using more than one discovery method promotes more accurate results. If the application cannot verify that an asset is live with one method, it will revert to another.

Note: The Web audit and Internet DMZ audit templates do not include any of these discovery methods.

Peripheral networks usually have very aggressive firewall rules in place, which blunts the effectiveness of asset discovery. So for these types of scans, it's more efficient to have the application "assume" that a target asset is live and proceed to the next phase of a scan, service discovery. This method costs time, because the application checks ports on all target assets, whether or not they are live. The benefit is accuracy, since it is checking all possible targets.

By default, the Scan Engine uses ICMP protocol, which includes a message type called ECHO REQUEST, also known as a ping, to seek out an asset during device discovery. A firewall may discard the pings, either because it is configured to block network access for any packets that meet certain criteria, or because it regards any scan as a potential attack. In either case, the application infers that the device is not present, and reports it as *DEAD* in the scan log.

Note: Selecting both TCP and UDP for device discovery causes the application to send out more packets than with one protocol, which uses up more network bandwidth.

You can select TCP and/or UDP as additional or alternate options for locating lives hosts. With these protocols, the application attempts to verify the presence of assets online by opening connections. Firewalls are often configured to allow traffic on port 80, since it is the default HTTP port, which supports Web services. If nothing is registered on port 80, the target asset will send a "port closed" response, or no response, to the Scan Engine. This at least establishes that the asset is online and that port scans can occur. In this case, the application reports the asset to be *ALIVE* in scan logs.

If you select TCP or UDP for device discovery, make sure to designate ports in addition to 80, depending on the services and operating systems running on the target assets. You can view TCP and UDP port settings on default scan templates, such as Discovery scan and Discovery scan (aggressive) to get an idea of commonly used port numbers.

TCP is more reliable than UDP for obtaining responses from target assets. It is also used by more services than UDP. You may wish to use UDP as a supplemental protocol, as target devices are also more likely to block the more common TCP and ICMP packets.

If a scan target is listed as a host name in the site configuration, the application attempts DNS resolution. If the host name does not resolve, it is considered *UNRESOLVED*, which, for the purposes of scanning, is the equivalent of *DEAD*.

UDP is a less reliable protocol for asset discovery since it doesn't incorporate TCP's handshake method for guaranteeing data integrity and ordering. Unlike TCP, if a UDP port doesn't respond to a communication attempt, it is usually regarded as being open.

Fine-tuning scans with verification of live assets

Asset discovery can be an efficient accuracy boost. Also, disabling asset discovery can actually bump up scan times. The application only scans an asset if it verifies that the asset is live. Otherwise, it moves on. For example, if it can first verify that 50 hosts are live on a sparse class C network, it can eliminate unnecessary port scans.

It is a good idea to enable ICMP and to configure intervening firewalls to permit the exchange of ICMP echo requests and reply packets between the application and the target network.

Make sure that TCP is also enabled for asset discovery, especially if you have strict firewall rules in your internal networks. Enabling UDP may be excessive, given the dependability issues of UDP ports. To make the judgment call with UDP ports, weigh the value of thoroughness (accuracy) against that of time.

If you do not select any discovery methods, scans assume that all target assets are live, and immediately begin service discovery.

Ports used for asset discovery

If the application uses TCP or UDP methods for asset discovery, it sends request packets to specific ports. If the application contacts a port and receives a response that the port is open, it reports the host to be “live” and proceeds to scan it.

The PCI audit template includes extra TCP ports for discovery. With PCI scans, it’s critical not to miss any live assets.

Configuration steps for verifying live assets

1. Go to the *Scan Template Configuration–Asset Discovery* page.
2. Select one or more of the displayed methods to locate live hosts.
3. If you select TCP or UDP, enter one or more port numbers for each selection. The application will send the TCP or UDP packets to these ports.
4. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Collecting information about discovered assets

You can collect certain information about discovered assets and the scanned network before performing vulnerability checks. All of these discovery settings are optional.

Finding other assets on the network

The application can query DNS and WINS servers to find other network assets that may be scanned.

Microsoft developed Windows Internet Name Service (WINS) for name resolution in the LAN manager environment of NT 3.5. The application can interrogate this broadcast protocol to locate the names of Windows workstations and servers. WINS usually is not required. It was developed originally as a system database application to support conversion of NETBIOS names to IP addresses.

If you enable the option to discover other network assets, the application will discover and interrogate DNS and WINS servers for the IP addresses of all supported assets. It will include those assets in the list of scanned systems.

Collecting Whois information

Note: Whois does not work with internal RFC1918 addresses.

Whois is an Internet service that obtains information about IP addresses, such as the name of the entity that owns it. You can improve Scan Engine performance by not requiring interrogation of a Whois server for every discovered asset if a Whois server is unavailable in the network.

Fingerprinting TCP/IP stacks

The application identifies as many details about discovered assets as possible through a set of methods called IP fingerprinting. By scanning an asset's IP stack, it can identify indicators about the asset's hardware, operating system, and, perhaps, applications running on the system. Settings for IP fingerprinting affect the accuracy side of the performance triangle.

The retries setting defines how many times the application will repeat the attempt to fingerprint the IP stack. The default retry value is 0. IP fingerprinting takes up to a minute per asset. If it can't fingerprint the IP stack the first time, it may not be worth additional time make a second attempt. However, you can set it to retry IP fingerprinting any number of times.

Whether or not you do enable IP fingerprinting, the application uses other fingerprinting methods, such as analyzing service data from port scans. For example, by discovering Internet Information Services (IIS) on a target asset, it can determine that the asset is a Windows Web server.

The certainty value, which ranges between 0.0 and 1.0 reflects the degree of certainty with which and asset is fingerprinted. If a particular fingerprint is below the minimum certainty value, the application discards the IP fingerprinting information for that asset. As with the performance settings related to asset discovery, these settings were carefully defined with best practices in mind, which is why they are identical.

Configuration steps for collecting information about discovered assets:

1. Go to the *Scan Template Configuration–Asset Discovery* page.
2. If desired, select the check box to discover other assets on the network, and include them in the scan.
3. If desired, select the option to collect Whois information.
4. If desired, select the option to fingerprint TCP/IP stacks.
5. If you enabled the fingerprinting option, enter a retry value, which is the number of repeated attempts to fingerprint IP stacks if first attempts fail.
6. If you enabled the fingerprinting option, enter a minimum certainty level. If a particular fingerprint is below the minimum certainty level, it is discarded from the scan results.
7. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Reporting unauthorized MAC addresses

You can configure scans to report unauthorized MAC addresses as vulnerabilities. The Media Access Control (MAC) address is a hardware address that uniquely identifies each node in a network.

In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sub layers: the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer.The MAC layer interfaces directly with the network media. Each different type of network media requires a different MAC layer. On networks that do not conform to the IEEE 802 standards but do conform to the OSI Reference Model, the node address is called the Data Link Control (DLC) address.

In secure environments it may be necessary to ensure that only certain machines can connect to the network. Also, certain conditions must be present for the successful detection of unauthorized MAC addresses:

- SNMP must be enabled on the router or switch managing the appropriate network segment.
- The application must be able to perform authenticated scans on the SNMP service for the router or switch that is controlling the appropriate network segment. See *Enabling authenticated scans of SNMP services* on page 593.
- The application must have a list of trusted MAC address against which to check the set of assets located during a scan. See *Creating a list of authorized MAC addresses* on page 594.
- The scan template must have MAC address reporting enabled. See *Enabling reporting of MAC addresses in the scan template* on page 594.
- The Scan Engine performing the scan must reside on the same segment as the systems being scanned.

Enabling authenticated scans of SNMP services

To enable the application to perform authenticated scans to obtain the MAC address, take the following steps:

1. Click **Edit** of the site for which you are creating the new scan template on the *Home* page of the console interface.

   The console displays the *Site Configuration* panel for that site.

2. Go to the *Credentials* page and click **Add credentials**.

   The console displays a *New Login* box.

3. Enter logon information for the SNMP service for the router or switch that is controlling the appropriate network segment. This will allow the application to retrieve the MAC addresses from the router using ARP requests.

4. Test the credential if desired.

   For detailed information about configuring credentials, see *Configuring scan credentials* on page 93.

5. Click **Save**.

   The new logon information appears on the *Credentials* page.

6. Click the **Save** tab to save the change to the site configuration.

Creating a list of authorized MAC addresses

To create a list of trusted MAC addresses, take the following steps:

1. Using a text editor, create a file listing trusted MAC addresses. The application will not report these addresses as violating the trusted MAC address vulnerability. You can give the file any valid name.
2. Save the file in the application directory on the host computer for the Security Console.

   The default path in a Windows installation is:

   C:Program Files\[installation_directory]\plugins\java\1\NetworkScanners\1\[file_name]

   The default location under Linux is:

   /opt/[installation_directory]/java/1/NetworkScanners/1/[filename]

Enabling reporting of MAC addresses in the scan template

To enable reporting of unauthorized MAC addresses in the scan template, take the following steps:

1. Go to the *Scan Template Configuration–Asset Discovery* page.
2. Select the option to report unauthorized MAC addresses.
3. Enter the full directory path location and file name of the file listing trusted Mac addresses.
4. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

With the trusted MAC file in place and the scanner value set, the application will perform trusted MAC vulnerability testing. To do this it first makes a direct ARP request to the target asset to pick up its MAC address. It also retrieves the ARP table from the router or switch controlling the

segment. Then, it uses SNMP to retrieve the MAC address from the asset and interrogates the asset using its NetBIOS name to retrieve its MAC address.

Configuring service discovery

Once the application verifies that a host is live, or running, it begins to scan ports to collect information about services running on the computer. The target range for service discovery can include TCP and UDP ports.

TCP ports (RFC 793) are the endpoints of logical connections through which networked computers carry on “conversations.”

Well Known ports are those most commonly found to be open on the Internet.

The range of ports may be extended beyond Well Known Port range. Each vulnerability check may add a set of ports to be scanned. Various back doors, trojan horses, viruses, and other worms create ports after they have installed themselves on computers. Rogue programs and hackers use these ports to access the compromised computers. These ports are not predefined, and they may change over time. Output reports will show which ports were scanned during vulnerability testing, including maliciously created ports.

Various types of port scan methods are available as custom options. Most built-in scan templates incorporate the Stealth scan (SYN) method, in which the port scanner process sends TCP packets with the SYN (synchronize) flag. This is the most reliable method. It's also fast. In fact, a SYN port scan is approximately 20 times faster than a scan with the full-connect method, which is one of the other options for the TCP port scan method.

The exhaustive template and penetration tests are exceptions in that they allow the application to determine the optimal scan method. This option makes it possible to scan through firewalls in some cases; however, it is somewhat less reliable.

Although most templates include UDP ports in the scope of a scan, they limit UDP ports to well-known numbers. Services that run on UDP ports include DNS, TFTP, and DHCP. If you want to be absolutely thorough in your scanning, you can include more UDP ports, but doing so will increase scan time.

Performance considerations for port scanning

Scanning all possible ports takes a lot of time. If the scan occurs through a firewall, and the firewall has been set up to drop packets sent to non-authorized devices, than a full-port scan may span several hours to several days. If you configure the application to scan all ports, it may be necessary to change additional parameters.

Service discovery is the most resource-sensitive phase of scanning. The application sends out hundreds of thousands of packets to scan ports on a mere handful of assets.

The more ports you scan, the longer the scan will take. And scanning the maximum number of ports is not necessarily more accurate. It is a best practice select target ports based on discovery data. If you simply are not sure of which ports to scan, use well known numbers. Be aware, though, that attackers may avoid these ports on purpose or probe additional ports for service attack opportunities.

Note: The application relies on network devices to return "ICMP port unreachable" packets for closed UDP ports.

If you want to be a little more thorough, use the target list of TCP ports from more aggressive templates, such as the exhaustive or penetration test template.

If you plan to scan UDP ports, keep in mind that aside from the reliability issues discussed earlier, scanning UDP ports can take a significant amount of time. By default, the application will only send two UDP packets per second to avoid triggering the ICMP rate-limiting mechanisms that are built into TCP/IP stacks for most network devices. Sending more packets could result in packet loss. A full UDP port scan can take up to nine hours, depending on bandwidth and the number of target assets.

To reduce scan time, do not run full UDP port scans unless it is necessary. UDP port scanning generally takes longer than TCP port scanning because UDP is a "connectionless" protocol. In a UDP scan, the application interprets non-response from the asset as an indication that a port is *open* or *filtered*, which slows the process. When configured to perform UDP scanning, the application matches the packet exchange pace of the target asset. Oracle Solaris only responds to 2 UDP packet failures per second as a rate limiting feature, so this scanning in this environment can be very slow in some cases.

Configuration steps for service discovery

1. Go to the *Scan Template Configuration–Service Discovery* page.

Tip: You can achieve the most "stealthy" scan by running a vulnerability test with port scanning disabled. However, if you do so, the application will be unable to discover services, which will hamper fingerprinting and vulnerability discovery.

2. Select a TCP port scan method from the drop-down list.
3. Select which TCP ports you wish to scan from the drop-down list.

   If you want to scan additional TCP ports, enter the numbers or range in the **Additional ports** text box.

Note: If you want to scan with PowerShell, add port 5985 to the port list if it is not already included. If you have enabled PowerShell but do not want to scan with that capability, make sure that port 5985 is not in the port list. See the topic *Configuring scan credentials* on page 93 for more information.

4. Select which UDP ports you want to scan from the drop-down list.

If you want to scan additional UDP ports, enter the desired range in the **Additional ports** text box.

Note: Consult Technical Support to change the default service file setting.

5. If you want to change the service names file, enter the new file name in the text box.

   This properties file lists each port and the service that commonly runs on it. If scans cannot identify actual services on ports, service names will be derived from this file in scan results.

   The default file, default-services.properties, is located in the following directory: <installation_directory/plugins/java/1/NetworkScanners/1.

   You can replace the file with a custom version that lists your own port/service mappings.

6. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Changing discovery performance settings

You can change default scan settings to maximize speed and resource usage during asset and service discovery. If you do not change any of these discovery performance settings, scans will auto-adjust based on network conditions.

Changing packet-related settings can affect the triangle. See *Keep the "triangle" in mind when you tune* on page 574. Shortening send-delay intervals theoretically increases scan speeds, but it also can lead to network congestion depending on bandwidth. Lengthening send-delay intervals increases accuracy. Also, longer delays may be necessary to avoid blacklisting by firewalls or IDS devices.

How ports are scanned

In the following explanation of how ports are scanned, the numbers indicated are default settings and can be changed. The application sends a block of 10 packets to a target port, waits 10 milliseconds, sends another 10 packets, and continues this process for each port in the range. At

the end of the scan, it sends another round of packets and waits 10 milliseconds for each block of packets that have not received a response. The application repeats these attempts for each port five times.

If the application receives a response within the defined number of retries, it will proceed with the next phase of scanning: service discovery. If it does not receive a response after exhausting all discovery methods defined in the template, it reports the asset as being *DEAD* in the scan log.

When the target asset is on a local system segment (not behind a firewall), the scan occurs more rapidly because the asset will respond that ports are closed. The difficulty occurs when the device is behind a firewall, which consumes packets so that they do not return to the Scan Engine. In this case the application will wait the maximum time between port scans. TCP port scanning can exceed five hours, especially if it includes full-port scans of 65K ports.

Try to scan the asset on the local segment inside the firewall. Try not to perform full TCP port scans outside a device that will drop the packets like a firewall unless necessary.

You can change the following performance settings:

Note: For minimum retries, packet-per-second rate, and simultaneous connection requests, the default value of 0 disables manual settings, in which case, the application auto-adjusts the settings. To enable manual settings, enter a value of 1 or greater.

Maximum retries

This is the maximum number of attempts to contact target assets. If the limit is exceeded with no response, the given asset is not scanned. The default number of UDP retries is 5, which is high for a scan through a firewall. If UDP scanning is taking longer than expected, try reducing the retry value to 2 or 3.

You may be able speed up the scanning process by reducing the maximum retry count from the default of 4. Lowering the number of retries for sending packets is a good accuracy adjustment in a network with high-traffic or strict firewall rules. In an environment like this, it's easier to lose packets. Consider setting the retry value at 3. Note that the scan will take longer.

Timeout interval

Set the number of milliseconds to wait between retries. You can set an initial timeout interval, which is the first setting that the scan will use. You also can set a range. For maximum timeout interval, any value lower than 5 ms disables manual settings, in which case, the application auto-adjusts the settings. The discovery may auto-adjust interval settings based on varying network conditions.

Scan delay

This is the number of milliseconds to wait between sending packets to each target host.

Note: Reducing these settings may cause scan results to become inaccurate.

Increasing the delay interval for sending TCP packets will prevent scans from overloading routers, triggering firewalls, or becoming blacklisted by Intrusion Detection Systems (IDS). Increasing the delay interval for sending packets is another measure that increases accuracy at the expense of time.

You can increase the accuracy of port scans by slowing them down with 10- to 25-millisecond delays.

Packet-per-second rate

This is the number of packets to send each second during discovery attempts. Increasing this rate can increase scan speed. However, more packets are likely to be dropped in congestion-heavy networks, which can skew scan results.

Note: To enable the defeat rate limit, you must have the Stealth (SYN) scan method selected. See *Scan templates* on page 684.

An additional control, called **Defeat Rate Limit** (also known as defeat-rst-rate limit), enforces the minimum packet-per-second rate. This may improve scan speed when a target host limits its rate of RST (reset) responses to a port scan. However, enforcing the packet setting under these circumstances may cause the scan to miss ports, which lowers scan accuracy. Disabling the defeat rate limit may cause the minimum packet setting to be ignored when a target host limits its rate of RST (reset) responses to a port scan. This can increase scan accuracy.

Parallelism (simultaneous connection requests)

This is the number of discovery connection requests to be sent to target hosts simultaneously. More simultaneous requests can mean faster scans, subject to network bandwidth. This setting has no effect if values have been set for scan delay.

Configuration steps for tuning discovery performance

1. Go to the *Scan Template Configuration–Discovery Performance* page.
2. For **Maximum retries**, drag the slider to the left or right to adjust the value if desired.
3. For **Timeout interval**, drag the sliders to the left or right to adjust the **Initial**, **Minimum**, and **Maximum** values if desired.
4. For **Scan Delay**, drag the sliders to the left or right to adjust the values if desired.
5. For **Packet-per-second rate**, drag the sliders to the left or right to adjust the **Minimum** and **Maximum** values if desired.
6. Select the **Defeat Rate Limit** checkbox to enforce the minimum packet-per-second rate if desired.
7. For **Parallelism**, drag the sliders to the left or right to adjust the **Minimum** and **Maximum** values if desired.
8. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Selecting vulnerability checks

When the application fingerprints an asset during the discovery phases of a scan, it automatically determines which vulnerability checks to perform, based on the fingerprint. On the *Vulnerability Checks* page of the *Scan Template Configuration* panel, you can manually configure scans to include more checks than those indicated by the fingerprint. You also can disable checks.

Unsafe checks include buffer overflow tests against applications like IIS, Apache, services like FTP and SSH. Others include protocol errors in some database clients that trigger system failures. Unsafe scans may crash a system or leave a system in an indeterminate state, even though it appears to be operating normally. Scans will most likely not do any permanent damage to the target system. *However*, if processes running in the system might cause data corruption in the event of a system failure, unintended side effects may occur.

The benefit of unsafe checks is that they can verify vulnerabilities that threaten denial of service attacks, which render a system unavailable by crashing it, terminating a service, or consuming services to such an extent that the system using them cannot do any work.

You should run scheduled unsafe checks against target assets outside of business hours and then restart those assets after scanning. It is also a good idea to run unsafe checks in a pre-production environment to test the resistance of assets to denial-of-service conditions.

If you want to perform checks for potential vulnerabilities, select the appropriate check box. For information about potential vulnerabilities, see *Setting up scan alerts* on page 143.

If you want to correlate reliable checks with regular checks, select the appropriate check box. With this setting enabled, the application puts more trust in operating system patch checks to attempt to override the results of other checks that could be less reliable. Operating system patch checks are more reliable than regular vulnerability checks because they can confirm that a target asset is at a patch level that is known to be not vulnerable to a given attack. For example, if a vulnerability check is positive for an Apache Web server based on inspection the HTTP banner, but an operating system patch check determines that the Apache package has been patched for this specific vulnerability, it will not report a vulnerability. Enabling reliable check correlation is a best practice that reduces false positives.

The application performs operating-system-level patch verification checks on the following targets:

- Microsoft Windows
- Red Hat
- CentOS
- Solaris
- VMware

Note: To use check correlation, you must use a scan template that includes patch verification checks, and you must typically include logon credentials in your site configuration. See *Configuring scan credentials* on page 93.

A scan template may specify certain vulnerability checks to be enabled, which means that the application will scan only for those vulnerability check types or categories with that template. If you do not specifically enable any vulnerability checks, then you are essentially enabling *all* of them, except for those that you specifically *disable*.

A scan template may specify certain checks as being disabled, which means that the application will scan for all vulnerabilities except for those vulnerability check types or categories with that template. In other words, *if no checks are disabled, it will scan for all vulnerabilities.* While the exhaustive template includes all possible vulnerability checks, the full audit and PCI audit templates exclude policy checks, which are more time consuming. The Web audit template appropriately only scans for Web-related vulnerabilities.

Configuration steps for vulnerability check settings

1. Go to the *Vulnerability Checks* page.

   Note the order of precedence for modifying vulnerability check settings, which is described at the top of the page.

2. Click the appropriate check box to perform unsafe checks.

   A safe vulnerability check will not alter data, crash a system, or cause a system outage during its validation routines.

Tip: To see which vulnerabilities are included in a category, click the category name.

3. Click **Add categories...**.

   The console displays a box listing vulnerability categories.

Tip: Categories that are named for manufacturers, such as Microsoft, can serve as supersets of categories that are named for their products. For example, if you select the Microsoft category, you inherently include all Microsoft product categories, such as Microsoft Path and Microsoft Windows. This applies to other "company" categories, such as Adobe, Apple, and Mozilla.

4. Click the check boxes for those categories you wish to scan for, and click **Save**.

   The console lists the selected categories on the *Vulnerability Checks* page.

Note: If you enable any specific vulnerability categories, you are implicitly disabling all other categories. Therefore, by not enabling specific categories, you are enabling all categories

5. Click **Remove categories...** to prevent the application from scanning for vulnerability categories listed on the *Vulnerability Checks* page.
6. Click the check boxes for those categories you wish to exclude from the scan, and click **Save**.

The console displays *Vulnerability Checks* page with those categories removed.

To select types for scanning, take the following steps:

Tip: To see which vulnerabilities are included in a check type, click the check type name.

1. Click **Add check types...**

   The console displays a box listing vulnerability types.

2. Click the check boxes for those categories you wish to scan for, and click **Save**.

The console lists the selected types on *Vulnerability Checks* page.

To avoid scanning for vulnerability types listed on the *Vulnerability Checks* page, click types listed on the *Vulnerability Checks* page:

1. Click **Remove check types...**.
2. Click the check boxes for those categories you wish to exclude from the scan, and click **Save**.

   The console displays *Vulnerability Checks* page with those types removed.

The following table lists current vulnerability types and the number of vulnerability checks that are performed for each type. The list is subject to change, but it is current at the time of this guide's publication.

Vulnerability types	Vulnerability types
Default account	Safe
Local	Sun patch
Microsoft hotfix	Unsafe
Patch	Version
Policy	Windows registry
RPM	

To select specific vulnerability checks, take the following steps:

1. Click **Enable vulnerability checks...**

   The console displays a box where you can search for specific vulnerabilities in the database.

2. Type a vulnerability name, or a part of it, in the search box.

3. Modify search settings as desired.

Note: The application only checks vulnerabilities relevant to the systems that it scans. It will not perform a check against a non-compatible system even if you specifically selected that check.

4. Click **Search**.

   The box displays a table of vulnerability names that match your search criteria.

5. Click the check boxes for vulnerabilities that you wish to include in the scan, and click **Save**.

   The selected vulnerabilities appear on the *Vulnerability Checks* page.

6. Click **Disable vulnerability checks...** to exclude specific vulnerabilities from the scan.

7. Search for the names of vulnerabilities you wish to exclude.

   The console displays the search results.

8. Click the check boxes for vulnerabilities that you wish to exclude from the scan, and click **Save**.

   The selected vulnerabilities appear on the *Vulnerability Checks* page.

   A specific vulnerability check may be included in more than one type. If you enable two vulnerability types that include the same check, it will only run that check once.

9. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Fine-tuning vulnerability checks

The fewer the vulnerabilities included in the scan template, the sooner the scan completes. It is difficult to gauge how long exploit test actually take. Certain checks may require more time than others.

Following are a few examples:

- The Microsoft IIS directory traversal check tests 500 URL combinations. This can take several minutes against a busy Web server.
- Unsafe, denial-of-service checks take a particularly long time, since they involve large amounts of data or multiple requests to target systems.
- Cross-site scripting (CSS/XSS) tests may take a long time on Web applications with many forms.

Be careful not to sacrifice accuracy by disabling too many checks—or essential checks. Choose vulnerability checks in a focused way whenever possible. If you are only scanning Web assets, enable Web-related vulnerability checks. If you are performing a patch verification scan, enable hotfix checks.

The application is designed to minimize scan times by grouping related checks in one scan pass. This limits the number of open connections and time interval that connections remain open. For checks relying solely on software version numbers, the application requires no further communication with the target system once it extracts the version information.

Using a plug-in to manage custom checks

If you have created custom vulnerability checks, use the custom vulnerability content plug-in to ensure that these checks are available for selection in your scan template. The process involves simply copying the check content into a directory of your Security Console installation.

In Linux, the location is in the plugins/java/1/CustomScanner/1 directory inside the root of your installation path. For example:

```
[installation_directory]/plugins/java/1/CustomScanner/1
```

In Windows, the location is in the plugins\java\1\CustomScanner\1 directory inside of the root of your installation path. For example:

```
[installation_directory]\plugins\java\1\CustomScanner\1
```

After copying the files, you can use the checks immediately by selecting them in your scan template configuration.

Selecting Policy Manager checks

If you work for a U.S. government agency, a vendor that transacts business with the government or for a company with strict configuration security policies, you may be running scans to verify that your assets comply with United States Government Configuration Baseline (USGCB) policies, Center for Internet Security (CIS) benchmarks, or Federal Desktop Core Configuration (FDCC). Or you may be testing assets for compliance with customized policies based on these standards. The built-in USGCB, CIS, and FDCC scan templates include checks for compliance with these standards. See *Scan templates* on page 684.

These templates do not include vulnerability checks, so if you want to run vulnerability checks with the policy checks, create a custom version of a scan template using one of the following methods:

- Add vulnerability checks to a customized copy of USGCB, CIS, DISA, or FDCC template.
- Add USGCB, CIS, DISA STIG, or FDCC checks to one of the other templates that includes the vulnerability checks that you want to run.
- Create a scan template and add USGCB, CIS, DISA STIG, or FDCC checks and vulnerability checks to it.

To use the second or third method, you will need to select USGCB, CIS, DISA STIGS, or FDCC checks by taking the following steps. You must have a license that enables the Policy Manager and FDCC scanning.

1. Select **Policies** in the *General* page of the *Scan Template Configuration* panel.
2. Go to the *Policy Manager* page of the *Scan Template Configuration* panel.
3. Select a policy.
4. Review the name, affected platform, and description for each policy.
5. Select the check box for any policy that you want to include in the scan.
6. If you are required to submit policy scan results in Asset Reporting Format (ARF) reports to the U.S. government for SCAP certification, select the check box to store SCAP data.

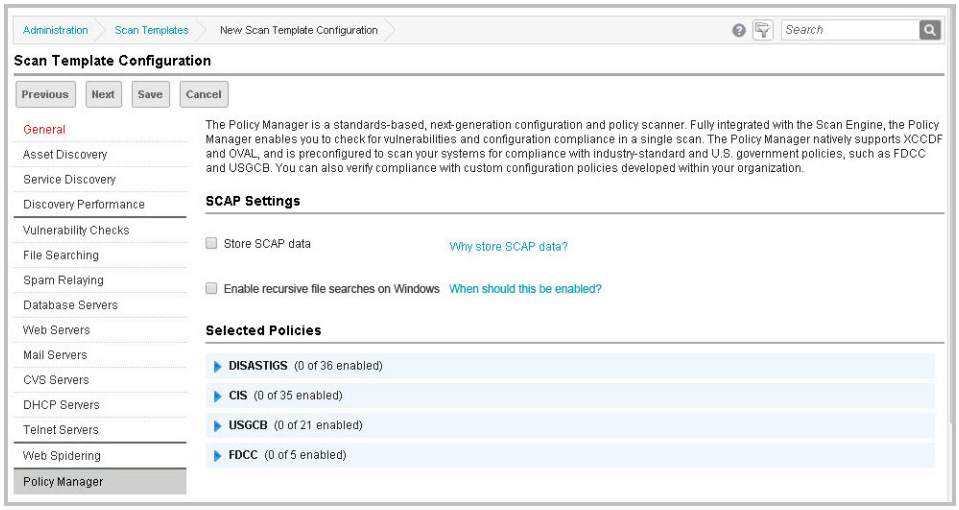
Note: Stored SCAP data can accumulate rapidly, which can have a significant impact on file storage.

7. If you want to enable recursive file searches on Windows systems, select the appropriate check box. It is recommended that you not enable this capability unless your internal security practices require it. See *Enabling recursive searches on Windows* on page 609.

Warning: Recursive file searches can increase scan times signficantly. A scan that typically completes in several minutes on an asset may not complete for several hours on that single asset, depending on various environmental conditions.

8. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

For information about verifying USGCB, CIS, or FDCC compliance, see See " Working with Policy Manager results" on page 297.



Selecting Policy Manager check settings

Enabling recursive searches on Windows

By default, recursive file searches are disabled for scans on assets running Microsoft Windows. Searching every sub-folder of a parent folder in a Windows file system can increase scan times on a single asset by hours, depending on the number of folders and files and other conditions. Only enable recursive file searches if your internal security practices require it or if you require it for certain rules in your policy scans. The following rules require recursive file searches:

DISA-6/Win2008
SV-29465r1_rule
Remove Certificate Installation Files

DISA-1/Win7
SV-25004r1_rule
Remove Certificate Installation Files

Note: Recursive file searches are enabled by default on Linux systems and cannot be disabled.

Configuring verification of standard policies

Configuring testing for Oracle policy compliance

To configure the application to test for Oracle policy compliance you must edit the default XML policy template for Oracle (oracle.xml), which is located in [installation_directory] /plugins/java/1/OraclePolicyScanner/1.

To configure the application to test for Oracle policy compliance:

1. Copy the default template to a new file name.
2. Edit the policy elements within the XML tags.
3. Move the new template file back into the [installation_directory] /plugins/java/1/OraclePolicyScanner/1 directory.

To add credentials for Oracle Database policy compliance scanning:

1. Go to the *Credentials* page for the site that will incorporate the new scan template.
2. Select *Oracle* as the login service domain.
3. Type a user name and password for an Oracle account with DBA access. See *Configuring scan credentials* on page 93.
4. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Configure testing for Lotus Domino policy compliance

To configure the application to test for Lotus Domino policy compliance you must edit the default XML policy template for Lotus Domino (domino.xml), which is located in [installation_directory] /plugins/java/1/NotesPolicyScanner/1.

To configure the application to test for Lotus Domino policy compliance:

1. Copy the default template to a new file name.
2. Edit the policy elements within the XML tags.
3. Move the new template file back into the [installation_directory] /plugins/java/1/NotesPolicyScanner/1.
4. Go to the *Lotus Domino Policy* page and enter the new policy file name in the text field.

To add credentials for Lotus Domino policy compliance scanning:

1. Go to the *Credentials* page for the site that will incorporate the new scan template.
2. Select *Lotus Notes/Domino* as the login service domain.
3. Type a Notes ID password in the text field. See *Configuring scan credentials* on page 93.
4. For Lotus Notes/Domino policy compliance scanning, you must install a Notes client on the same host computer that is running the Security Console.
5. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Configure testing for Windows Group Policy compliance

You can configure Nexpose to verify whether assets running with Windows operating systems are compliant with Microsoft security standards. The installation package includes three different policy templates that list security criteria against that you can use to check settings on assets. These templates are the same as those associated with Windows Policy Editor and Active Directory Group Policy. Each template contains all of the policy elements for one of the three types of Windows target assets: workstation, general server, and domain controller.

A target asset must meet all the criteria listed in the respective template for the application to regard it as compliant with Windows Group Policy. To view the results of a policy scan, create a report based on the Audit or Policy Evaluation report template. Or, you can create a custom report template that includes the Policy Evaluation section. See *Fine-tuning information with custom report templates* on page 543.

The templates are *.inf* files located in the plugins/java/1/WindowsPolicyScanner/1 path relative to the application base installation directory:

- The basicwk.inf template is for workstations.
- The basicsv.inf template is for general servers.
- The basicdc.inf template is for domain controllers.

Note: Use caution when running the same scan more than once with less than the lockout policy time delay between scans. Doing so could also trigger account lockout.

You also can import template files using the Security Templates Snap-In in the Microsoft Group Policy management Console, and then saving each as an *.inf* file with a specific name corresponding to the type of target asset.

You must provide the application with proper credentials to perform Windows policy scanning. See *Configuring scan credentials* on page 93.

Go to the *Windows Group Policy* page, and enter the *.inf* file names for workstation, general server, and domain controller policy names in the appropriate text fields.

To save the new scan template, click **Save**.

Configure testing for CIFS/SMB account policy compliance

Nexpose can test account policies on systems supporting CIFS/SMB, such as Microsoft Windows, Samba, and IBM AS/400:

1. Go to the **CIFS/SMB Account Policy** page.
2. Type an account lockout threshold value in the appropriate text field.

   This the maximum number of failed logins a user is permitted before the asset locks out the account.
3. Type a minimum password length in the appropriate text field.
4. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Configure testing for AS/400 policy compliance

To configure Nexpose to test for AS/400 policy compliance:

1. Go to the *AS/400 Policy* page.
2. Type an account lockout threshold value in the appropriate text field.

   This the maximum number of failed logins a user is permitted before the asset locks out the account. The number corresponds to the QMAXSIGN system value.
3. Type a minimum password length in the appropriate text field.

   This number corresponds to the QPWDMINLEN system value and specifies the minimum length of the password field required.
4. Select a **minimum security level** from the drop-down list.

   This level corresponds to the minimum value that the QSECURITY system value should be set to. The level values range from Password *security (20)* to *Advanced integrity protection* (50).
5. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Configure testing for UNIX policy compliance

To configure Nexpose to test for UNIX policy compliance:

1. Go to the *Unix Policy* page.
2. Type a number in the text field labeled **Minimum account umask value**.

   This setting controls the permissions that the target system grants to any new files created on it. If the application detects broader permissions than those specified by this value, it will report a policy violation.
3. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Configuring Web spidering

Nexpose can spider Web sites to discover their directory structures, default directories, the files and applications on their servers, broken links, inaccessible links, and other information.

The application then analyzes this data for evidence of security flaws, such as SQL injection, cross-site scripting (CSS/XSS), backup script files, readable CGI scripts, insecure password use, and other issues resulting from software defects or configuration errors.

Some built-in scan templates use the Web spider by default:

- Web audit
- HIPAA compliance
- Internet DMZ audit
- Payment Card Industry (PCI) audit
- Full audit

You can adjust the settings in these templates. You can also configure Web spidering settings in a custom template. The spider examines links within each Web page to determine which pages have been scanned. In many Web sites, pages that are yet to be scanned will show a base URL, followed by a parameter directed-link, in the address bar.

For example, in the address www.exampleinc.com/index.html?id=6, the ?id=6 parameter probably refers to the content that should be delivered to the browser. If you enable the setting to include query strings, the spider will check the full string www.exampleinc.com/index.html?id=6 against all URL pages that have been already retrieved to see whether this page has been analyzed.

If you do not enable the setting, the spider will only check the base URL without the ?id=6 parameter.

To gain access to a Web site for scanning, the application makes itself appear to the Web server application as a popular Web browser. It does this by sending the server a Web page request as a browser would. The request includes pieces of information called headers. One of the headers, called User-Agent, defines the characteristics of a user's browser, such as its version number and the Web application technologies it supports. User-Agent represents the application to the Web site as a specific browser, because some Web sites will refuse HTTP requests from browsers that they do not support. The default User-Agent string represents the application to the target Web site as Internet Explorer 7.

Configuration steps and options for Web spidering

Configure general Web spider settings:

1. Go to the *Web Spidering* page of the *Scan Template Configuration* panel.
2. Select the check box to enable Web spidering.

Note: Including query strings with Web spidering check box causes the spider to make many more requests to the Web server. This will increase overall scan time and possibly affect the Web server's performance for legitimate users.

3. Select the appropriate check box to include query strings when spidering if desired.
4. If you want the spider to test for persistent cross-site scripting during a single scan, select the check box for that option.

   This test helps to reduce the risk of dangerous attacks via malicious code stored on Web servers. Enabling it may increase Web spider scan times.

Note: Changing the default user agent setting may alter the content that the application receives from the Web site.

5. If you want to change the default value in the **Browser ID (User-Agent)** field enter a new value.

   If you are unsure of what to enter for the User-Agent string, consult your Web site developer.

6. Select the option to check the use of common user names and passwords if desired. The application reports the use of these credentials as a vulnerability. It is an insecure practice because attackers can easily guess them. With this setting enabled, the application attempts to log onto Web applications by submitting common user names and passwords to discovered authentication forms. Multiple logon attempts may cause authentication services to lock out accounts with these credentials.

(Optional) Enable the Web spider to check for the use of weak credentials:

As the Web spider discovers logon forms during a scan, it can determine if any of these forms accept commonly used user names or passwords, which would make them vulnerable to automated attacks that exploit this practice. To perform the check, the Web spider attempts to log

on through these forms with commonly used credentials. Any successful attempt counts as a vulnerability.

Note: This check may cause authentication services with certain security policies to lock out accounts with these commonly used credentials.

1. Go the *Weak Credential Checking* area on the Web spidering configuration page, and select the check box labeled **Check use of common user names and passwords**.

Configure Web spider performance settings:

1. Enter a maximum number of foreign hosts to resolve, or leave the default value of 100.

   This option sets the maximum number of unique host names that the spider may resolve. This function adds substantial time to the spidering process, especially with large Web sites, because of frequent cross-link checking involved. The acceptable host range is 1 to 500.

2. Enter the amount of time, in milliseconds, in the **Spider response timeout** field to wait for a response from a target Web server. You can enter a value from 1 to 3600000 ms (1 hour). The default value is 120000 ms (2 minutes). The Web spider will retry the request based on the value specified in the **Maximum retries for spider requests** field.

3. Type a number in the field labeled **Maximum directory levels to spider** to set a directory depth limit for Web spidering.

   Limiting directory depth can save significant time, especially with large sites. For unlimited directory traversal, type 0 in the field. The default value is 6.

Note: If you run recurring scheduled scans with a time limit, portions of the target site may remain unscanned at the end of the time limit. Subsequent scans will not resume where the Web spider left off, so it is possible that the target Web site may never be scanned in its entirety.

4. Type a number in the **Maximum spidering time (minutes)** field to set a maximum number of minutes for scanning each Web site.

   A time limit prevents scans from taking longer than allotted time windows for scan jobs, especially with large target Web sites. If you leave the default value of 0, no time limit is applied. The acceptable range is 1 to 500.

5. Type a number in the **Maximum pages to spider** field to limit the number of pages that the spider requests.

   This is a time-saving measure for large sites. The acceptable range is 1 to 1,000,000 pages.

Note: If you set both a time limit and a page limit, the Web spider will stop scanning the target Web site when the first limit is reached.

6. Enter the number of time to retry a request after a failure in the **Maximum retries for spider requests** field. Enter a value from 0 to 100. A value of 0 means do not retry a failed request. The default value is 2 retries.

Configure Web spider settings related to regular expressions:

1. Enter a regular expression for sensitive data field names, or leave the default string.

   The application reports field names that are designated to be sensitive as vulnerabilities: *Form action submits sensitive data in the clear*. Any matches to the regular expression will be considered sensitive data field names.

2. Enter a regular expression for sensitive content. The application reports as vulnerabilities strings that are designated to be sensitive. If you leave the field blank, it does not search for sensitive strings.

Configure Web spider settings related to directory paths:

1. Select the check box to instruct the spider to adhere to standards set forth in the *robots.txt* protocol.

   Robots.txt is a convention that prevents spiders and other Web robots from accessing all or part of Web site that are otherwise publicly viewable.

Note: Scan coverage of any included bootstrap paths is subject to time and page limits that you set in the Web spider configuration. If the scan reaches your specified time or page limit before scanning bootstrap paths, it will not scan those paths.

2. Enter the base URL paths for applications that are not linked from the main Web site URLs in the **Bootstrap paths** field if you want the spider to include those URLS.

Example: /myapp. Separate multiple entries with commas. If you leave the field blank, the spider does not include bootstrap paths in the scan.

3. Enter the base URL paths to exclude in the **Excluded paths** field. Separate multiple entries with commas.

   If you specify excluded paths, the application does not attempt to spider those URLs or discovery any vulnerabilities or files associated with them. If you leave the field blank, the spider does not exclude any paths from the scan.

Configure any other scan template settings as desired. When you have finished configuring the scan template, click **Save**.

Fine-tuning Web spidering

The Web spider crawls Web servers to determine the complete layout of Web sites. It is a thorough process, which makes it valuable for protecting Web sites. Most Web application vulnerability tests are dependent on Web spidering.

Nexpose uses spider data to evaluate custom Web applications for common problems such as SQL injection, cross-site scripting (CSS/XSS), backup script files, readable CGI scripts, insecure use of passwords, and many other issues resulting from custom software defects or incorrect configurations.

By default, the Web spider crawls a site using three threads and a per-request delay of 20 ms. The amount of traffic that this generates depends on the amount of discovered, linked site content. If you're running the application on a multiple-processor system, increase the number of spider threads to three per processor.

A complete Web spider scan will take slightly less than 90 seconds against a responsive server hosting 500 pages, assuming the target asset can serve one page on average per 150 ms. A scan against the same server hosting 10,000 pages would take approximately 28 minutes.

When you configure a scan template for Web spidering, enter the maximum number of directories, or depth, as well as the maximum number of pages to crawl per Web site. These values can limit the amount of time that Web spidering takes. By default, the spider ignores cross-site links and stays only on the end point it is scanning.

If your asset inventory doesn't include Web sites, be sure to turn this feature off. It can be very time consuming.

Configuring scans of various types of servers

Configuring spam relaying settings

Mail relay is a feature that allows SMTP servers to act as open gateways through which mail applications can send e-mail. Commercial operators, who send millions of unwanted spam e-mails, often target mail relay for exploitation. Most organizations now restrict mail relay services to specific domain users.

To configure spam relay settings:

1. Go to the *Spam Relaying* page:
2. Type an e-mail address in the appropriate text field.

   This e-mail address should be external to your organization, such as a Yahoo! or Hotmail address. The application will attempt to send e-mail from this account to itself using any mail services and mail scripts that it discovers during the scan. If the application receives the e-mail, this indicates that the servers are vulnerable.
3. Type a URL in the **HTTP_REFERRER to use** field.

   This is typically a Web form that spammers might use to generate Spam e-mails.
4. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Configuring scans of database servers

Nexposeperforms several classes of vulnerability and policy checks against a number of databases, including:

- MS SQL/Server versions 6, 7, 2000, 2005, 2008
- Oracle versions 6 through 10
- Sybase Adaptive Server Enterprise (ASE) versions 9, 10 and 11
- DB2
- AS/400
- PostgreSQL versions 6, 7, 8
- MySQL

For all databases, the application discovers tables and checks system access, default credentials, and default scripts. Additionally, it tests table access, stored procedure access, and decompilation.

To configure to scan database servers:

1. Go to the *Database Servers* page.
2. Enter the name of a DB2 database in the appropriate text field that the database can connect to.
3. Enter the name of a Postgres database in the appropriate text field that the application can connect to.

   Nexpose attempts to verify an SID on a target asset through various methods, such as discovering common configuration errors and default guesses. You can now specify additional SIDs for verification.
4. Enter the names of Oracle SIDs in the appropriate text field, to which it can connect. Separate multiple SIDs with commas.
5. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Configuring scans of mail servers

You can configure Nexpose to scan mail servers.

To configure to scan mail servers:

1. Go to the *Mail Servers* page.
2. Type a read timeout value in the appropriate text field.

   This setting is the interval at which the application retries accessing the mail server. The default value is 30 seconds.
3. Type an inaccurate time difference value in the appropriate text field.

   This setting is a threshold outside of which the application will report inaccurate time readings by system clocks. The inaccuracy will be reported in the system log.
4. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Configuring scans of CVS servers

Nexpose tests a number of vulnerabilities in the Concurrent Versions System (CVS) code repository. For example, in versions prior to v1.11.11 of the official CVS server, it is possible for an attacker with write access to the CVSROOT/passwd file to execute arbitrary code as the cvsd process owner, which usually is root.

To configure scanning CVS servers:

1. Go to the *CVS Servers* page.
2. Enter the name of the CVS repository root directory in the text box.
3. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Configuring scans of DHCP servers

DHCP Servers provide Border Gateway Protocol (BGP) information, domain naming help, and Address Resolution Protocol (ARP) table information, which may be used to reach hosts that are

otherwise unknown. Hackers exploit vulnerabilities in these servers for address information.

To configure Nexpose to scan DHCP servers:

1. Go to the *DHCP servers* page.
2. Type a DHCP address range in the text field. The application will then target those specific servers for DHCP interrogation.
3. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Configuring scans of Telnet servers

Telnet is an unstructured protocol, with many varying implementations. This renders Telnet servers prone to yielding inaccurate scan results. You can improve scan accuracy by providing Nexpose with regular expressions.

To configure scanning of Telnet servers:

1. Go to the *Telnet Servers* page.
2. Type a character set in the appropriate text field.
3. Type a regex for a logon prompt in the appropriate text field.
4. Type a regex for a password prompt in the appropriate text field.
5. Type a regex for failed logon attempts in the appropriate text field.
6. Type a regex for questionable logon attempts in the appropriate text field.

   For more information, go to *Using regular expressions* on page 678.
7. Configure any other template settings as desired. When you have finished configuring the scan template, click **Save**.

Configuring file searches on target systems

If Nexpose gains access to an asset's file system by performing an exploit or a credentialed scan, it can search for the names of files in that system.

File name searching is useful for finding software programs that are not detected by fingerprinting. It also is a good way to verify compliance with policies in corporate environments that don't permit storage of certain types of files on workstation drives:

- copyrighted content
- confidential information, such as patient file data in the case of HIPAA compliance
- unauthorized software

The application reads the contents of these files, and it does not retrieve them. You can view the names of scanned file names in the *File and Directory Listing* pane of a scan results page.

Using other tuning options

Beyond customizing scan templates, you can do other things to improve scan performance.

Change Scan Engine deployment

Depending on bandwidth availability, adding Scan Engines can reduce scan time over all, and it can improve accuracy. Where you put Scan Engines is as important as how many you have. It's helpful to place Scan Engines on both sides of network dividing points, such as firewalls. See the topic *Distribute Scan Engines strategically* in the administrator's guide.

Edit site configuration

Tailor your site configuration to support your performance goals. Try increasing the number of sites and making sites smaller. Try pairing sites with different scan templates. Adjust your scan schedule to avoid bandwidth conflicts.

Increase resources

Resources fall into two main categories:

- Network bandwidth
- RAM and CPU capacity of hosts

If your organization has the means and ability, enhance network bandwidth. If not, find ways to reduce bandwidth conflicts when running scans.

Increasing the capacity of host computers is a little more straightforward. The *installation guide* lists minimum system requirements for installation. Your system may meet those requirements, but if you want to bump up maximum number of scan threads, you may find your host system slowing down or becoming unstable. This usually indicates memory problems.

If increasing scan threads is critical to meeting your performance goals, consider installing the 64-bit version of Nexpose. A Scan Engine running on a 64-bit operating system can use as much RAM as the operating system supports, as opposed to a maximum of approximately 4 GB on 32-bit systems. The vertical scalability of 64-bit Scan Engines significantly increases the potential number simultaneous scans that Nexpose can run.

Always keep in mind that best practices for Scan Engine placement. See the topic *Distribute Scan Engines strategically* in the administrator's guide. Bandwidth is also important to consider.

Make your environment “scan-friendly”

Any well constructed network will have effective security mechanisms in place, such as firewalls. These devices will regard Nexpose as a hostile entity and attempt to prevent it from communicating with assets that they are designed to attack.

If you can find ways to make it easier for the application to coexist with your security infrastructure—without exposing your network to risk or violating security policies—you can enhance scan speed and accuracy.

For example, when scanning Windows XP workstations, you can take a few simple measures to improve performance:

- Make the application a part of the local domain.
- Give the application the proper domain credentials.
- Configure the XP firewall to allow it to connect to Windows and perform patch-checking
- Edit the domain policy to give the application communication access to the workstations.

Open firewalls on Windows scan targets

You can open firewalls on Windows assets to allow Nexpose to perform deep scans on those targets within your network.

By default, Microsoft Windows XP SP2, Vista, Server 2003, and Server 2008 enable firewalls to block incoming TCP/IP packets. Maintaining this setting is generally a smart security practice. However, a closed firewall limits the application to discovering network assets during a scan. Opening a firewall gives it access to critical, security-related data as required for patch or compliance checks.

To find out how to open a firewall without disabling it on a Windows platform, see Microsoft’s documentation for that platform. Typically, a Windows domain administrator would perform this procedure.

Managing certificates for scanning

During scans, Nexpose checks Web sites and TLS or SSL servers for specific Root certificates to verify that these entities are validated by trusted Certificate Authorities (CAs).

The Security Console installation includes a number of preset certificates trusted by commonly used browsers from Microsoft, Google, Mozilla, and Apple. Additionally, you can import Root certificates that were expressly created by trusted CAs for targets that you want to scan.

The application reports a certificate signed by an unknown or untrusted entity as a vulnerability. A malicious party pretending to be a trusted entity can stage a man-in-the-middle attack, eavesdropping on TLS/SSL connections.

Importing custom certificates

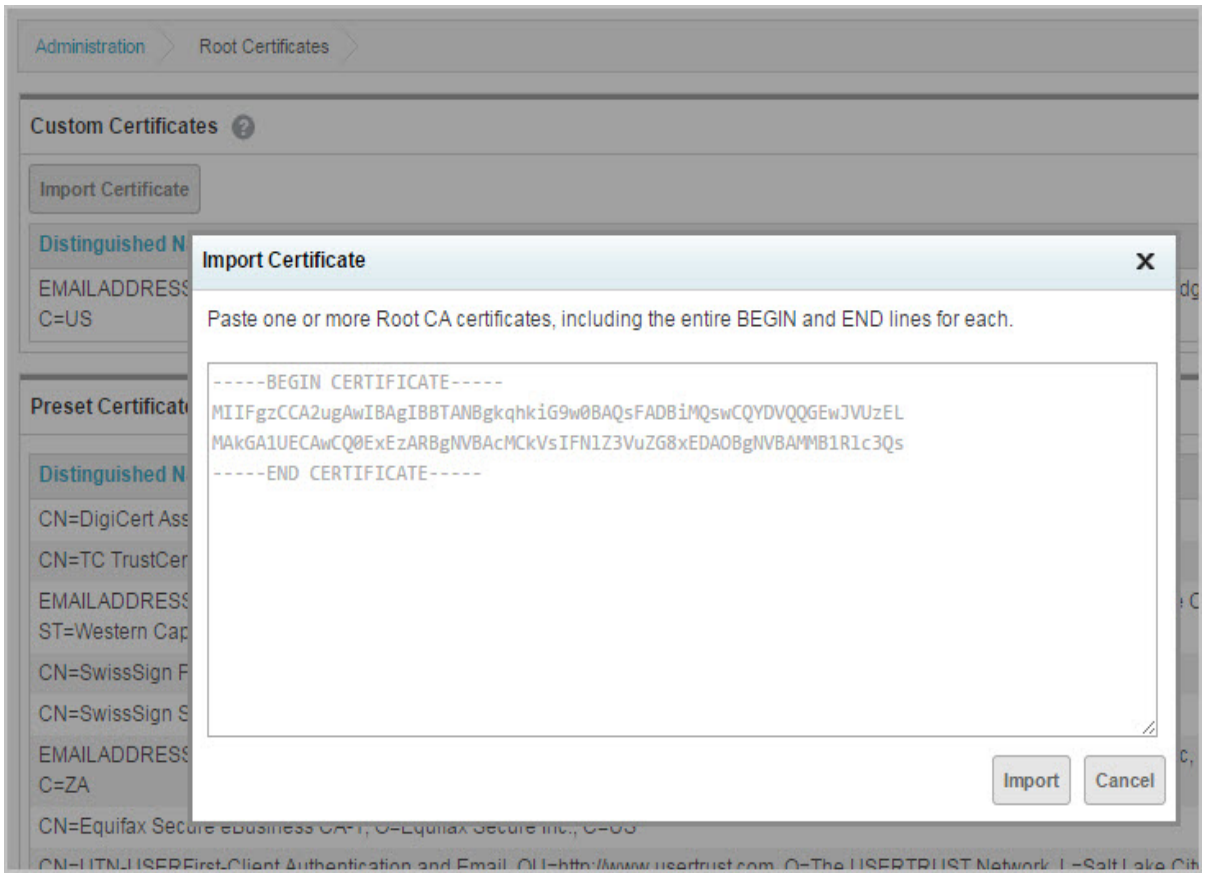
The permission required for this task is Manage Global Settings, which typically belongs to a Global Administrator.

Note: Make sure the custom certificate is a Root CA certificate. Otherwise, the full certificate chain cannot be validated during a scan. Also, the certificate must be in Privacy Enhanced Mail (PEM) base64 encoded format.

1. Open the certificate file on the computer hosting it, and copy the contents of the file, including the entire BEGIN and END lines. Example:

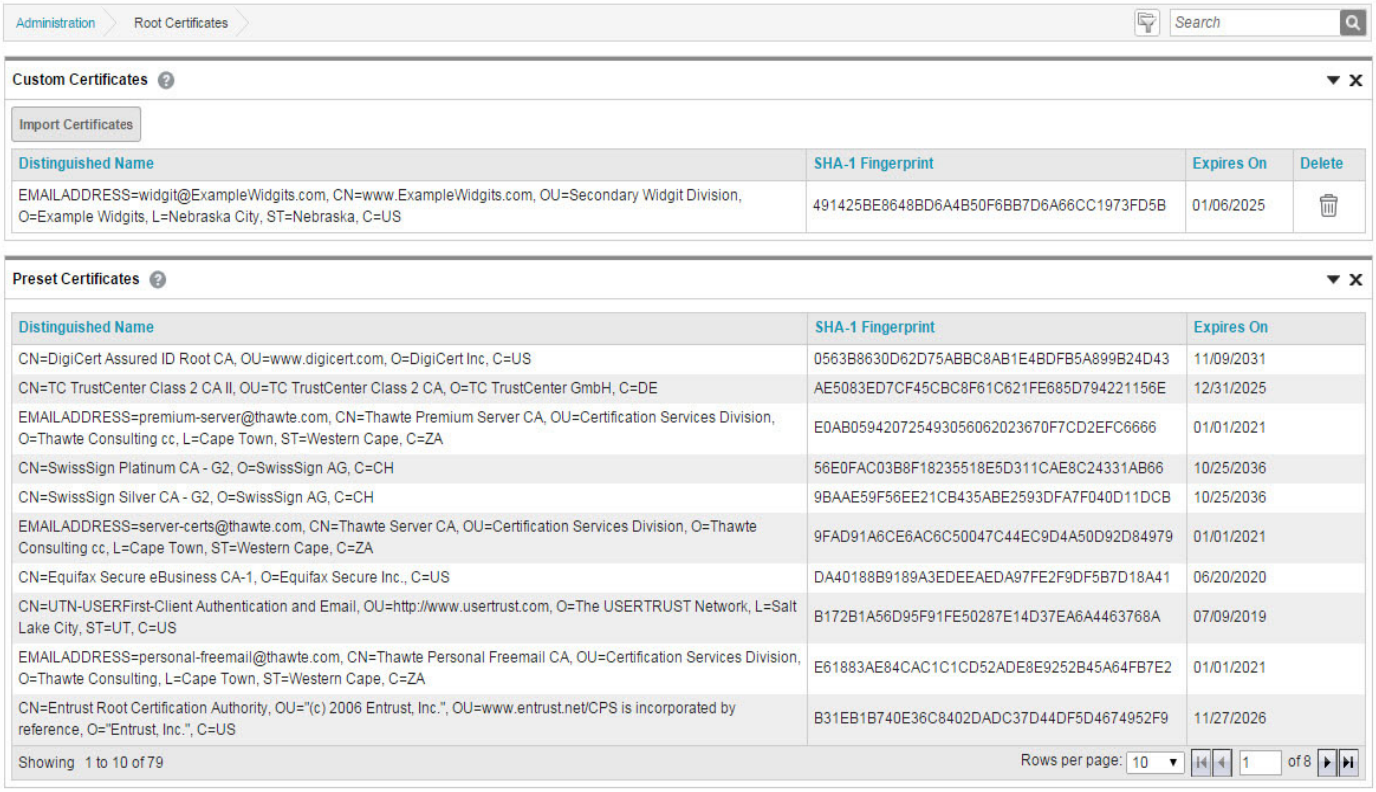
```
-----BEGIN CERTIFICATE-----
MIIHQDCCBSigAwIBAgIJAMStF8UUH6doMA0GCSqGSIb3DQEBCwUAMIHBMQswCQYD
VQQGEwJVUzERMA8GA1UECBMITmVicmFza2ExFjAUBgNVBAcTDU5lYnJhc2thIENp
-----END CERTIFICATE-----
```

2. Click the **Administration** tab in the Security Console Web interface.
3. In the *Scan Options* area of the *Administration* page, click the **Manage** link for *Root Certificates*.
4. On the *Certificates* page, click the **Import Certificates** button.
5. Paste the copied certificate into the text box and click *Import*.



The dialog box for importing a Root certificate

The certificate appears in the *Custom Certificates* table. You also can view preset certificates on the *Root Certificates* page.



The Root Certificates page

Removing certificates

Removing a root certificate from the trust store affects future scans in that any scanned certificates that were signed by the root certificate authority will no longer be trusted. They will be reported as vulnerabilities.

The permission required for removing custom certificates is *Manage Global Settings*, which typically belongs to a Global Administrator.

1. Click the **Administration** tab in the Security Console Web interface.
2. In the *Scan Options* area of the *Administration* page, click the **Manage** link for *Root Certificates*.
3. On the *Certificates* page, find the certificate you want to delete from the *Custom Certificates* table.
4. Click the **Delete** icon. The table refreshes and no longer displays the deleted certificate.

Note: You cannot delete preset certificates.

Creating a custom policy

Note: To edit policies you must have the Policy Editor license. Contact your account representative if you want to add this feature.

You create a custom policy by editing copies of built-in configuration policies or other custom policies. A policy consists of rules that may be organized within groups or sub-groups. You edit a custom policy to fit the requirements of your environment by changing the values required for compliance.

You can create a custom policy and then periodically check the settings to improve scan results or adapt to changing organizational requirements.

For example, you need a different way to present vulnerability data to show compliance percentages to your auditors. You create a custom policy to track one vulnerability to measure the risks over time and show improvements. Or you show what percentage of computers are compliant for a specific vulnerability.

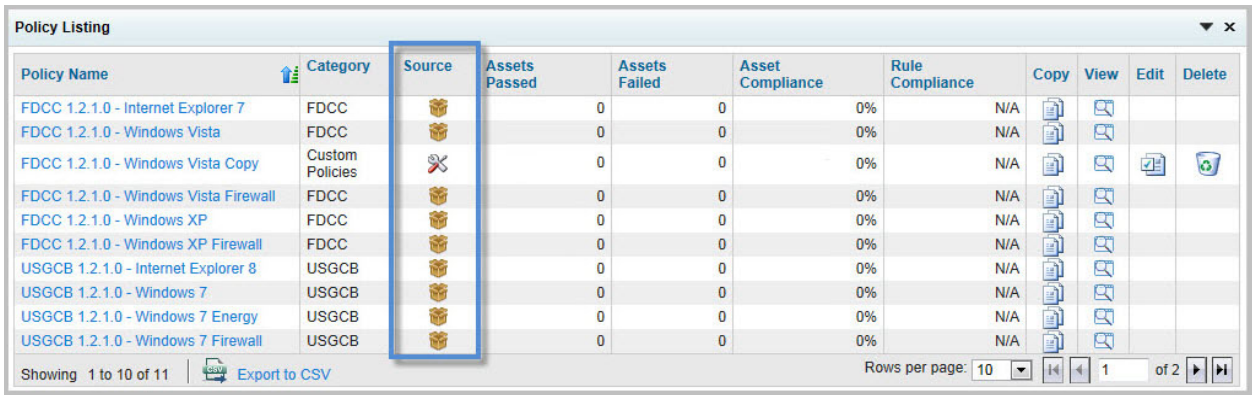
There are two policy types:

- Built-in policies are installed with the application (Policy Manager configuration policies based on USGCB, FDCC, or CIS). These policies are not editable.

  Policy Manager is a license-enabled scanning feature that performs checks for compliance with United States Government Configuration Baseline (USGCB) policies, Center for Internet Security (CIS) benchmarks, and Federal Desktop Core Configuration (FDCC) policies.

- Custom policies are editable copies of built-in policies. You can make copies of a custom policy if you need custom policies with similar changes, such as policies for different locations.

You can determine which policies are editable (custom) on the *Policy Listing* table. The *Source* column displays which policies are built-in and custom. The **Copy**, **Edit** and **Delete** buttons display for only custom policies for users with Manage Policies permission.



Policy – viewing the policy source column

Editing policies during a scan

You can edit policies during a scan without affecting your results. While you modify policies, manual or scheduled scans that are in process or paused scans that are resumed use the policy configuration settings in effect when the scan initially launched. Changes saved to a custom policy are applied during the next scheduled scan or a subsequent manual scan.

If your session times out when you try to save a policy, reestablish a session and then save your changes to the policy.

Editing a policy

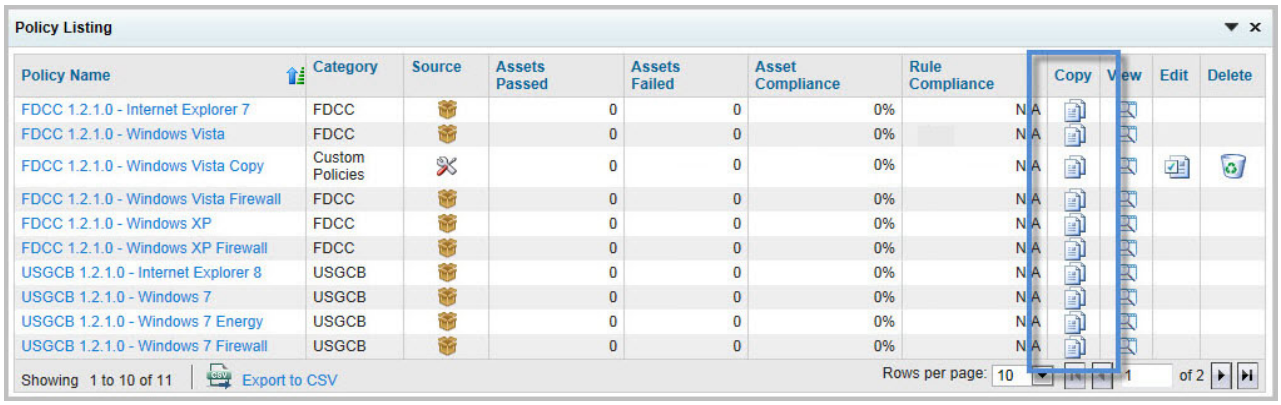
Note: To edit policies, you need Manage Policies permissions. Contact your administrator about your user permissions.

The following section demonstrates how to edit the different items in a custom policy. You can edit the following items:

- custom policy–customize name and description
- groups–customize name and description
- rules–customize name and description and modify the values for checks

To create an editable policy, complete these steps:

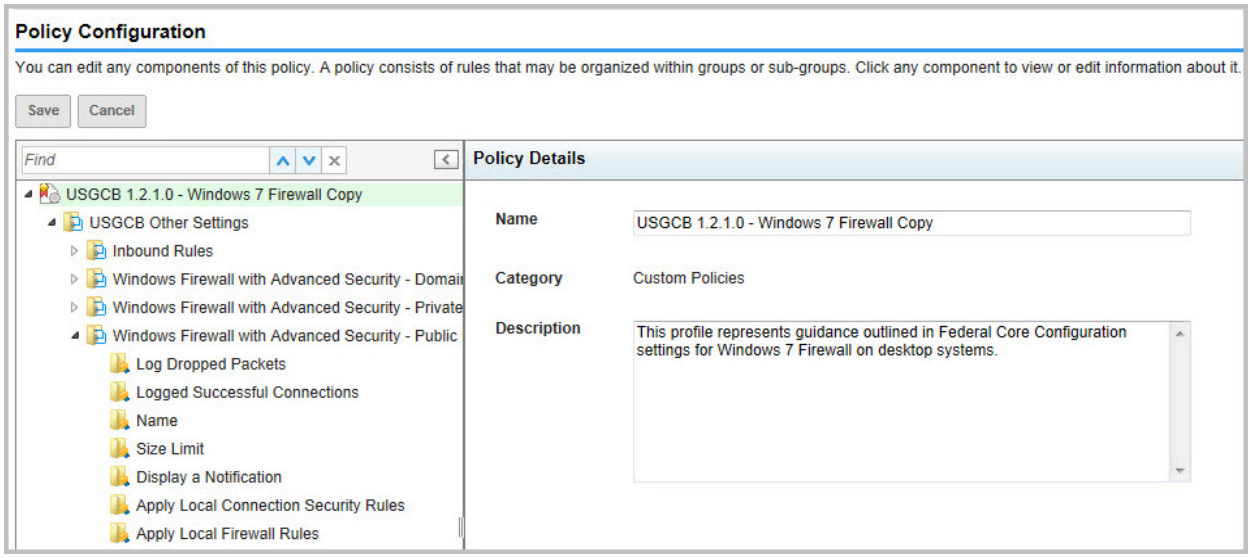
1. Click **Copy** next to a built-in or custom policy.



Policy – copying a built-in policy

The application creates a copy of the policy.

2. You can modify the *Name* to identify which policies are customized for your organization. For example, add your organization name or abbreviation, such as *XYZ Org -USGCB 1.2.1.0 - Windows 7 Firewall*.



Policy – creating a custom policy

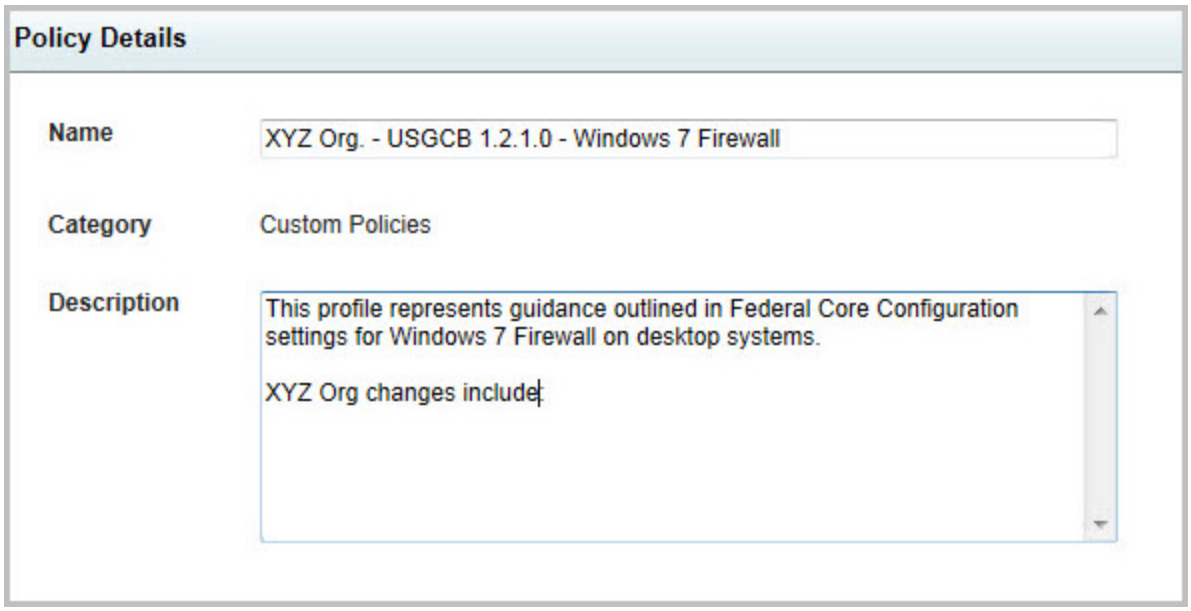
A unique ID (UID) is assigned to built-in and saved custom policies. If you use the same name for multiple policies then a UID icon (UID) displays when you save the custom policy. When you are adding policies to a scan template, refer to the UID if there are multiple policies with the same name. This helps you select the correct policy for the scan template.



Policy – viewing the UID for policies with duplicate names

Hover over the UID icon to display the unique ID for the policy.

3. (Optional) You can modify the *Description* to explain what settings are applied in the custom policy using this policy.

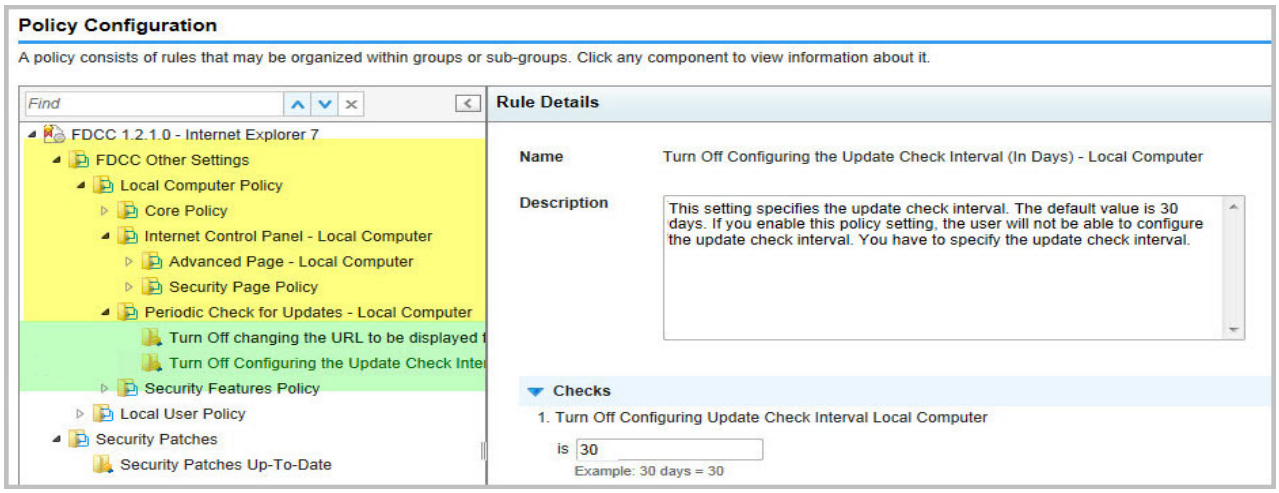


Policy Editor – editing custom policy name and description

4. Click **Save**.

Viewing policy hierarchy

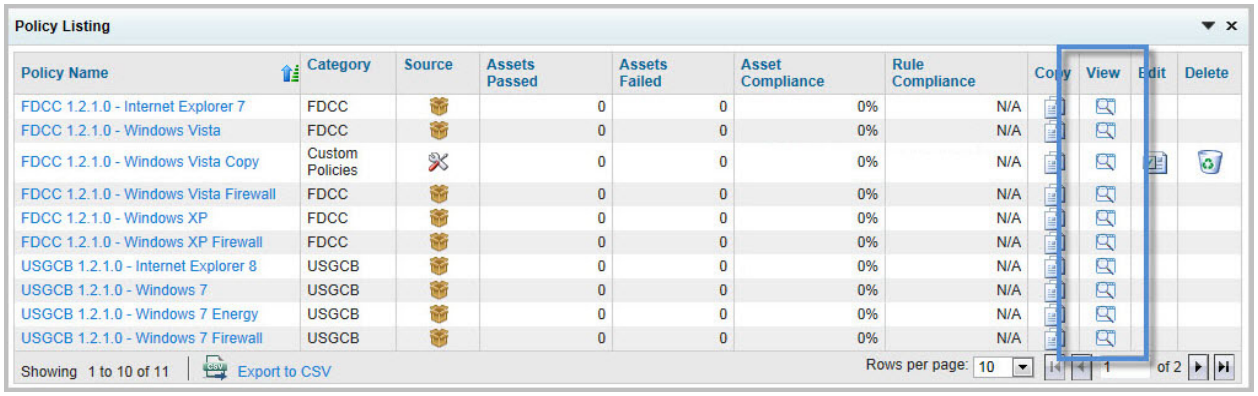
The *Policy Configuration* panel displays the groups and rules in item order for the selected policy. By opening the groups, you drill down to an individual group or rule in a policy.



Policy – viewing the policy hierarchy

To view policy hierarchy for password rules, complete these steps:

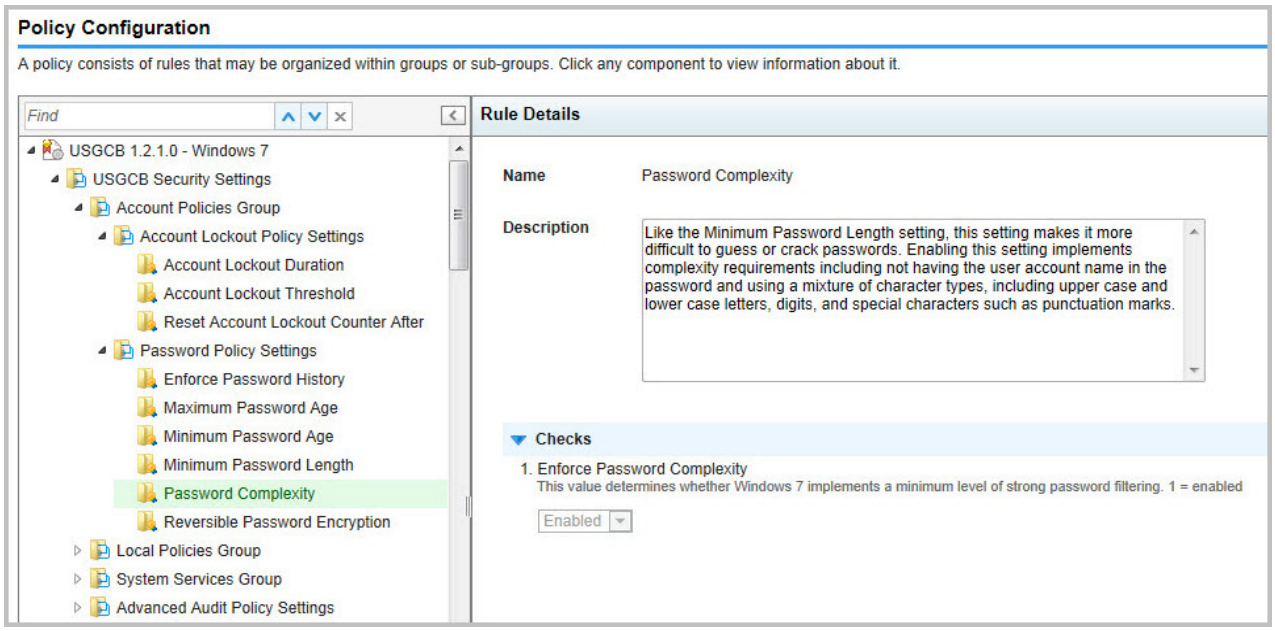
1. Click **View** on the *Policy Listing* table to display the policy configuration.



*Policy – clicking **View** to display the policy*

2. Click the icon to expand groups or rules to display details on the *Policy Configuration* panel.

   Use the policy *Find* box to locate a specific rule. See *Using policy find* on page 636.



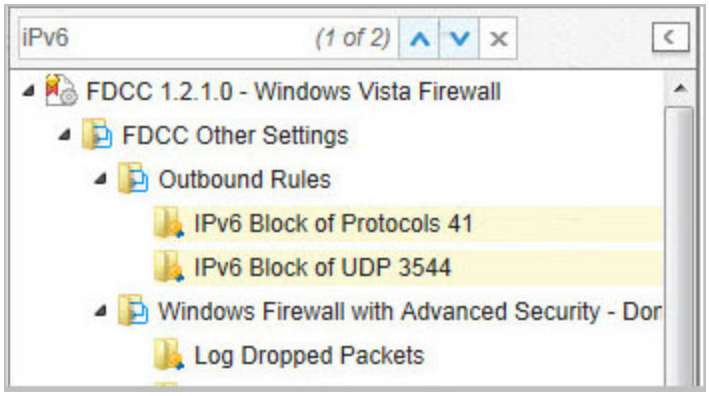
Policy – viewing the policy hierarchy

3. Select an item (rule or group) in the policy tree (hierarchy) to display the detail in the right panel.

   For example, your organization has specific requirements for password compliance. Select the Password Complexity rule to view the checks used during a scan to verify password compliance. If your organization policy does not enforce strong passwords then you can change the value to Disabled.

Using policy find

Use the policy find to quickly locate the policy item that you want to modify.



Policy – typing search criteria

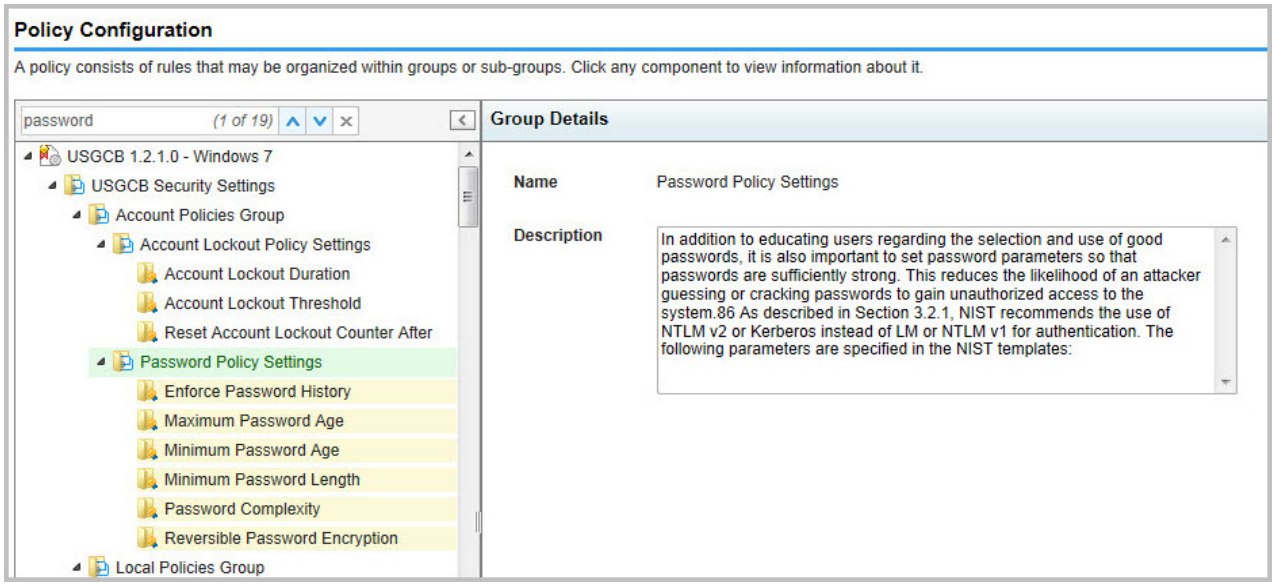
For example, type IPv6 to locate all policy items with that criteria. Click the **Up** ( ) and **Down** ( ) arrows to display the next or previous instance of IPv6 found by the policy find.

To find an item in a policy, complete these steps:

1. Type a word or phrase in the policy *Find* box.

   For example, type password.

   As you type, the application searches then highlights all matches in the policy hierarchy.

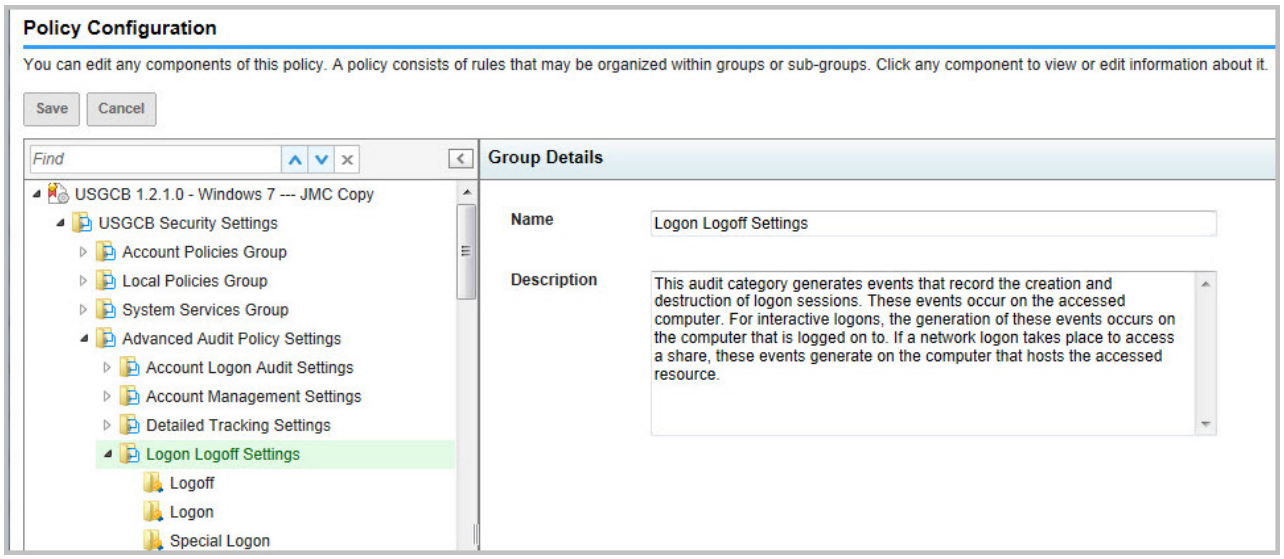


Policy – browsing find results

2. Click the **Up** ( ) and **Down** ( ) arrows to move to the next or previous items that match the find criteria.
3. (Optional) Refine your criteria if you receive too many results. For example, replace password with password age.
4. To clear the find results, click **Clear** ( ).

Editing policy groups

You modify the group *Name* and *Description* to change the description of items that you customized. The policy find uses this text to locate items in the policy hierarchy. See *Using policy find* on page 636.



Policy – editing group name or description

You select a group in the policy hierarchy to display the details. You can modify this text to identify which groups contain modified (custom) rules and add a description of what type of changes.

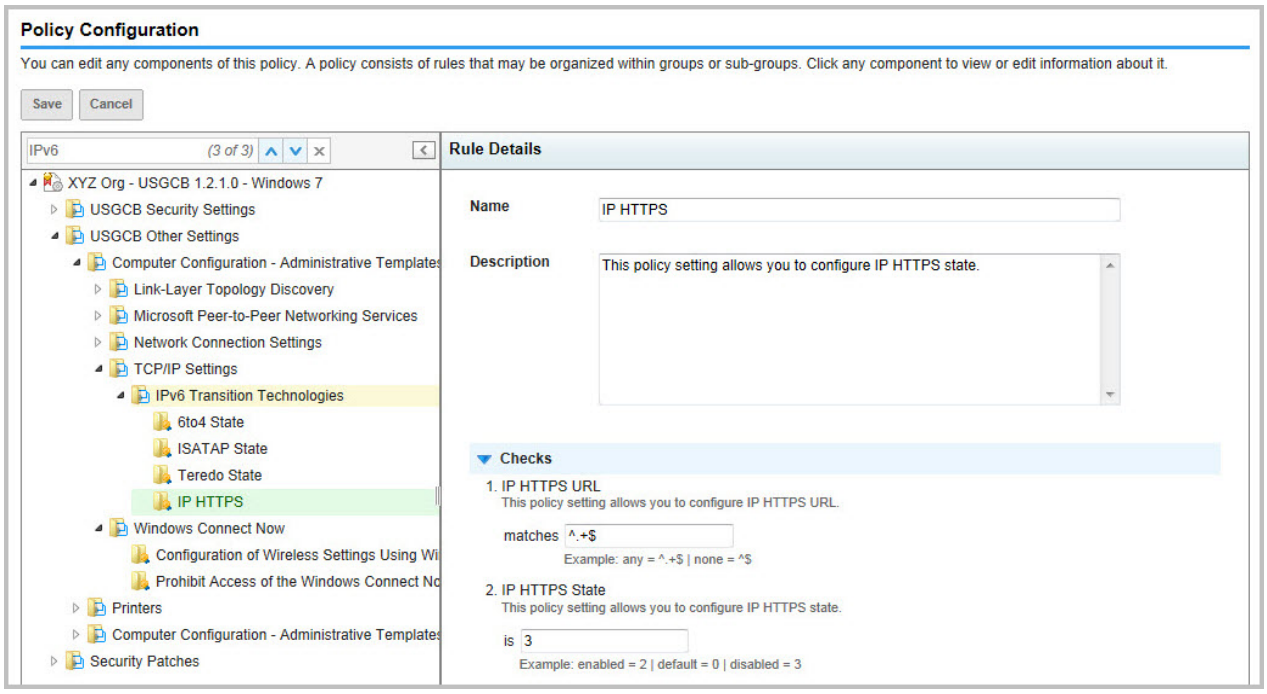
Editing policy rules

You can modify policy rules to get different scan results. You select a rule in the Policy Configuration hierarchy to see the list of editable checks and values related to that rule.

To edit a rule value, complete these steps:

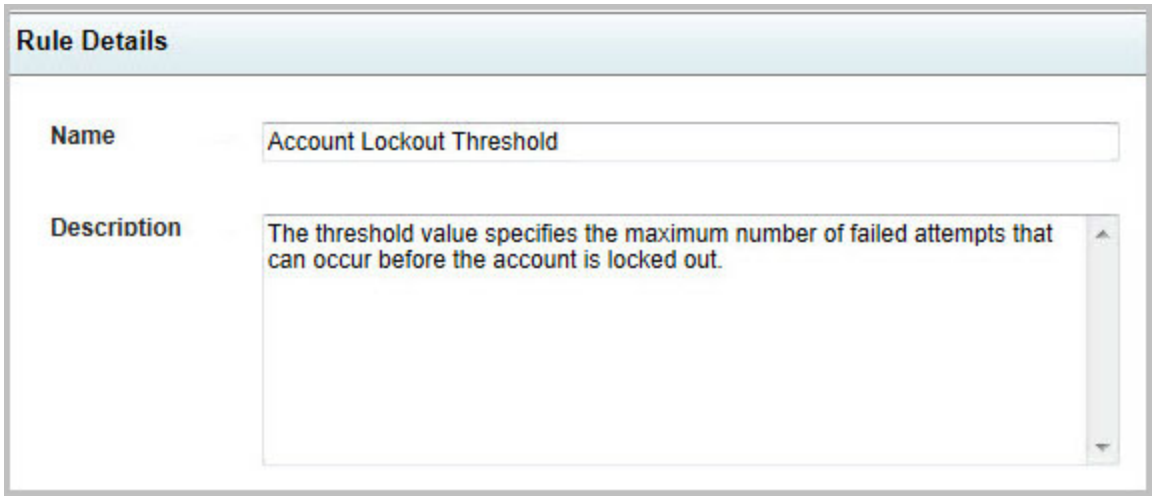
1. Select a rule in the policy hierarchy.

   The rule details display.



Policy—selecting a rule

(Optional) Customize the *Name* and *Description* for your organization. Text in the *Name* is used by policy find. See *Using policy find* on page 636.

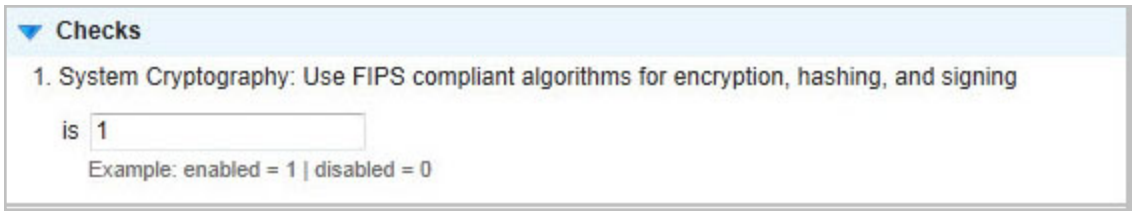


Policy—modifying rule values

2. Modify the checks for the rule using the fields displayed.

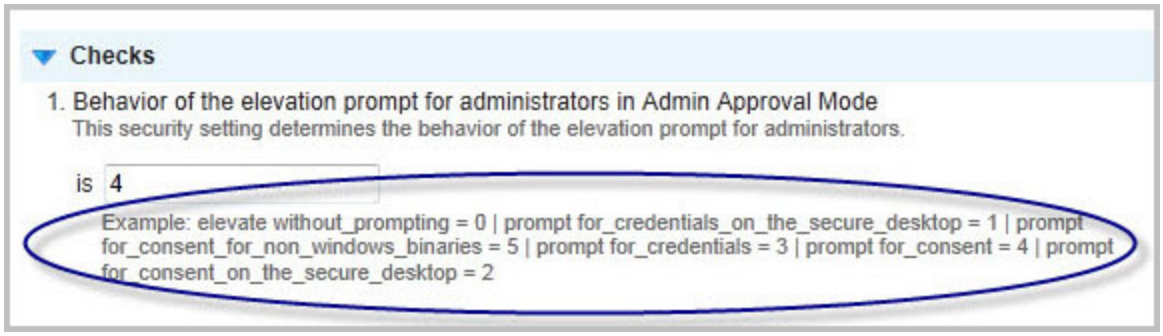
   Refer to the guidelines about what value to apply to get the correct result.

For example, disable the Use FIPS compliant algorithms for encryption, hashing and signing rule by typing '0' in the text box.



Policy – disabling a rule

For example, change the Behavior of the elevation prompt for administrators in Admin Approval Mode check by typing a value for the total seconds. The guidelines list the options for each value.



Policy – entering the value for a check option.

3. Repeat these steps to edit other rules in the policy.
4. Click **Save**.

Deleting a policy

Note: To delete policies, you need Manage Policies permissions. Contact your administrator about your user permissions.

You can remove custom policies that you no longer use. When you delete a policy, all scan data related to the policy is removed. The policy must be removed from scan templates and report configurations before deleting.

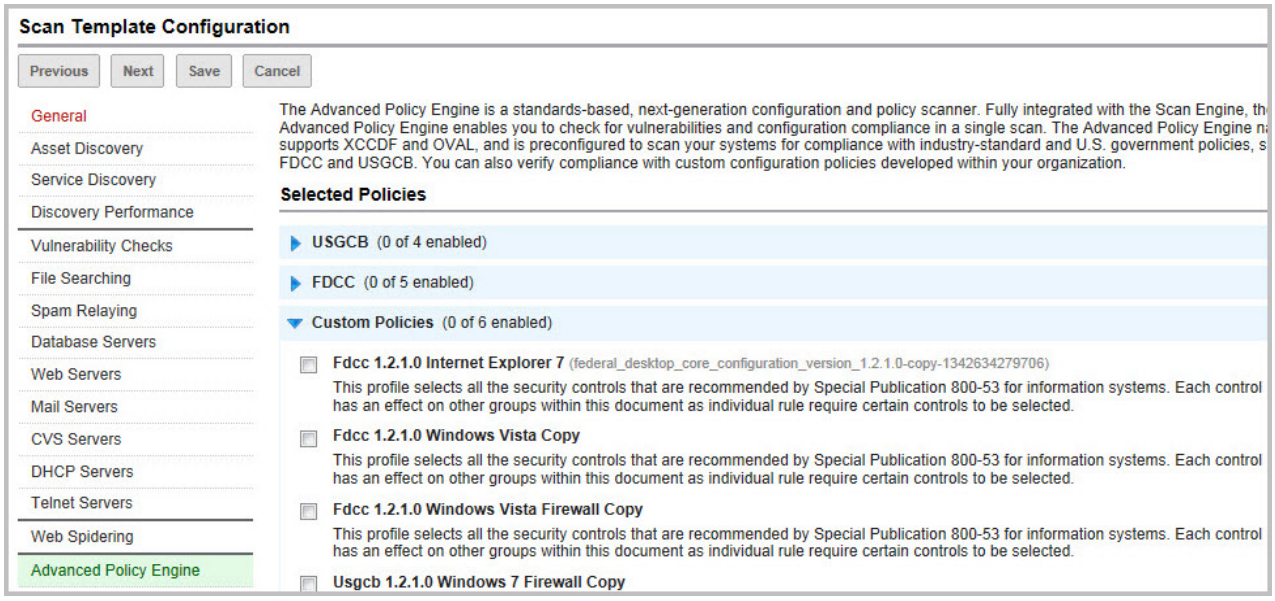
Click **Delete** for the custom policy that you want to remove.

If you try to delete a policy while running a scan, then a warning message displays indicating that the policy can not be deleted.

Adding Custom Policies in Scan Templates

Note: To perform policy checks in scans, make sure that your Scan Engines are updated to the August 8, 2012 release.

You add custom policies to the scan templates to apply your modifications across your sites. The *Policy Manager* list contains the custom policies.



Policy – enabling a custom policy in the scan template

Click *Custom Policies* to display the custom policies. Select the custom policies to add.

Uploading custom SCAP policies

There is no one-size-fits-all solution for managing configuration security. The application provides policies that you can apply to scan your environments. However, you may create custom scripts to verify items specific to your company, such as health check scripts that prioritize security settings. You can create policies from scratch, upload your custom content to use in policy scans, and run it with your other policy and vulnerability checks.

You must log on as Global Administrator to upload policies.

Note: To upload policies you must have the Policy Editor capability enabled in your license. Contact your account representative if you want to update your license.

File specifications

SCAP 1.2 datastreams and datastream collections are in XML format.

SCAP 1.0 policy files must be compressed to an archive (ZIP or JAR file format) with no folder structure. The archive can contain only XML or TXT files. If the archive contains other file types, such as CSV, then the application does not upload the policy.

The archive file must contain the following XML files:

- **XCCDF file**—This file contains the structure of the policy. It must have a unique name (title) and ID (benchmark ID). This file is required.
  The SCAP XCCDF benchmark file name must end with *-xccdf.xml* (For example, XYZ-xccdf.xml).
- **OVAL file**—These files contain policy checks. The file names must end with *-oval.xml* (For example, XYZ-oval.xml).

If unsupported OVAL check types are in the policy, the policy fails to upload. The policy files must contain supported OVAL check types, such as:

- accesstoken_test
- auditeventpolicysubcategories_test
- auditeventpolicy_test
- family_test
- fileeffectiverights53_test
- lockoutpolicy_test
- passwordpolicy_test
- registry_test
- sid_test
- unknown_test
- user_test
- variable_test

The following XML files can be included in the archive file to define specific policy information. These files are not required for a successful upload.

- **CPE files**—These files contain the Uniform Resource Identifiers (URI) that correspond to fingerprinted platforms and applications.
  The file must begin with *cpe:* and includes segments for the hardware facet, the operating system facet, and the application environment facet of the fingerprinted item (For example, cpe:/o:microsoft:windows_xp:-:sp3:professional).
- **CCE files**—These files contain CCE identifiers for known system configurations to facilitate fast and accurate correlation of configuration data across multiple information sources and tools.
- **CVE files**—These files contain CVE (Common Vulnerabilities and Exposures) identifiers to known vulnerabilities and exposures.

Version and file name conventions

You can name your custom policies to meet your company's needs. The application identifies policies by the benchmark ID and title. You must create unique names and IDs in your benchmark file to upload them successfully. The application verifies that the benchmark version to identifies a benchmark (v1.2.1.0) that is supported.

Note: The application does not upload custom policies with the same name and benchmark ID as an existing policy.

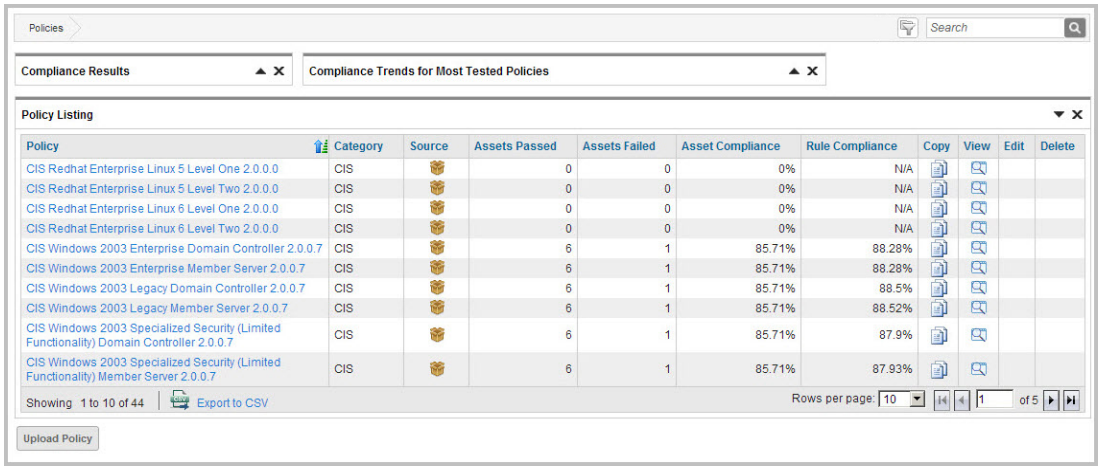
Uploading SCAP policies

Note: Custom policies uploaded to the application can be edited with the Policy Manager. See *Creating a custom policy* on page 631.

To upload a policy, complete the following steps:

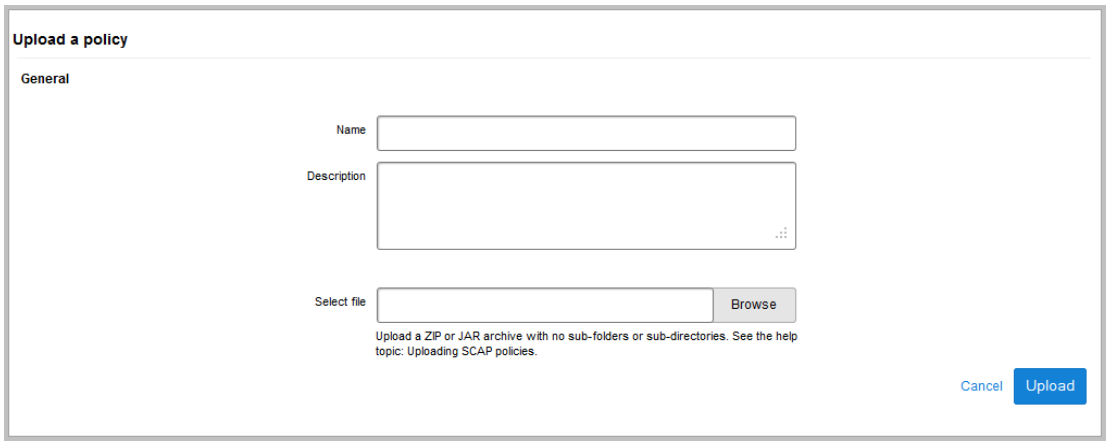
1. Click the **Policies** tab.
2. Click the **Upload Policy** button.

   If you cannot see this button then you must log on as Global Administrator.



*Clicking the **Upload Policy** button*

The system displays the *Upload a policy* panel.



Entering SCAP policy file information

3. Enter a name to identify the policy. This is a required field.

   To identify which policies are customized for your organization you can devise a file naming convention. For example, add your organization name or abbreviation, such as *XYZ Org - USGCB 1.2.1.0 - Windows 7 Firewall*.

4. Enter a description that explains what settings are applied in the custom policy.

5. Click the Browse button to locate the archive file.

6. Click the Upload button to upload the policy.
   - If the policy uploads successfully, go to step 7.
   - If you receive an error message the policy is not loaded. You must resolve the issue noted in the error message then repeat these steps until the policy loads successfully. For more information about errors, see *Troubleshooting upload errors* on page 646.

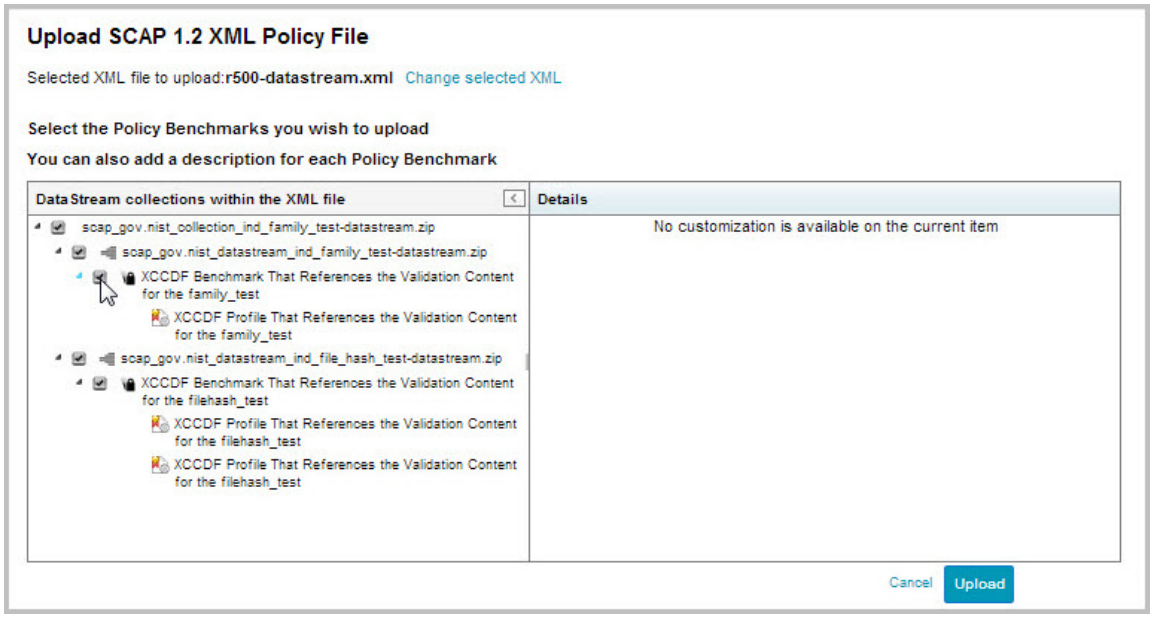
   During the upload, a "spinning" image appears:  . The time to complete the upload depends on the policy's complexity and size, which typically reflects the number of rules that it includes.

   When the upload completes, your custom policies appear in the *Policy Listing* panel on the **Policies** page. You can edit these policies using the Policy Manager. See *Creating a custom policy* on page 631.

7. Add your custom policies to the scan templates to apply to future scans. See *Selecting Policy Manager checks* on page 608.

Uploading specific benchmarks or datastreams

You can select any combination of datastream or the underlying benchmark in the following manner: Upload an SCAP 1.2 XML policy file using the steps described in *Uploading custom SCAP policies* on page 642. After you specify the XML file for upload, the Security Console displays a page for selecting individual components from the datastream collection. All components are selected by default. To prevent any component from being included, clear the check box for that component. Then, click **Upload**.



Selecting SCAP 1.2 XML components for upload

Troubleshooting upload errors

Policies are not uploaded to the application unless certain criteria are met. Error messages identify the criteria that have not been met. You must resolve the issues and upload the policy successfully to apply your custom SCAP policy to scans.

Each of the following errors (in italics) is listed with the resolution indented after it. In the error messages, *value* is a placeholder for a specific reference in the error message.

The SCAP XCCDF Benchmark file [value] cannot be parsed.
Content is not allowed in prolog.

There are characters positioned before the first bracket (<). For example:

- abc<?xml version="1.0" encoding="UTF-8">
- There are hidden characters at the beginning of the SCAP XCCDF benchmark file. The following items are hidden characters:
    - White space
    - Byte Order Mark character in UTF8 encoded XML file, that is caused by text editors like Microsoft® Notepad.
    - Any other type of invisible characters.
- Use a hex editor to remove the hidden characters.
- There is a mismatch in the encoding declaration and the SCAP XCCDF benchmark file. For example, there is a UTF8 declaration for a UTF16 XML file.
- The SCAP XCCDF benchmark file contains unsupported character encoding.
- If the XML encoding declaration is missing then it will default to the server's default encoding. If the XML content contains characters that are not supported by the default character encoding then the SCAP XCCDF benchmark file cannot be parsed.

  Add a UTF8 declaration to the SCAP XCCDF benchmark file.

The SCAP XCCDF Benchmark file cannot be found. Verify that the SCAP XCCDF benchmark file name ends in "-xccdf.xml" and is not under a folder in the archive.

The application cannot find the SCAP XCCDF benchmark file in the archive.

The SCAP XCCDF benchmark file name must end with -xccdf.xml (For example, XYZ-xccdf.xml). The archive (ZIP or JAR) cannot have a folder structure.

Verify that the SCAP XCCDF benchmark file exists in the archive using the required naming convention.

The SCAP XCCDF Benchmark version could not be found in [value].

The SCAP XCCDF benchmark file must contain a valid schema version.

Add the schema version (SCAP policy) to the SCAP XCCDF benchmark file.

The SCAP XCCDF Benchmark version [value] is unsupported.

The SCAP XCCDF benchmark file must contain a version in supported format (for example, 1.1.4). The application currently supports version 1.1.4 or earlier.

Replace the version number using a valid format. Verify that there are no blank spaces.

The SCAP XCCDF Benchmark file must contain an ID for the Benchmark to be uploaded.

The SCAP XCCDF benchmark file must contain a benchmark ID.

Add a benchmark ID to the SCAP XCCDF benchmark file.

The SCAP XCCDF Benchmark file [value] contains a Benchmark ID that contains an invalid character: [value]. The Benchmark cannot be uploaded.

The benchmark ID has an invalid character, such as a blank space.

Replace the benchmark ID using a valid format.

The SCAP XCCDF Benchmark file [value] contains a reference to an OVAL definition file [value] that is not included in the archive.

Verify that the archive file contains all policy definition files referenced in the SCAP XCCDF benchmark file. Or remove the reference to the missing definition file.

The SCAP XCCDF Benchmark file [value] contains a test [value] that is not supported within the product. The test must be removed for the policy to be uploaded.

The SCAP XCCDF benchmark file includes a test that the application does not support.

Remove the test from the SCAP XCCDF benchmark file .

The uploaded archive is not a valid zip or jar archive.

The format of the archive is invalid.

The archive (ZIP or JAR) cannot have a folder structure.

Compress your policy files to an archive (ZIP or JAR) with no folder structure.

The SCAP XCCDF Benchmark file contains a rule [value] that refers to a check system that is not supported. Please only use OVAL check systems.

There are unsupported items (such as OVAL check types).

Remove the unsupported items from the SCAP XCCDF benchmark file.

The item [value] is not a XCCDF Benchmark or Group. Only XCCDF Benchmarks or Groups can contain other items.

Revise the SCAP XCCDF benchmark file. so only benchmarks or groups contain other benchmark items.

The SCAP XCCDF item [value] requires a group or rule [value] to be enabled that is not present in the Benchmark and cannot be uploaded.

A requirement in the SCAP XCCDF benchmark file is missing a reference to a group or rule.

Review the requirement specified in the error message to determine what group or rule to add.

The SCAP XCCDF item [value] requires a group or rule [value] to not be enabled that is not present in the Benchmark and cannot be uploaded.

A conflict in the SCAP XCCDF benchmark file is referencing an item that is not recognized or is the wrong item.

Review the conflict specified in the error message to determine which item to replace.

The SCAP XCCDF item [value] requires a group or rule [value] to not be enabled, but the item reference is neither a group or rule. The Benchmark cannot be uploaded.

A conflict in the SCAP XCCDF benchmark file is missing a reference to a group or rule.

Review the conflict specified in the error message to determine what group or rule to add.

The SCAP XCCDF Benchmark contains two profiles with the same Profile ID [value]. This is illegal and the Benchmark cannot be uploaded.

There are two profiles in the SCAP XCCDF benchmark file that have the same ID.

Revise the SCAP XCCDF benchmark file so that each <profile> has a unique ID.

The SCAP XCCDF Benchmark contains a value [value] that does not have a default value set. The value [value] must have a default value defined if there is no selector tag. The Benchmark failed to upload.

A default selection must be included for items with multiple options for an element, such as a rule.

If the item has multiple options that can be selected then you must specify the default option.

The SCAP XCCDF Benchmark [value] contains reference to a CPE platform [value] that is not referenced in the CPE Dictionary. The SCAP XCCDF Benchmark cannot be uploaded.

The application does not recognize CPE platform reference in the SCAP XCCDF benchmark file.

Remove the CPE platform reference from the SCAP XCCDF benchmark file.

The SCAP XCCDF Benchmark file [value] contains an infinite loop and is illegal. The Benchmark cannot be uploaded.

Review the SCAP XCCDF benchmark file to locate the infinite loop and revise the code to correct this error.

The SCAP XCCDF Benchmark file [value] contains an item that attempts to extend another item that does not exist, or is an illegal extension. The Benchmark cannot be uploaded.

There is an item referenced in the SCAP XCCDF benchmark file that is not included in the Benchmark.

Revise the SCAP XCCDF benchmark file to remove the reference to the missing item or add the item to the Benchmark.

The referenced check [value] in [value] is invalid or missing.

There is an check referenced in the SCAP XCCDF benchmark file that is not included in the Benchmark.

Revise the SCAP XCCDF benchmark file to remove the reference to the missing check or add the check to the Benchmark.

[value] benchmark files were found within the archive, you can only upload one benchmark at a time.

The archive must contain only one benchmark or it cannot be uploaded.

Create a separate archive for each benchmark and upload each archive to the application.

The SCAP XCCDF Benchmark Value [value] cannot be created within the policy [value].

The application cannot resolve the value within the policy.

Review the benchmark and revise the value.

The SCAP XCCDF Benchmark file [value] cannot be parsed.
[value]

The SCAP XCCDF benchmark file cannot be parsed due to the issue indicated at the end of the error message.

The SCAP XCCDF item [value] does not reference a valid value [value] and the Benchmark cannot be parsed.

A requirement in the SCAP XCCDF benchmark file is referencing an item that is not recognized or is the wrong item.

Review the requirement specified in the error message to determine which item to replace.

The SCAP XCCDF Benchmark file contains a XCCDF Value [value] that has no value provided. The Benchmark cannot be parsed.

Add a value to XCCDF value reference in the SCAP XCCDF benchmark file.

The SCAP OVAL file [value] cannot be parsed.
[value]

This parsing error identifies the issue preventing the SCAP OVAL file from loading.

Review the SCAP OVAL file and located the issue listed in the error message to determine the appropriate revision.

The SCAP OVAL Source file [value] could not be found.

The application cannot find the SCAP OVAL Source file in the archive. This file must end with -oval.xml or -patches.xml.

Verify that the SCAP OVAL Source file exists in the archive and the file name ends in the correct format.

Working with risk strategies to analyze threats

One of the biggest challenges to keeping your environment secure is prioritizing remediation of vulnerabilities. If Nexpose discovers hundreds or even thousands of vulnerabilities with each scan, how do you determine which vulnerabilities or assets to address first?

Each vulnerability has a number of characteristics that indicate how easy it is to exploit and what an attacker can do to your environment after performing an exploit. These characteristics make up the vulnerability's risk to your organization.

Every asset also has risk associated with it, based on how sensitive it is to your organization's security. For example, if a database that contains credit card numbers is compromised, the damage to your organization will be significantly greater than if a printer server is compromised.

The application provides several strategies for calculating risk. Each strategy emphasizes certain characteristics, allowing you to analyze risk according to your organization's unique security needs or objectives. You can also create custom strategies and integrate them with the application.

After you select a risk strategy you can use it in the following ways:

- Sort how vulnerabilities appear in Web interface tables according to risk. By sorting vulnerabilities you can make a quick visual determination as to which vulnerabilities need your immediate attention and which are less critical.
- View risk trends over time in reports, which allows you to track progress in your remediation effort or determine whether risk is increasing or decreasing over time in different segments of your network.

Working with risk strategies involves the following activities:

- *Changing your risk strategy and recalculating past scan data* on page 658
- *Using custom risk strategies* on page 660
- *Changing the appearance order of risk strategies* on page 662

Comparing risk strategies

- *Real Risk strategy* on page 656
- *TemporalPlus strategy* on page 656
- *Temporal strategy* on page 657
- *Weighted strategy* on page 657
- *PCI ASV 2.0 Risk strategy* on page 658

Each risk strategy is based on a formula in which factors such as likelihood of compromise, impact of compromise, and asset importance are calculated. Each formula produces a different range of numeric values. For example, the Real Risk strategy produces a maximum score of 1,000, while the Temporal strategy has no upper bounds, with some high-risk vulnerability scores reaching the hundred thousands. This is important to keep in mind if you apply different risk strategies to different segments of scan data. See *Changing your risk strategy and recalculating past scan data* on page 658.

Many of the available risk strategies use the same factors in assessing risk, each strategy evaluating and aggregating the relevant factors in different ways. The common risk factors are grouped into three categories: vulnerability impact, initial exploit difficulty, and threat exposure. The factors that comprise vulnerability impact and initial exploit difficulty are the six base metrics employed in the Common Vulnerability Scoring System (CVSS).

- Vulnerability impact is a measure of what can be compromised on an asset when attacking it through the vulnerability, and the degree of that compromise. Impact is comprised of three factors:
- *Confidentiality impact* indicates the disclosure of data to unauthorized individuals or systems.
- *Integrity impact* indicates unauthorized data modification.
- *Availability impact* indicates loss of access to an asset's data.
- Initial exploit difficulty is a measure of likelihood of a successful attack through the vulnerability, and is comprised of three factors:
- *Access vector* indicates how close an attacker needs to be to an asset in order to exploit the vulnerability. If the attacker must have local access, the risk level is low. Lesser required proximity maps to higher risk.
- *Access complexity* is the likelihood of exploit based on the ease or difficulty of perpetrating the exploit, both in terms of the skill required and the circumstances which must exist in order for the exploit to be feasible. Lower access complexity maps to higher risk.
- *Authentication requirement* is the likelihood of exploit based on the number of times an attacker must authenticate in order to exploit the vulnerability. Fewer required authentications map to higher risk.
- Threat exposure includes three variables:
- *Vulnerability age* is a measure of how long the security community has known about the vulnerability. The longer a vulnerability has been known to exist, the more likely that the threat community has devised a means of exploiting it and the more likely an asset will encounter an attack that targets the vulnerability. Older vulnerability age maps to higher risk.
- *Exploit exposure* is the rank of the highest-ranked exploit for a vulnerability, according to the Metasploit Framework. This ranking measures how easily and consistently a known exploit can compromise a vulnerable asset. Higher exploit exposure maps to higher risk.

- *Malware exposure* is a measure of the prevalence of any malware kits, also known as exploit kits, associated with a vulnerability. Developers create such kits to make it easier for attackers to write and deploy malicious code for attacking targets through the associated vulnerabilities.

Review the summary of each model before making a selection.

Real Risk strategy

This strategy is recommended because you can use it to prioritize remediation for vulnerabilities for which exploits or malware kits have been developed. A security hole that exposes your environment to an unsophisticated exploit or an infection developed with a widely accessible malware kit is likely to require your immediate attention. The Real Risk algorithm applies unique exploit and malware exposure metrics for each vulnerability to CVSS base metrics for likelihood and impact.

Specifically, the model computes a maximum impact between 0 and 1,000 based on the confidentiality impact, integrity impact, and availability impact of the vulnerability. The impact is multiplied by a likelihood factor that is a fraction always less than 1. The likelihood factor has an initial value that is based on the vulnerability's initial exploit difficulty metrics from CVSS: access vector, access complexity, and authentication requirement. The likelihood is modified by threat exposure: likelihood matures with the vulnerability's age, growing ever closer to 1 over time. The rate at which the likelihood matures over time is based on exploit exposure and malware exposure. A vulnerability's risk will never mature beyond the maximum impact dictated by its CVSS impact metrics.

The Real Risk strategy can be summarized as base impact, modified by initial likelihood of compromise, modified by maturity of threat exposure over time. The highest possible Real Risk score is 1,000.

TemporalPlus strategy

Like the Temporal strategy, TemporalPlus emphasizes the length of time that the vulnerability has been known to exist. However, it provides a more granular analysis of vulnerability impact by expanding the risk contribution of partial impact vectors.

The TemporalPlus risk strategy aggregates proximity-based impact of the vulnerability, using confidentiality impact, integrity impact, and availability impact in conjunction with access vector. The impact is tempered by an aggregation of the exploit difficulty metrics, which are access complexity and authentication requirement. The risk then grows over time with the vulnerability age.

The TemporalPlus strategy has no upper bounds. Some high-risk vulnerability scores reaching the hundred thousands.

This strategy distinguishes risk associated with vulnerabilities with “partial” impact values from risk associated with vulnerabilities with “none” impact values for the same vectors. This is especially important to keep in mind if you switch to TemporalPlus from the Temporal strategy, which treats them equally. Making this switch will increase the risk scores for many vulnerabilities already detected in your environment.

Temporal strategy

This strategy emphasizes the length of time that the vulnerability has been known to exist, so it could be useful for prioritizing older vulnerabilities for remediation. Older vulnerabilities are regarded as likelier to be exploited because attackers have known about them for a longer period of time. Also, the longer a vulnerability has been in an existence, the greater the chance that less commonly known exploits exist.

The Temporal risk strategy aggregates proximity-based impact of the vulnerability, using confidentiality impact, integrity impact, and availability impact in conjunction with access vector. The impact is tempered by dividing by an aggregation of the exploit difficulty metrics, which are access complexity and authentication requirement. The risk then grows over time with the vulnerability age.

The Temporal strategy has no upper bounds. Some high-risk vulnerability scores reach the hundred thousands.

Weighted strategy

The Weighted strategy can be useful if you assign levels of importance to sites or if you want to assess risk associated with services running on target assets. The strategy is based primarily on site importance, asset data, and vulnerability types, and it emphasizes the following factors:

- vulnerability severity, which is the number—ranging from 1 to 10—that the application calculates for each vulnerability
- number of vulnerability instances
- number and types of services on the asset; for example, a database has higher business value
- the level of importance, or weight, that you assign to a site when you configure it; see *Configuring a dynamic site* on page 200 or *Getting started: Info & Security* on page 61.
- Weighted risk scores scale with the number of vulnerabilities. A higher number of vulnerabilities on an asset means a higher risk score. The score is expressed in single- or double-digit numbers with decimals.

PCI ASV 2.0 Risk strategy

The PCI ASV 2.0 Risk strategy applies a score based on the Payment Card Industry Data Security Standard (PCI DSS) Version 2.0 to every discovered vulnerability. The scale ranges from 1 (lowest severity) to 5 (highest severity). With this model, Approved Scan Vendors (ASVs) and other users can assess risk from a PCI perspective by sorting vulnerabilities based on PCI 2.0 scores and viewing these scores in PCI reports. Also, the five-point severity scale provides a simple way for your organization to assess risk at a glance.

Changing your risk strategy and recalculating past scan data

You may choose to change the current risk strategy to get a different perspective on the risk in your environment. Because making this change could cause future scans to show risk scores that are significantly different from those of past scans, you also have the option to recalculate risk scores for past scan data.

Doing so provides continuity in risk tracking over time. If you are creating reports with risk trend charts, you can recalculate scores for a specific scan date range to make those scores consistent with scores for future scans. This ensures continuity in your risk trend reporting.

For example, you may change your risk strategy from Temporal to Real Risk on December 1 to do exposure-based risk analysis. You may want to demonstrate to management in your organization that investment in resources for remediation at the end of the first quarter of the year has had a positive impact on risk mitigation. So, when you select Real Risk as your strategy, you will want to calculate Real Risk scores for all scan data since April 1.

Calculation time varies. Depending on the amount of scan data that is being recalculated, the process may take hours. You cannot cancel a recalculation that is in progress.

Note: You can perform regular activities, such as scanning and reporting while a recalculation is in progress. However, if you run a report that incorporates risk scores during a recalculation, the scores may appear to be inconsistent. The report may incorporate scores from the previously used risk strategy as well as from the newly selected one.

To change your risk strategy and recalculate past scan data, take the following steps:

Go to the *Risk Strategies* page.

1. Click the **Administration** tab in the Security Console Web interface.

   The console displays the *Administration* page.

2. Click **Manage** for *Global Settings*.

The Security Console displays the *Global Settings* panel.

3. Click **Risk Strategy** in the left navigation pane.

   The Security Console displays the *Risk Strategies* page

Select a new risk strategy.

1. Click the arrow for any risk strategy on the *Risk Strategies* page to view information about it.

   Information includes a description of the strategy and its calculated factors, the strategy's source (built-in or custom), and how long it has been in use if it is the currently selected strategy.

2. Click the radio button for the desired risk strategy.

3. Select **Do not recalculate** if you do not want to recalculate scores for past scan data.

4. Click **Save**. You can ignore the following steps.

(*Optional*) View risk strategy usage history.

This allows you to see how different risk strategies have been applied to all of your scan data. This information can help you decide exactly how much scan data you need to recalculate to prevent gaps in consistency for risk trends. It also is useful for determining why segments of risk trend data appear inconsistent.

1. Click **Usage history** on the *Risk Strategies* page.

2. Click the **Current Usage** tab in the *Risk Strategy Usage* box to view all the risk strategies that are currently applied to your entire scan data set.

   Note the *Status* column, which indicates whether any calculations did not complete successfully. This could help you troubleshoot inconsistent sections in your risk trend data by running the calculations again.

3. Click the *Change Audit* tab to view every modification of risk strategy usage in the history of your installation.

   The table in this section lists every instance that a different risk strategy was applied, the affected date range, and the user who made the change. This information may also be useful for troubleshooting risk trend inconsistencies or for other purposes.

4. (Optional) Click the **Export to CSV** icon to export the change audit information to CSV format, which you can use in a spreadsheet for internal purposes.

Recalculate risk scores for past scan data.

1. Click the radio button for the date range of scan data that you want to recalculate. If you select **Entire history**, the scores for all of your data since your first scan will be recalculated.
2. Click **Save**.

   The console displays a box indicating the percentage of recalculation completed.

Using custom risk strategies

You may want to calculate risk scores with a custom strategy that analyzes risk from perspectives that are very specific to your organization's security goals. You can create a custom strategy and use it in Nexpose.

Each risk strategy is an XML document. It requires the *RiskModel* element, which contains the *id* attribute, a unique internal identifier for the custom strategy.

RiskModel contains the following required sub-elements.

- *name*: This is the name of the strategy as it will appear in the *Risk Strategies* page of the Web interface. The datatype is xs:string.
- *description*: This is the description of the strategy as it will appear in the *Risk Strategies* page of the Web interface. The datatype is xs:string.

Note: The Rapid7 Professional Services Organization (PSO) offers custom risk scoring development. For more information, contact your account manager.

- *VulnerabilityRiskStrategy*: This sub-element contains the mathematical formula for the strategy. It is recommended that you refer to the XML files of the built-in strategies as models for the structure and content of the VulnerabilityRiskStrategy sub-element.

A custom risk strategy XML file contains the following structure:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<RiskModel id="custom_risk_strategy">
```

```
        <name>Primary custom risk strategy</name>
    <description>
        This custom risk strategy emphasizes a number of important factors.
    </description>
    <VulnerabilityRiskStrategy>
        [formula]
    </VulnerabilityRiskStrategy>
</RiskModel>
```

Note: Make sure that your custom strategy XML file is well-formed and contains all required elements to ensure that the application performs as expected.

To make a custom risk strategy available in Nexpose, take the following steps:

1. Copy your custom XML file into the directory

   [installation_directory]/shared/riskStrategies/custom/global.

2. Restart the Security Console.

The custom strategy appears at the top of the list on the *Risk Strategies* page.

Setting the appearance order for a risk strategy

To set the order for a risk strategy, add the optional order sub-element with a number greater than 0 specified, as in the following example. Specifying a 0 would cause the strategy to appear last.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<RiskModel id="janes_risk_strategy">
   <name>Jane's custom risk strategy</name>
    <description>
    Jane's custom risk strategy emphasizes factors important to Jane.
    </description>
```

```
    <order>1</order>
    <VulnerabilityRiskStrategy>
        [formula]
    </VulnerabilityRiskStrategy>
</RiskModel>
```

To set the appearance order:

1. Open the desired risk strategy XML file, which appears in one of the following directories:

- for a custom strategy: [installation_directory]/shared/riskStrategies/custom/global
- for a built-in strategy: [installation_directory]/shared/riskStrategies/builtin

3. Add the *order* sub-element with a specified numeral to the file, as in the preceding example.
4. Save and close the file.
5. Restart the Security Console.

Changing the appearance order of risk strategies

You can change the order of how risk strategies are listed on the *Risk Strategies* page. This could be useful if you have many strategies listed and you want the most frequently used ones listed near the top. To change the order, you assign an order number to each individual strategy using the optional *order* element in the risk strategy's XML file. This is a sub-element of the *RiskModel* element. See *Using custom risk strategies* on page 660.

For example: Three people in your organization create custom risk strategies: *Jane's Risk Strategy*, *Tim's Risk Strategy*, and *Terry's Risk Strategy*. You can assign each strategy an order number. You can also assign order numbers to built-in risk strategies.

A resulting order of appearance might be the following:

- *Jane's Risk Strategy* (1)
- *Tim's Risk Strategy* (2)
- *Terry's Risk Strategy* (3)
- Real Risk (4)
- TemporalPlus (5)
- Temporal (6)
- Weighted (7)

Note: The order of built-in strategies will be reset to the default order with every product update.

Custom strategies always appear above built-in strategies. So, if you assign the same number to a custom strategy and a built-in strategy, or even if you assign a lower number to a built-in strategy, custom strategies always appear first.

If you do not assign a number to a risk strategy, it will appear at the bottom in its respective group (custom or built-in). In the following sample order, one custom strategy and two built-in strategies are numbered 1.

One custom strategy and one built-in strategy are not numbered:

- *Jane's Risk Strategy* (1)
- *Tim's Risk Strategy* (2)
- *Terry's Risk Strategy* (no number assigned)
- Weighted (1)
- Real Risk (1)
- TemporalPlus (2)
- Temporal (no number assigned)

Note that a custom strategy, *Tim's*, has a higher number than two numbered, built-in strategies; yet it appears above them.

Understanding how risk scoring works with scans

An asset goes through several phases of scanning before it has a status of *completed* for that scan. An asset that has not gone through all the required scan phases has a status of *in progress*. Nexpose only calculates risk scores based on data from assets with *completed* scan status.

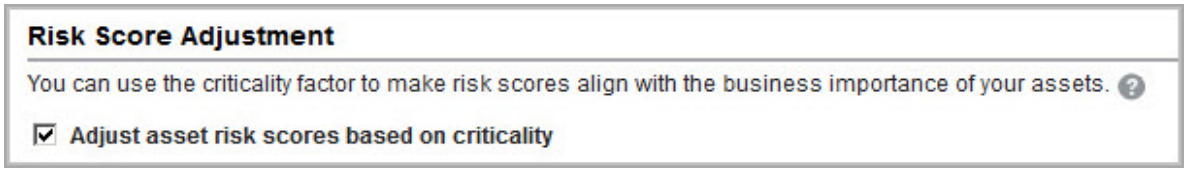
If a scan pauses or stops, The application does not use results from assets that do not have *completed* status for the computation of risk scores. For example: 10 assets are scanned in parallel. Seven have *completed* scan status; three do not. The scan is stopped. Risk is calculated based on the results for the seven assets with *completed* status. For the three *in progress* assets, it uses data from the last completed scan.

To determine scan status consult the scan log. See *Viewing the scan log* on page 231.

Adjusting risk with criticality

The Risk Score Adjustment setting allows you to customize your assets' risk score calculations according to the *business context* of the asset. For example, if you have set the Very High criticality level for assets belonging to your organization's senior executives, you can configure the risk score adjustment so that those assets will have higher risk scores than they would have otherwise. You can specify modifiers for your user-applied criticality levels that will affect the asset risk score calculations for assets with those levels set.

Note that you must enable Risk Score Adjustment for the criticality levels to be taken into account in calculating the risk score; it is not set by default.



Risk Score Adjustment must be manually enabled

To enable and configure Risk Score Adjustment:

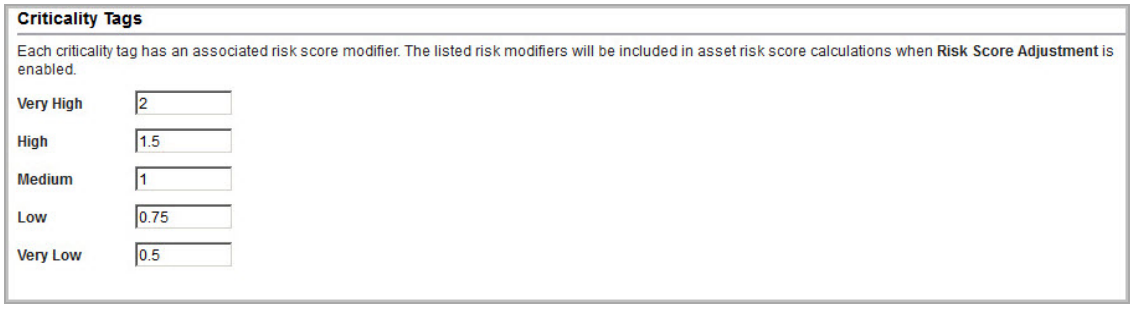
1. On the Administration page, in Global and Console Settings, click the **Manage** link for global settings.
2. In the Global Settings page, select **Risk Score Adjustment**.
3. Select **Adjust asset risk scores based on criticality.**
4. Change any of the modifiers for the listed criticality levels, per the constraints listed below.

Constraints:

- Each modifier must be greater than 0.
- You can specify up to two decimal places. For example, frequently-used modifiers are values such as .75 or .25.
- The numbers must correspond proportionately to the criticality levels. For example, the modifier for the High criticality level must be less than or equal to modifier for the Very High criticality level, and greater than or equal to the modifier for the Medium criticality level. The numbers can be equal to each other: For example, they can all be set to 1.

The default values are:

- Very High: 2
- High: 1.5
- Medium: 1
- Low: 0.75
- Very Low: 0.5



Adjust the multipliers for the criticality levels

Interaction with risk strategy

The *Risk Strategy* and Risk Score Adjustment are independent factors that both affect the risk score.

To calculate the risk score for an individual asset, Nexposeuses the algorithm corresponding to the selected risk strategy. If Risk Score Adjustment is set and the asset has a criticality tag applied, the application then multiplies the risk score determined by the risk strategy by the modifier specified for that criticality tag.



Both the original and context-driven risk scores are displayed for an individual asset

The risk score for a site or asset group is based upon the scores for the assets in that site or group. The calculation used to determine the risk for the entire site or group depends on the risk strategy. Note that even though it is possible to apply criticality through an asset group, the criticality actually gets applied to each asset and the total risk score for the group is calculated based upon the individual asset risk scores.



The risk score for a site or asset-group is based on the context-driven risk scores of the assets in it.

Viewing risk scores

If Risk Score Adjustment is enabled, nearly every risk score you see in your Nexposeinstallation will be the context-driven risk score that takes into account the risk strategy and the risk score adjustment. The one exception is the Original risk score available on the page for a selected asset. The Original risk score takes into account the risk strategy but not the risk score adjustment. Note that the values displayed are rounded to the nearest whole number, but the calculations are performed on more specific values. Therefore, the context-driven risk score shown may not be the exact product of the displayed original risk score and the multiplier.

When you first apply a criticality tag to an asset, the context-driven risk score on the page for that asset should update very quickly. There will be a slight delay in recalculating the risk scores for any sites or asset groups that include that asset.

Sending custom fingerprints to paired Scan Engines

If you develop custom fingerprints, you can have the Security Console distribute them automatically to any paired Scan Engine that is currently in use when a scan is run. To do so, simply copy the fingerprint files to the [installation_directory]/plugins/fp/custom/ directory on your Security Console host.

You do not have to restart the Security Console afterward. The NSC.log file, located in the [installation_directory]/nsc/logs/ directory, will display a message indicating the location and number of the newly added fingperprints.

Ensuring correct formatting for the fingerprints

Custom fingerprint XML files must meet certain formatting criteria in order to work properly, as in the following example:

```
<?xml version="1.0"?>
    <fingerprints matches="ssh.banner">
        <fingerprint pattern="^RomSShell_([\d\.]+)$">
            <description>Allegro RomSShell SSH</description>
            <example service.version="4.62">RomSShell_4.62</example>
            <param pos="0" name="service.vendor" value="Allegro"/>
            <param pos="0" name="service.product" value="RomSShell"/>
            <param pos="1" name="service.version"/>
        </fingerprint>
    </fingerprints>
```

The first line consists of the XML version declaration.

The first element is a *fingerpints* block with a *matches* attribute indicating what data the fingerprint file is intended to match.

The *matches* attribute is normally in the form of *protocol.field*.

The *fingerprints* element contains one or more *fingerprint* elements.

Every fingerprint contains a *pattern* attribute with the regular expression to match against the data.

An optional *flags* attribute controls how the regular expression is to be interpreted. See the Recog documentation for FLAG_MAP for more information.

Each fingerprint contains a *description* element with a human-readable string describing the fingerprint.

At least one *example* element is included, though multiple example elements are preferable. These elements are used in test coverage present in rspec, which validates that the provided data matches the specified regular expression. Additionally, if the fingerprint is using the *param* elements to extract field values from the data, you can add these expected extractions as attributes for the example elements. In the preceding example the string

```
<example service.version="4.62">RomSShell_4.62</example>
```

tests that *RomSShell_4.62* matches the provided regular expression and that the value of service.version is 4.62.

Each *param* elements contains a *pos* attribute that indicates what capture field from the pattern should be extracted, or 0 for a static string.

The *name* attribute is the key that will be reported in a successful match, and the value will either be a static string for *pos* values of 0 or missing and taken from the captured field.

Best practices for creating fingerprints

Create a single fingerprint for each product as long as the pattern remains clear and readable. If that is not possible, separate the pattern logically into additional fingerprints.

Create regular expressions that allow flexible version number matching. This ensures greater probability of matching a product. For example, all known public releases of a product report either major.minor or major.minor.build format version numbers. If the fingerprint strictly matches this version number format, it would fail to match a modified build of the product that reports only a major version number format.

Testing custom fingerprints via command line

You can test fingerprints via command line by entering *executing bin/recog_verify* against the fingerprint file:

```
$ bin/recog_verify xml/ssh_banners.xml
```

You can test matches via command line similarly:

```
$ echo 'OpenSSH_6.6p1 Ubuntu-2ubuntu1' | bin/recog_match xml/ssh_
banners.xml -
MATCH: {"service.version"=>"6.6p1", "openssh.comment"=>"Ubuntu-
2ubuntu1", "service.vendor"=
```

Resources

This section provides useful information and tools to help you get optimal use out of the application.

Scan templates on page 684: This section lists all built-in scan templates and their settings. It provides suggestions for when to use each template.

Report templates and sections on page 689: This section lists all built-in report templates and the information that each contains. It also lists and describes report sections that make up document report templates and data fields that make up CSV export templates. This information is useful for configuring custom report templates.

Performing configuration assessment on page 682: This section describes how you can use the application to verify compliance with configuration security standards such as USGCB and CIS.

Using regular expressions on page 678: This section provides tips on using regular expressions in various activities, such as configuring scan authentication on Web targets.

Using Exploit Exposure on page 681: This section describes how the application integrates exploitability data for vulnerabilities.

Glossary on page 718: This section lists and defines terms used and referenced in the application.

Finding out what features your license supports

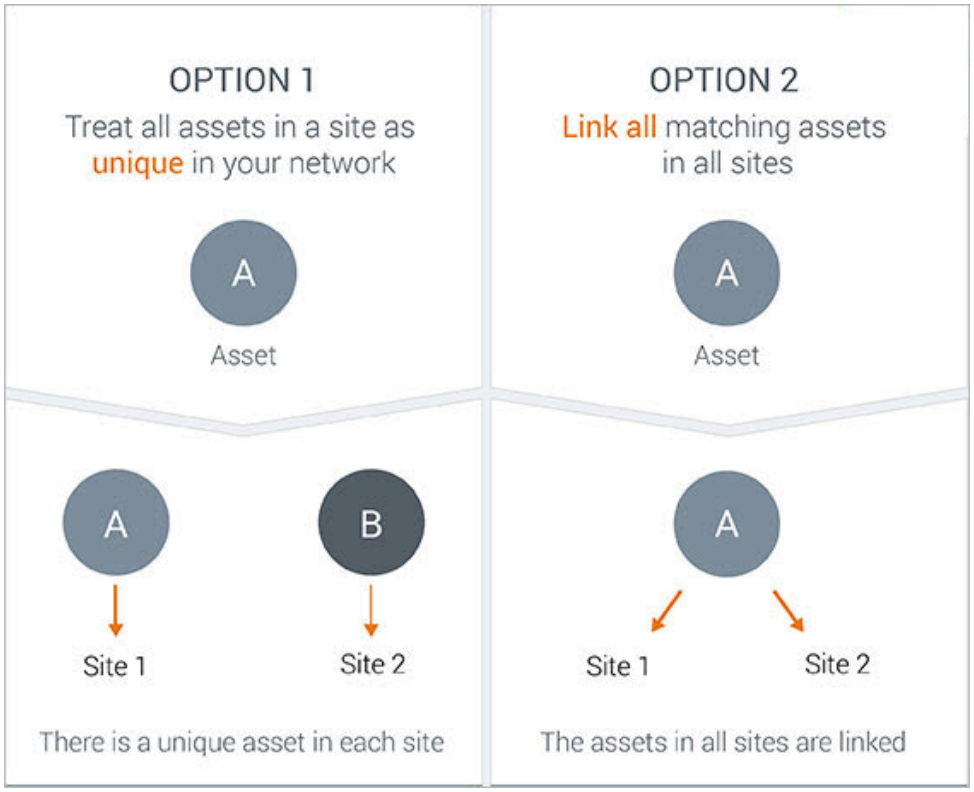
Some features of the application are only available with certain licenses. To determine if your license supports a particular feature, follow these steps:

1. Click the **Administration** tab.
2. On the *Administration* page, under Global and Console Settings, select the **Administer** link.
3. In the *Security Console Configuration* panel, select **Licensing**.

The features that your license enables are marked with a green check mark on the *Licensing* page.

Linking assets across sites

You can choose whether to link assets in different sites or treat them as unique entities. By linking matching assets in different sites, you can view and report on your assets in a way that aligns with your network configuration and reflects your asset counts across the organization. Below is some information to help you decide whether to enable this option.



Option 1

A corporation operates a chain of retail stores, each with the same network mapping, so it has created a site for each store. It **does not link assets across sites**, because each site reflects a unique group of assets.

Option 2

A corporation has a global network with a unique configuration in each location. It has created sites to focus on specific categories, and these categories may overlap. For example, a Linux server may be in one site called *Finance* and another called *Ubuntu machines*. The corporation **links assets across sites** so that in investigations and reporting, it is easier to recognize the Linux server as a single machine.

What exactly is an "asset"?

An asset is a set of proprietary, unique data gathered from a target device during a scan. This data, which distinguishes the scanned device when integrated into Nexpose, includes the following:

- IP address
- host name
- MAC address
- vulnerabilities
- risk score
- user-applied tags
- site membership
- asset ID (a unique identifier applied by Nexpose when the asset information is integrated into the database)

If the option to link assets across sites is disabled, Nexpose regards each asset as distinct from any other asset in any other site whether or not a given asset in another site is likely to be the same device.

For example, an asset named *server1.example.com*, with an IP address of 10.0.0.1 and a MAC address of 00:0a:95:9d:68:16 is part of one site called *Boston* and another site called *PCI targets*. Because this asset is in two different sites, it has two unique asset IDs, one for each site, and thus is regarded as two different entities.

Note: Assets are considered *matching* if they have certain proprietary characteristics in common, such as host name, IP address, and MAC address.

If the option to link assets across sites is enabled, Nexpose determines whether assets in different sites match, and if they do, treats the assets that match each other as a single entity .

Do I *want* to link assets across sites?

The information below describes some considerations to take into account when deciding whether to enable this option.

Use Cases

You have two choices when adding assets to your site configurations:

- **Link matching assets across sites.** Assets are considered *matching* if they have certain characteristics in common, such as host name, IP address, and MAC address. Linking makes sense if you scan assets in multiple sites. For example, you may have a site for all assets in your Boston office and another site of assets that you need to scan on a quarterly basis for compliance reasons. It is likely that certain assets would belong to both sites. In this case, it makes sense to link matching assets across all sites.
- **Treat each asset within each site as unique.** In other words, continue using Nexpose in the same way prior to the release of the linking capability. This approach makes sense if you do not scan any asset in more than one site. For example, if your company is a retail chain in which each individual store location is a site, you'll probably want to keep each asset in each site unique.

Security considerations

- Once assets are linked across sites, users will have a unified view of an asset. Access to an asset will be determined by factors other than site membership. If this option is enabled, and a user has access to an asset through an asset group, for instance, that user will have access to all information about that asset from any source, whether or not the user has access to the source itself. Examples: The user will have access to data from scans in sites to which they do not have access, discovery connections, Metasploit, or other means of collecting information about the asset.

Site-level controls

- With this option enabled, vulnerability exceptions cannot be created at the site level through the user interface at this time. They can be created at the site level through the API. Site-level exceptions created before the option was enabled will continue to apply.
- When this option is enabled, you will have two distinct options for removing an asset:
  - **Removing** an asset from a site breaks the link between the site and the asset, but the asset is still available in other sites in which is it was already present. However, if the asset is only in one site, it will be deleted from the entire workspace.
  - **Deleting** an asset deletes it from throughout your workspace in the application.

Transition considerations

- Disabling asset linking after it has been enabled will result in each asset being assigned to the site in which it was first scanned, which means that each asset's data will be in only one site. To reserve the possibility of returning to your previous scan results, back up your application database before enabling the feature.
- The links across sites will be created over time, as assets are scanned. During the transition period until you have scanned all assets, some will be linked across sites and others will not. Your risk score may also vary during this period.

If you choose to link assets across all sites on an installation that preceded the April 8, 2015 release, you will see some changes in your asset data and reports:

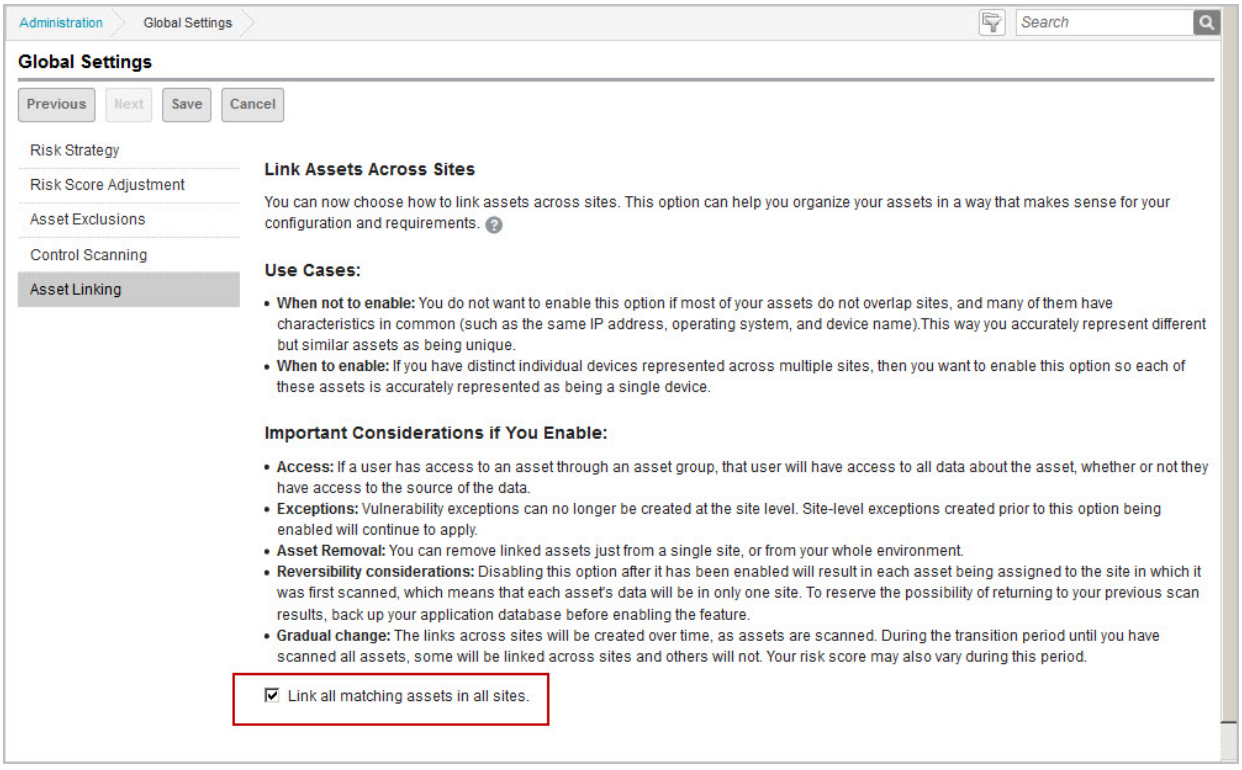
- You will notice that some assets are not updating with scans over time. As you scan, new data for an asset will link with the most recently scanned asset. For example if an asset with IP address 10.0.0.1 is included in both the *Boston* and the *PCI targets* sites, the latest scan data will link with one of those assets and continue to update that asset with future scans. The non-linked, older asset will not appear to update with future scans. The internal logic for selecting which older asset is linked depends on a number of factors, such scan authentication and the amount of information collected on each "version" of the asset.
- Your site risk scores will likely decrease over time because the score will be multiplied by fewer assets.

Enabling or disabling asset linking across sites

Note: The cross-site asset linking feature is enabled by default for new installations as of the April 8, 2015, product update.

To enable assets in different sites to be recognized as a single asset:

1. Review the above considerations.
2. Log in to the application as a Global Administrator.
3. Go to the **Administration** page.
4. Under *Global and Console Settings*, next to *Console*, select **Manage**.
5. Select **Asset Linking**.
6. Select the check box for **Link all matching assets in all sites**.



Enabling linking assets across sites.

To disable linking so that matching assets in different sites are considered unique:

1. Review the above considerations. Also note that removing the links will take some time.
2. Log in to the application as a Global Administrator.
3. Go to the **Administration** page.
4. Under *Global and Console Settings*, next to *Console*, select **Manage**.
5. Select **Asset Linking**.
6. Clear the check box for **Link all matching assets in all sites**.
7. Click **Save** under *Global Settings*.

Using regular expressions

A regular expression, also known as a “regex,” is a text string used for searching for a piece of information or a message that an application will display in a given situation. Regex notation patterns can include letters, numbers, and special characters, such as dots, question marks, plus signs, parentheses, and asterisks. These patterns instruct a search application not only what string to search for, but how to search for it.

Regular expressions are useful in configuring scan activities:

- searching for file names on local drives; see *How the file name search works with regex* on page 679
- searching for certain results of logon attempts to Telnet servers; see *Configuring scans of Telnet servers* on page 623
- determining if a logon attempt to a Web server is successful; see *How to use regular expressions when logging on to a Web site* on page 680

General notes about creating a regex

A regex can be a simple pattern consisting of characters for which you want to find a direct match. For example, the pattern *nap* matches character combinations in strings only when exactly the characters *n*, *a*, and *p* occur together and in that exact sequence. A search on this pattern would return matches with strings such as *snap* and *synapse*. In both cases the match is with the substring *nap*. There is no match in the string *an aperture* because it does not contain the substring *nap*.

When a search requires a result other than a direct match, such as one or more n's or white space, the pattern requires special characters. For example, the pattern *ab*c* matches any character combination in which a single *a* is followed by 0 or more *b*s and then immediately followed by *c*. The asterisk indicates 0 or more occurrences of the preceding character. In the string *cbbabbbbcdebc*, the pattern matches the substring *abbbbc*.

The asterisk is one example of how you can use a special character to modify a search. You can create various types of search parameters using other single and combined special characters.

How the file name search works with regex

Nexpose searches for matching files by comparing the search string against the entire directory path and file name. See *Configuring file searches on target systems on page 624*. Files and directories appear in the results table if they have any greedy matches against the search pattern. If you don't include regex anchors, such ^ and $, the search can result in multiple matches. Refer to the following examples to further understand how the search algorithm works with regular expressions. Note that the search matches are in **bold** typeface.

With search pattern *.*xls*

- the following search input,

  C$/Documents and Settings/user/My Documents/patientData.xls

  results in one match:

  C$/Documents and Settings/user/My Documents/patientData.xls

- the following search input,

  C$/Documents and Settings/user/My Documents/patientData.doc

  results in no matches

- the following search input,

  C$/Documents and Settings/user/My Documents/xls/patientData.xls

  results in one match:

  C$/Documents and Settings/user/My Documents/xls/patientData.xls

- the following search input,

  C$/Documents and Settings/user/My Documents/xls/patientData.doc

  results in one match:

  C$/Documents and Settings/user/My Documents/xls/patientData.doc

With search pattern ^.*xls$:

- the following search input,

  C$/Documents and Settings/user/My Documents/patientData.xls

results in one match:

C$/Documents and Settings/user/My Documents/patientData.xls

- the following search input,

  C$/Documents and Settings/user/My Documents/patientData.docresults in no matches

How to use regular expressions when logging on to a Web site

When Nexpose makes a successful attempt to log on to a Web application, the Web server returns an HTML page that a user typically sees after a successful logon. If the logon attempt fails, the Web server returns an HTML page with a failure message, such as “Invalid password.”

Configuring the application to log on to a Web application with an HTML form or HTTP headers involves specifying a regex for the failure message. During the logon process, it attempts to match the regex against the HTML page with the failure message. If there is a match, the application recognizes that the attempt failed. It then displays a failure notification in the scan logs and in the Security Console Web interface. If there is no match, the application recognizes that the attempt was successful and proceeds with the scan.

Using Exploit Exposure

With Nexpose Exploit Exposure™, you can now use the application to target specific vulnerabilities for exploits using the Metasploit exploit framework. Verifying vulnerabilities through exploits helps you to focus remediation tasks on the most critical gaps in security.

For each discovered vulnerability, the application indicates whether there is an associated exploit and the required skill level for that exploit. If a Metasploit exploit is available, the console displays the ™ icon and a link to a Metasploit module that provides detailed exploit information.

Why exploit your own vulnerabilities?

On a logistical level, exploits can provide critical access to operating systems, services, and applications for penetration testing.

Also, exploits can afford better visibility into network security, which has important implications for different stakeholders within your organization:

- Penetration testers and security consultants use exploits as compelling proof that security flaws truly exist in a given environment, eliminating any question of a false positive. Also, the data they collect during exploits can provide a great deal of insight into the seriousness of the vulnerabilities.
- Senior managers demand accurate security data that they can act on with confidence. False positives can cause them to allocate security resources where they are not needed. On the other hand, if they refrain from taking action on reported vulnerabilities, they may expose the organization to serious breaches. Managers also want metrics to help them determine whether or not security consultants and vulnerability management tools are good investments.
- System administrators who view vulnerability data for remediation purposes want to be able to verify vulnerabilities quickly. Exploits provide the fastest proof.

Performing configuration assessment

Performing regular audits of configuration settings on your assets may be mandated in your organization. Whether you work for a United States government agency, a company that does business with the federal government, or a company with strict security rules, you may need to verify that your assets meet a specific set of configuration standards. For example, your company may require that all of your workstations lock out users after a given number of incorrect logon attempts.

Like vulnerability scans, policy scans are useful for gauging your security posture. They help to verify that your IT department is following secure configuration practices. Using the application, you can scan your assets as part of a configuration assessment audit. A license-enabled feature named Policy Manager provides compliance checks for several configuration standards:

USGCB 2.0 policies

The United States Government Configuration Baseline (USGCB) is an initiative to create security configuration baselines for information technology products deployed across U.S. government agencies. USGCB 2.0 evolved from FDCC (see below), which it replaces as the configuration security mandate in the U.S. government. Companies that do business with the federal government or have computers that connect to U.S. government networks must conform to USGCB 2.0 standards. For more information, go to usgcb.nist.gov.

USGCB 1.0 policies

USGCB 2.0 is not an “update” of 1.0. The two versions are considered separate entities. For that reason, the application includes USGCB 1.0 checks in addition to those of the later version. For more information, go to usgcb.nist.gov.

FDCC policies

The Federal Desktop Core Configuration (FDCC) preceded USGCB as the U.S. government-mandated set of configuration standards. For more information, go to fdcc.nist.gov.

CIS benchmarks

These benchmarks are consensus-based, best-practice security configuration guidelines developed by the not-for-profit Center for Internet Security (CIS), with input and approval from the U.S. government, private-sector businesses, the security industry, and academia. The benchmarks include technical control rules and values for hardening network devices, operating systems, and middleware and software applications. They are widely held to be the configuration security standard for commercial businesses. For more information, go to www.cisecurity.org.

How do I run configuration assessment scans?

Configure a site with a scan template that includes Policy Manager checks. Depending on your license, the application provides built-in USGCB, FDCC, and CIS templates. These templates do not include vulnerability checks. If you prefer to run a combined vulnerability/policy scan, you can configure a custom scan template that includes vulnerability checks and Policy Manager policies or benchmarks. See the following sections for more information:

- *Selecting the type of scanning you want to do* on page 584
- *Selecting Policy Manager checks* on page 608

How do I know if my license enables Policy Manager?

To verify that your license enables Policy Manager and includes the specific checks that you want to run, go the *Licensing* page on the *Security Console Configuration* panel. See *Viewing, activating, renewing, or changing your license* in the administrator's guide.

What platforms are supported by Policy Manager checks?

For a complete list of platforms that are covered by Policy Manager checks, go to the Rapid7Community at https://community.rapid7.com/docs/DOC-2061.

How do I view Policy Manager scan results?

Go to the *Policies* page, where you can view results of policy scans, including those of individual rules that make up policies. You can also override rule results. See *Working with Policy Manager results* on page 297.

Can I create custom checks based on Policy Manager checks?

You can customize policy checks based on Policy Manager checks. See *Creating a custom policy* on page 631.

Scan templates

This appendix lists all built-in scan templates available in Nexpose. It provides a description for each template and suggestions for when to use it.

CIS

This template incorporates the Policy Manager scanning feature for verifying compliance with Center for Internet Security (CIS) benchmarks. The scan runs application-layer audits. Policy checks require authentication with administrative credentials on targets. Vulnerability checks are not included.

DISA

This scan template performs Defense Information Systems Agency (DISA) policy compliance tests with application-layer auditing on supported DISA-benchmarked systems. Policy checks require authentication with administrative credentials on targets. Vulnerability checks are not included. Only default ports are scanned.

Denial of service

This basic audit of all network assets uses both safe and unsafe (denial-of-service) checks. This scan does not include in-depth patch/hotfix checking, policy compliance checking, or application-layer auditing. You can run a denial of service scan in a preproduction environment to test the resistance of assets to denial-of service conditions.

Discovery scan

This scan locates live assets on the network and identifies their host names and operating systems. This template does not include enumeration, policy, or vulnerability scanning.

You can run a discovery scan to compile a complete list of all network assets. Afterward, you can target subsets of these assets for intensive vulnerability scans, such as with the Exhaustive scan template.

Discovery scan (aggressive)

This fast, cursory scan locates live assets on high-speed networks and identifies their host names and operating systems. The system sends packets at a very high rate, which may trigger IPS/IDS sensors, SYN flood protection, and exhaust states on stateful firewalls. This template does not perform enumeration, policy, or vulnerability scanning.

This template is identical in scope to the discovery scan, except that it uses more threads and is, therefore, much faster. The trade-off is that scans run with this template may not be as thorough as with the Discovery scan template.

Exhaustive

This thorough network scan of all systems and services uses only safe checks, including patch/hotfix inspections, policy compliance assessments, and application-layer auditing. This scan could take several hours, or even days, to complete, depending on the number of target assets.

Scans run with this template are thorough, but slow. Use this template to run intensive scans targeting a low number of assets.

FDCC

This template incorporates the Policy Manager scanning feature for verifying compliance with all Federal Desktop Core Configuration (FDCC) policies. The scan runs application-layer audits on all Windows XP and Windows Vista systems. Policy checks require authentication with administrative credentials on targets. Vulnerability checks are not included. Only default ports are scanned.

If you work for a U.S. government organization or a vendor that serves the government, use this template to verify that your Windows Vista and XP systems comply with FDCC policies.

Full audit

This full network audit of all systems uses only safe checks, including network-based vulnerabilities, patch/hotfix checking, and application-layer auditing. The system scans only default ports and disables policy checking, which makes scans faster than with the Exhaustive scan. Also, This template does not check for potential vulnerabilities.

Use this template to run a thorough vulnerability scan.

Full audit without Web Spider

This full network audit uses only safe checks, including network-based vulnerabilities, patch/hotfix checking, and application-layer auditing. The system scans only default ports and disables policy checking, which makes scans faster than with the Exhaustive scan. It also does not include the Web spider, which makes it faster than the full audit that does include it. Also, This template does not check for potential vulnerabilities.

This is the default scan template. Use it to run a fast vulnerability scan right “out of the box.”

HIPAA compliance

This template uses safe checks in this audit of compliance with HIPAA section 164.312 (“Technical Safeguards”). The scan will flag any conditions resulting in inadequate access control, inadequate auditing, loss of integrity, inadequate authentication, or inadequate transmission security (encryption).

Use this template to scan assets in a HIPAA-regulated environment, as part of a HIPAA compliance program.

Internet DMZ audit

This penetration test covers all common Internet services, such as Web, FTP, mail (SMTP/POP/IMAP/Lotus Notes), DNS, database, Telnet, SSH, and VPN. This template does not include in-depth patch/hotfix checking and policy compliance audits.

Use this template to scan assets in your DMZ.

Linux RPMs

This scan verifies proper installation of RPM patches on Linux systems. For best results, use administrative credentials.

Use this template to scan assets running the Linux operating system.

Microsoft hotfix

This scan verifies proper installation of hotfixes and service packs on Microsoft Windows systems. For optimum success, use administrative credentials.

Use this template to verify that assets running Windows have hotfix patches installed on them.

PCI ASV external audit

Previously called payment card industry (PCI) audit

This audit of Payment Card Industry (PCI) compliance uses only safe checks, including network-based vulnerabilities, patch /hotfix verification, and application-layer testing. All TCP ports and well-known UDP ports are scanned. Policy checks are not included.

This template should be used by an Approved Scanning Vendor (ASV) to scan assets as part of a PCI compliance program. For your internal PCI discovery scans, use the PCI Internal audit template.

PCI internal audit

This template is intended for discovering vulnerabilities in accordance with the Payment Card Industry (PCI) Data Security Standard (DSS) requirements. It includes all network-based vulnerabilities and web application scanning. It specifically excludes potential vulnerabilities as well as vulnerabilities specific to the external perimeter.

This template is intended for your organization's internal scans for PCI compliance purposes.

Penetration test

This in-depth scan of all systems uses only safe checks. Host-discovery and network penetration features allow the system to dynamically detect assets that might not otherwise be detected. This template does not include in-depth patch/hotfix checking, policy compliance checking, or application-layer auditing.

With this template, you may discover assets that are out of your initial scan scope. Also, running a scan with this template is helpful as a precursor to conducting formal penetration test procedures.

Safe network audit

This non-intrusive scan of all network assets uses only safe checks. This template does not include in-depth patch/hotfix checking, policy compliance checking, or application-layer auditing.

This template is useful for a quick, general scan of your network.

Sarbanes-Oxley (SOX) compliance

This is a safe-check Sarbanes-Oxley (SOX) audit of all systems. It detects threats to digital data integrity, data access auditing, accountability, and availability, as mandated in Section 302 (“Corporate Responsibility for Fiscal Reports”), Section 404 (“Management Assessment of Internal Controls”), and Section 409 (“Real Time Issuer Disclosures”) respectively.

Use this template to scan assets as part of a SOX compliance program.

SCADA audit

This is a “polite,” or less aggressive, network audit of sensitive Supervisory Control And Data Acquisition (SCADA) systems, using only safe checks. Packet block delays have been increased; time between sent packets has been increased; protocol handshaking has been disabled; and simultaneous network access to assets has been restricted.

Use this template to scan SCADA systems.

USGCB

This template incorporates the Policy Manager scanning feature for verifying compliance with all United States Government Configuration Baseline (USGCB) policies. The scan runs application-layer audits on all Windows 7 systems. Policy checks require authentication with administrative credentials on targets. Vulnerability checks are not included. Only default ports are scanned.

If you work for a U.S. government organization or a vendor that serves the government, use this template to verify that your Windows 7 systems comply with USGCB policies.

Web audit

This audit of all Web servers and Web applications is suitable public-facing and internal assets, including application servers, ASPs, and CGI scripts. The template does not include patch checking or policy compliance audits. Nor does it scan FTP servers, mail servers, or database servers, as is the case with the DMZ Audit scan template.

Use this template to scan public-facing Web assets.

Report templates and sections

Use this appendix to help you select the right built-in report template for your needs. You can also learn about the individual sections or data fields that make up report templates, which is helpful for creating custom templates.

This appendix includes the following information:

- *Built-in report templates and included sections* on page 689
- *Document report sections* on page 704
- *Export template attributes* on page 712

Built-in report templates and included sections

Creating custom document templates enables you to include as much, or as little, information in your reports as your needs dictate. For example, if you want a report that only lists all assets organized by risk level, a custom report might be the best solution. This template would include only the section. Or, if you want a report that only lists vulnerabilities, create a template with the section.

Configuring a document report template involves selecting the sections to be included in the template. Each report template in the following section lists all sections available for each of the document report templates, including those that appear in built-in report templates and those that you can include in a customized template. You may find that a given built-in template contains all the sections that you require in a particular report, making it unnecessary to create a custom template. Built-in reports and sections are listed below:

- *Asset Report Format (ARF)* on page 692
- *Audit Report* on page 692
- *Baseline Comparison* on page 694
- *Executive Overview* on page 695
- *Newly Discovered Assets* on page 696
- *Highest Risk Vulnerabilities* on page 695
- *PCI Attestation of Compliance* on page 696
- *PCI Audit (legacy)* on page 697
- *PCI Executive Overview (legacy)* on page 697
- *PCI Executive Summary* on page 698
- *PCI Host Details* on page 699
- *PCI Vulnerability Details* on page 699
- *Policy Evaluation* on page 700
- *Remediation Plan* on page 700
- *Report Card* on page 701
- *Top 10 Assets by Vulnerability Risk* on page 701
- *Top 10 Assets by Vulnerabilities* on page 702
- *Top Remediations* on page 702
- *Top Remediations with Details* on page 702
- *Vulnerability Exception Activity* on page 711
- *Vulnerability Trends* on page 703

Asset Report Format (ARF)

The Asset Report Format (ARF) XML template organizes data for submission of policy and benchmark scan results to the U.S. Government for SCAP 1.2 compliance.

Audit Report

Of all the built-in templates, the Audit is the most comprehensive in scope. You can use it to provide a detailed look at the state of security in your environment.

- The Audit Report template provides a great deal of granular information about discovered assets:
- host names and IP addresses
- discovered services, including ports, protocols, and general security issues
- risk scores, depending on the scoring algorithm selected by the administrator
- users and asset groups associated with the assets
- discovered databases*
- discovered files and directories*
- results of policy evaluations performed*
- spidered Web sites*

It also provides a great deal of vulnerability information:

- affected assets
- vulnerability descriptions
- severity levels
- references and links to important information sources, such as security advisories
- general solution information

Additionally, the Audit Report template includes charts with general statistics on discovered vulnerabilities and severity levels.

* To gather this “deep” information the application must have logon credentials for the target assets. An Audit Report based on a non-credentialed scan will not include this information. Also, it must have policy testing enabled in the scan template configuration.

Note that the Audit Report template is different from the PCI Audit template. See *PCI Audit (legacy)* on page 697.

The Audit report template includes the following sections:

- Cover Page
- Discovered Databases
- Discovered Files and Directories
- Discovered Services
- Discovered System Information
- Discovered Users and Groups
- Discovered Vulnerabilities
- Executive Summary
- Policy Evaluation
- Spidered Web Site Structure
- Vulnerability Report Card by Node

Baseline Comparison

You can use the Baseline Comparison to observe security-related trends or to assess the results of a scan as compared with the results of a previous scan that you are using as a baseline, as in the following examples.

- You may use the first scan that you performed on a site as a baseline. Being the first scan, it may have revealed a high number of vulnerabilities that you subsequently remediated. Comparing current scan results to those of the first scan will help you determine how effective your remediation work has been.
- You may use a scan that revealed an especially low number of vulnerabilities as a benchmark of good security “health”.
- You may use the last scan preceding the current one to verify whether a certain patch removed a vulnerability in that scan.

Trending information indicates changes discovered during the scan, such as the following:

- new assets and services
- assets or services that are no longer running since the last scan
- new vulnerabilities
- previously discovered vulnerabilities did not appear in the most current scan

Trending information is useful in gauging the progress of remediation efforts or observing environmental changes over time. For trending to be accurate and meaningful, make sure that the compared scans occurred under identical conditions:

- the same site was scanned
- the same scan template was used
- if the baseline scan was performed with credentials, the recent scan was performed with the same credentials.

The Baseline Comparison report template includes the following sections:

- Cover Page
- Executive Summary

Executive Overview

You can use the Executive Overview template to provide a high-level snapshot of security data. It includes general summaries and charts of statistical data related to discovered vulnerabilities and assets.

Note that the Executive Overview template is different from the *PCI Executive Overview*. See *PCI Executive Overview (legacy)* on page 697.

The Executive Overview template includes the following sections:

- Baseline Comparison
- Cover Page
- Executive Summary
- Risk Trends

Highest Risk Vulnerabilities

The Highest Risk Vulnerabilities template lists the top 10 discovered vulnerabilities according to risk level. This template is useful for targeting the biggest threats to security as priorities for remediation.

Each vulnerability is listed with risk and CVSS scores, as well references and links to important information sources.

The Highest Risk Vulnerabilities report template includes the following sections:

- Cover Page
- Highest Risk Vulnerability Details
- Table of Contents

Newly Discovered Assets

With this template you can view assets that were discovered in scans within a specified time period. It is useful for tracking changes to your asset inventory. In addition to general information about each asset, the report lists risk scores and indicates whether assets have vulnerabilities with associated exploits or malware kits.

PCI Attestation of Compliance

This is one of three PCI-mandated report templates to be used by ASVs for PCI scans as of September 1, 2010.

The PCI Attestation of Compliance is a single page that serves as a cover sheet for the completed PCI report set.

In the top left area of the page is a form for entering the customer's contact information. If the ASV added scan customer organization information in the site configuration on which the scan data is based, the form will be auto-populated with that information. See *Including organization information in a site* in the *user's guide or Help*. In the top right area is a form with auto-populated fields for the ASV's information.

The *Scan Status* section lists a high-level summary of the scan, including whether the overall result is a Pass or Fail, some statistics about what the scan found, the date the scan was completed, and scan expiration date, which is the date after which the results are no longer valid.

In this section, the ASV must note the number of components left out of the scope of the scan.

Two separate statements appear at the bottom. The first is for the customer to attest that the scan was properly scoped and that the scan result only applies to external vulnerability scan requirement of PCI Data Security Standard (DSS). It includes the attestation date, and an indicated area to fill in the customer's name.

The second statement is for the ASV to attest that the scan was properly conducted, QA-tested, and reviewed. It includes the following auto-populated information:

- attestation date for scan customer
- ASV name*
- certificate number*
- ASV reviewer name* (the individual who conducted the scan and review process)

To support auto-population of these fields*, you must enter create appropriate settings in the oem.xml configuration file. See The *ASV guide*, which you can request from Technical Support.

The PCI Attestation report template includes the following section:

- Asset and Vulnerabilities Compliance Overview

PCI Audit (legacy)

This is one of two reports no longer used by ASVs in PCI scans as of September 1, 2010. It provides detailed scan results, ranking each discovered vulnerability according to its Common Vulnerability Scoring System (CVSS) ranking.

Note that the *PCI* Audit template is different from the Audit Report template. See *Audit Report* on page 692.

The PCI Audit (Legacy) report template includes the following sections:

- Cover Page
- Payment Card Industry (PCI) Scanned Hosts/Networks
- Payment Card Industry (PCI) Vulnerability Details
- Payment Card Industry (PCI) Vulnerability Synopsis
- Table of Contents
- Vulnerability Exceptions

PCI Executive Overview (legacy)

This is one of two reports no longer used by ASVs in PCI scans as of September 1, 2010. It provides high-level scan information.

Note that the *PCI Executive Overview* template is different from the template *PCI Executive Summary*. See *PCI Executive Summary* on page 698.

The PCI Executive Overview (Legacy) report template includes the following sections:

- Cover Page
- Payment Card Industry (PCI) Executive Summary
- Table of Contents

PCI Executive Summary

This is one of three PCI-mandated report templates to be used by ASVs for PCI scans as of September 1, 2010.

The PCI Executive Summary begins with a *Scan Information* section, which lists the dates that the scan was completed and on which it expires. This section includes the auto-populated ASV name and an area to fill in the customer's company name. If the ASV added scan customer organization information in the site configuration on which the scan data is based, the customer's company name will be auto-populated. See *Getting started: Info & Security* on page 61.

The *Component Compliance Summary* section lists each scanned IP address with a Pass or Fail result.

The *Asset and Vulnerabilities Compliance Overview* section includes charts that provide compliance statistics at a glance.

The *Vulnerabilities Noted for each IP Address* section includes a table listing each discovered vulnerability with a set of attributes including PCI severity, CVSS score, and whether the vulnerability passes or fails the scan. The assets are sorted by IP address. If the ASV marked a vulnerability for exception in the application, the exception is indicated here. The column labeled *Exceptions, False Positives, or Compensating Controls* field in the PCI Executive Summary report is auto-populated with the user name of the individual who excluded a given vulnerability.

In the concluding section, *Special Notes*, ASVs must disclose the presence of any software that may pose a risk due to insecure implementation, rather than an exploitable vulnerability. The notes should include the following information:

- the IP address of the affected asset
- the note statement, written according to PCIco (see the *PCI ASV Program Guide v1.2*)
- information about the issue such as name or location of the affected software
- the customer's declaration of secure implementation or description of action taken to either remove the software or secure it

Any instance of remote access software or directory browsing is automatically noted. ASVs must add any information pertaining to point-of-sale terminals and absence of synchronization between load balancers. ASVs must obtain and insert customer declarations or description of action taken for each special note before officially releasing the Attestation of Compliance.

The PCI Executive Overview report template includes the following sections:

- Payment Card Industry (PCI) Component Compliance Summary
- Payment Card Industry (PCI) Scan Information
- Payment Card Industry (PCI) Special Notes
- Payment Card Industry (PCI) Vulnerabilities Noted (sub-sectioned into High, Medium, and Small)

PCI Host Details

This template provides detailed, sorted scan information about each asset, or host, covered in a PCI scan. This perspective allows a scanned merchant to consume, understand, and address all the PCI-related issues on an asset-by-asset basis. For example, it may be helpful to note that a non-PCI-compliant asset may have a number of vulnerabilities specifically related to its operating system or a particular network communication service running on it.

The PCI Host Details report template includes the following sections:

- Payment Card Industry (PCI) Host Details
- Table of Contents

PCI Vulnerability Details

This is one of three PCI-mandated report templates to be used by ASVs for PCI scans as of September 1, 2010.

The PCI Vulnerability Details report begins with a *Scan Information* section, which lists the dates that the scan was completed and on which it expires. This section includes the auto-populated ASV name and an area to fill in the customer's company name.

Note: The PCI Vulnerability Details report takes into account approved vulnerability exceptions to determine compliance status for each vulnerability instance.

The *Vulnerability Details* section includes statistics and descriptions for each discovered vulnerability, including affected IP address, Common Vulnerability Enumeration (CVE) identifier, CVSS score, PCI severity, and whether the vulnerability passes or fails the scan. Vulnerabilities are grouped by severity level, and within grouping vulnerabilities are listed according to CVSS score.

The PCI Vulnerability Details report template includes the following sections:

- Payment Card Industry (PCI) Scan Information
- Payment Card Industry (PCI) Vulnerability Details
- Table of Contents

Policy Evaluation

The Policy Evaluation displays the results of policy evaluations performed during scans.

The application must have proper logon credentials in the site configuration and policy testing enabled in the scan template configuration. See *Establishing scan credentials* and *Modifying and creating scan templates* in the *administrator's guide*.

Note that this template provides a subset of the information in the Audit Report template.

The Policy Evaluation report template includes the following sections:

- Cover Page
- Policy Evaluation

Remediation Plan

The Remediation Plan template provides detailed remediation instructions for each discovered vulnerability. Note that the report may provide solutions for a number of scenarios in addition to the one that specifically applies to the affected target asset.

The Remediation Plan report template includes the following sections:

- Cover Page
- Discovered System Information
- Remediation Plan
- Risk Assessment

Report Card

The Report Card template is useful for finding out whether, and how, vulnerabilities have been verified. The template lists information about the test that Nexpose performed for each vulnerability on each asset. Possible test results include the following:

- not vulnerable
- not vulnerable version
- exploited

For any vulnerability that has been excluded from reports, the test result will be the reason for the exclusion, such as *acceptable risk*.

The template also includes detailed information about each vulnerability.

The Report Card report template includes the following sections:

- Cover Page
- Index of Vulnerabilities
- Vulnerability Report Card by Node

Top 10 Assets by Vulnerability Risk

Note: The Top 10 Assets by Vulnerability Risk and Top 10 Assets by Vulnerabilities report templates do not contain individual sections that can be applied to custom report templates.

The Top 10 Assets by Vulnerability Risk lists the 10 assets with the highest risk scores. For more information about ranking, see *Viewing active vulnerabilities* on page 265 *Viewing active vulnerabilities*.

This report is useful for prioritizing your remediation efforts by providing your remediation team with an overview of the assets in your environment that pose the greatest risk.

Top 10 Assets by Vulnerabilities

The Top 10 Assets by Vulnerabilities report lists 10 the assets in your organization that have the most vulnerabilities. This report does not account for cumulative risk.

You can use this report to view the most vulnerable services to determine if services should be turned off to reduce risk. This report is also useful for prioritizing remediation efforts by listing the assets that have the most vulnerable services.

Top Remediations

The Top Remediations template provides high-level information for assessing the highest impact remediation solutions. The template includes the percentage of total vulnerabilities resolved, the percentage of vulnerabilities with malware kits, the percentage of vulnerabilities with known exploits, and the number of assets affected when the top remediation solutions are applied.

The Top Remediations template includes information in the following areas:

- the number of vulnerabilities that will be remediated, including vulnerabilities with no exploits or malware that will be remediated
- vulnerabilities and total risk score associated with the solution
- the number of targeted vulnerabilities that have known exploits associated with them
- the number of targeted vulnerabilities with available malware kits
- the number of assets to be addressed by remediation
- the amount of risk that will be reduced by the remediations

Top Remediations with Details

The Top Remediations with Details template provides expanded information for assessing remediation solutions and implementation steps. The template includes the percentage of total vulnerabilities resolved and the number of assets affected when remediation solutions are applied.

The Top Remediations with Details includes the information from the Top Rememdiations template with information in the following areas:

- remediation steps that need to be performed
- vulnerabilities and total risk score associated with the solution
- the assets that require the remediation steps

Vulnerability Trends

The Vulnerability Trends template provides information about how vulnerabilities in your environment have changed, if your remediation efforts have succeeded, how assets have changed over time, how asset groups have been affected when compared to other asset groups, and how effective your asset scanning process is. To manage the readability and size of the report, when you configure the date range there is a limit of 15 data points that can be included on a chart. For example, you can set your date range for a weekly interval for a two-month period, and you will have eight data points in your report. You can configure the period of time for the report to see if you are improving your security posture and where you can make improvements.

Note: Ensure you schedule adequate time to run this report template because of the large amount of data that it aggregates. Each data point is the equivalent of a complete report. It may take a long time to complete.

The Vulnerability Trends template provides charts and details in the following areas:

- assets scanned and vulnerabilities
- severity levels
- trend by vulnerability age
- vulnerabilities with malware or exploits

The Vulnerability Trends template helps you improve your remediation efforts by providing information about the number of assets included in a scan and if any have been excluded, if vulnerability exceptions have been applied or expired, and if there are new vulnerability definitions that have been added to the application. The Vulnerability Trends survey template differs from the vulnerability trend section in the Baseline report by providing information for more in-depth analysis regarding your security posture and remediation efforts provides.

Document report sections

Some of the following documents report sections can have vulnerability filters applied to them. This means that specific vulnerabilities can be included or excluded in these sections based on the report *Scope* configuration. When the report is generated, sections with filtered vulnerabilities will be so identified. Document report templates that do not contain any of these sections do not contain filtered vulnerability data. The document report sections are listed below:

Asset and Vulnerabilities Compliance Overview on page 705

Baseline Comparison on page 706

Cover Page on page 706

Discovered Databases on page 706

Discovered Files and Directories on page 706

Discovered Services on page 707

Discovered System Information on page 707

Discovered Users and Groups on page 707

Discovered Vulnerabilities on page 707

Executive Summary on page 708

Highest Risk Vulnerability Details on page 708

Index of Vulnerabilities on page 708

Payment Card Industry (PCI) Component Compliance Summary on page 708

Payment Card Industry (PCI) Executive Summary on page 708

Payment Card Industry (PCI) Host Details on page 708

Payment Card Industry (PCI) Scan Information on page 709

Payment Card Industry (PCI) Scanned Hosts/Networks on page 709

Payment Card Industry (PCI) Special Notes on page 709

Payment Card Industry (PCI) Vulnerabilities Noted for each IP Address on page 709

Payment Card Industry (PCI) Vulnerability Details on page 710

Payment Card Industry (PCI) Vulnerability Synopsis on page 710

Policy Evaluation on page 710

Remediation Plan on page 710

Risk Assessment on page 710

Risk Trend on page 711

Scanned Hosts and Networks on page 711

Table of Contents on page 711

Trend Analysis on page 711

Vulnerabilities by IP Address and PCI Severity Level on page 711

Vulnerability Details on page 711

Vulnerability Exceptions on page 711

Vulnerability Report Card by Node on page 712

Vulnerability Report Card Across Network on page 712

Vulnerability Test Errors on page 712

Asset and Vulnerabilities Compliance Overview

This section includes charts that provide compliance statistics at a glance.

Baseline Comparison

This section appears when you select the Baseline Report template. It provides a comparison of data between the most recent scan and the baseline, enumerating the following changes:

- discovered assets that did not appear in the baseline scan
- assets that were discovered in the baseline scan but not in the most recent scan
- discovered services that did not appear the baseline scan
- services that were discovered in the baseline scan but not in the most recent scan
- discovered vulnerabilities that did not appear in the baseline scan
- vulnerabilities that were discovered in the baseline scan but not in the most recent scan

Additionally, this section provides suggestions as to why changes in data may have occurred between the two scans. For example, newly discovered vulnerabilities may be attributable to the installation of vulnerable software that occurred after the baseline scan.

In generated reports, this section appears with the heading *Trend Analysis*.

Cover Page

The *Cover Page* includes the name of the site, the date of the scan, and the date that the report was generated. Other display options include a customized title and company logo.

Discovered Databases

This section lists all databases discovered through a scan of database servers on the network.

For information to appear in this section, the scan on which the report is based must meet the following conditions:

- database server scanning must be enabled in the scan template
- the application must have correct database server logon credentials

Discovered Files and Directories

This section lists files and directories discovered on scanned assets.

For information to appear in this section, the scan on which the report is based must meet the following conditions:

- file searching must be enabled in the scan template
- the application must have correct logon credentials

See *Configuring scan credentials* on page 93 for information on configuring these settings.

Discovered Services

This section lists all services running on the network, the IP addresses of the assets running each service, and the number of vulnerabilities discovered on each asset.

Vulnerability filters can be applied.

Discovered System Information

This section lists the IP addresses, alias names, operating systems, and risk scores for scanned assets.

Discovered Users and Groups

This section provides information about all users and groups discovered on each node during the scan.

Note: In generated reports, the Discovered Vulnerabilities section appears with the heading *Discovered and Potential Vulnerabilities*.

Discovered Vulnerabilities

This section lists all vulnerabilities discovered during the scan and identifies the affected assets and ports. It also lists the Common Vulnerabilities and Exposures (CVE) identifier for each vulnerability that has an available CVE identifier. Each vulnerability is classified by severity.

If you selected a *Medium* technical detail level for your report template, the application provides a basic description of each vulnerability and a list of related reference documentation. If you selected a *High* level of technical detail, it adds a narrative of how it found the vulnerability to the description, as well as remediation options. Use this section to help you understand and fix vulnerabilities.

This section does not distinguish between potential and confirmed vulnerabilities.

Vulnerability filters can be applied.

Executive Summary

This section provides statistics and a high-level summation of the scan data, including numbers and types of network vulnerabilities.

Highest Risk Vulnerability Details

This section lists highest risk vulnerabilities and includes their categories, risk scores, and their Common Vulnerability Scoring System (CVSS) Version 2 scores. The section also provides references for obtaining more information about each vulnerability.

Index of Vulnerabilities

This section includes the following information about each discovered vulnerability:

- severity level
- Common Vulnerability Scoring System (CVSS) Version 2 rating
- category
- URLs for reference
- description
- solution steps

In generated reports, this section appears with the heading *Vulnerability Details*.

Vulnerability filters can be applied.

Payment Card Industry (PCI) Component Compliance Summary

This section lists each scanned IP address with a Pass or Fail result.

Payment Card Industry (PCI) Executive Summary

This section includes a statement as to whether a set of assets collectively passes or fails to comply with PCI security standards. It also lists each scanned asset and indicates whether that asset passes or fails to comply with the standards.

Payment Card Industry (PCI) Host Details

This section lists information about each scanned asset, including its hosted operating system, names, PCI compliance status, and granular vulnerability information tailored for PCI scans.

Payment Card Industry (PCI) Scan Information

This section includes name fields for the scan customer and approved scan vendor (ASV). The customer's name must be entered manually. If the ASV has configured the oem.xml file to auto-populate the name field, it will contain the ASV's name. Otherwise, the ASV's name must be entered manually as well. For more information, see the *ASV guide*, which you can request from Technical Support.

This section also includes the date the scan was completed and the scan expiration date, which is the last day that the scan results are valid from a PCI perspective.

Payment Card Industry (PCI) Scanned Hosts/Networks

This section lists the range of scanned assets.

Note: Any instance of remote access software or directory browsing is automatically noted.

Payment Card Industry (PCI) Special Notes

In this PCI report section, ASVs manually enter the notes about any scanned software that may pose a risk due to insecure implementation, rather than an exploitable vulnerability. The notes should include the following information:

- the IP address of the affected asset
- the note statement, written according to PCIco (see the *PCI ASV Program Guide v1.2*)
- the type of special note, which is one of four types specified by PCIco (see the *PCI ASV Program Guide v1.2*)
- the scan customer's declaration of secure implementation or description of action taken to either remove the software or secure it

Payment Card Industry (PCI) Vulnerabilities Noted for each IP Address

This section includes a table listing each discovered vulnerability with a set of attributes including PCI severity, CVSS score, and whether the vulnerability passes or fails the scan. The assets are sorted by IP address. If the ASV marked a vulnerability for exception, the exception is indicated here. The column labeled *Exceptions, False Positives, or Compensating Controls* field in the PCI Executive Summary report is auto-populated with the user name of the individual who excluded a given vulnerability.

Note: The PCI Vulnerability Details report takes into account approved vulnerability exceptions to determine compliance status for each vulnerability instance.

Payment Card Industry (PCI) Vulnerability Details

This section contains in-depth information about each vulnerability included in a PCI Audit report. It quantifies the vulnerability according to its severity level and its Common Vulnerability Scoring System (CVSS) Version 2 rating.

This latter number is used to determine whether the vulnerable assets in question comply with PCI security standards, according to the CVSS v2 metrics. Possible scores range from 1.0 to 10.0. A score of 4.0 or higher indicates failure to comply, with some exceptions. For more information about CVSS scoring or go to the FIRST Web site at http://www.first.org/cvss/cvss-guide.html.

Payment Card Industry (PCI) Vulnerability Synopsis

This section lists vulnerabilities by categories, such as types of client applications and server-side software.

Policy Evaluation

This sections lists the results of any policy evaluations, such as whether Microsoft security templates are in effect on scanned systems. Section contents include system settings, registry settings, registry ACLs, file ACLs, group membership, and account privileges.

Remediation Plan

This section consolidates information about all vulnerabilities and provides a plan for remediation. The database of vulnerabilities feeds the *Remediation Plan* section with information about patches and fixes, including Web links for downloading them. For each remediation, the database provides a time estimate. Use this section to research fixes, patches, work-arounds, and other remediation measures.

Vulnerability filters can be applied.

Risk Assessment

This section ranks each node (asset) by its risk index score, which indicates the risk that asset poses to network security. An asset's confirmed and unconfirmed vulnerabilities affect its risk score.

Risk Trend

This section enables you to create graphs illustrating risk trends in reports in your Executive Summary. The reports can include your five highest risk sites, asset groups, assets, or you can select all assets in your report scope.

Scanned Hosts and Networks

This section lists the assets that were scanned. If the IP addresses are consecutive, the console displays the list as a range.

Table of Contents

This section lists the contents of the report.

Trend Analysis

This section appears when you select the Baseline report template. It compares the vulnerabilities discovered in a scan against those discovered in a baseline scan. Use this section to gauge progress in reducing vulnerabilities improving network's security.

Vulnerabilities by IP Address and PCI Severity Level

This section, which appears in PCI Audit reports, lists each vulnerability, indicating whether it has passed or failed in terms of meeting PCI compliance criteria. The section also includes remediation information.

Vulnerability Details

The Vulnerability Details section includes statistics and descriptions for each discovered vulnerability, including affected IP address, Common Vulnerability Enumeration (CVE) identifier, CVSS score, PCI severity, and whether the vulnerability passes or fails the scan. Vulnerabilities are grouped by severity level, and within grouping vulnerabilities are listed according to CVSS score.

Vulnerability Exception Activity

Use this template to view all vulnerability exceptions that were applied or requested within a specified time period. The report includes information about each exception or exception request, including the parties involved, statuses, and the reasons for the exceptions. This information is useful for examining your organization's vulnerability management practices.

Vulnerability Exceptions

This section lists each vulnerability that has been excluded from report and the reason for each exclusion. You may not wish to see certain vulnerabilities listed with others, such as those to be

targeted for remediation; but business policies may dictate that you list excluded vulnerabilities if only to indicate that they were excluded. A typical example is the PCI Audit report. Vulnerabilities of a certain severity level may result in an audit failure. They may be excluded for certain reasons, but the exclusions must be noted.

Do not confuse an excluded vulnerability with a disabled vulnerability check. An excluded vulnerability has been discovered by the application, which means the check was enabled.

Vulnerability filters can be applied.

Vulnerability Report Card by Node

This section lists the results of vulnerability tests for each node (asset) in the network. Use this section to assess the vulnerability of each asset.

Vulnerability filters can be applied.

Vulnerability Report Card Across Network

This section lists all tested vulnerabilities, and indicates how each node (asset) in the network responded when the application attempted to confirm a vulnerability on it. Use this section as an overview of the network's susceptibility to each vulnerability.

Vulnerability filters can be applied.

Vulnerability Test Errors

This section displays vulnerabilities that were not confirmed due to unexpected failures. Use this section to anticipate or prevent system errors and to validate that scan parameters are set properly.

Vulnerability filters can be applied.

Export template attributes

When creating a custom export template, you can select from a full set of vulnerability data attributes. The following table lists the name and description of each attribute that you can include.

Attribute name	Description
Asset Alternate IPv4 Addresses	This is the set of alternate IPv4 addresses of the scanned asset.
Asset Alternate IPv6 Addresses	This is the set of alternate IPv6 addresses of the scanned asset.
Asset IP Address	This is the IP address of the scanned asset.
Asset MAC Addresses	These are the MAC addresses of the scanned asset. In the case of multi-homed assets, multiple MAC addresses are separated by commas. Example: 00:50:56:39:06:F5, 00:50:56:39:06:F6
Asset Names	These are the host names of the scanned asset. On the Assets page, asset names may be referred to as *aliases*.
Asset OS Family	This is the fingerprinted operating system family of the scanned asset. Only the family with the highest-certainty fingerprint is listed. Examples: Linux, Windows
Asset OS Name	This is the fingerprinted operating system of the scanned asset. Only the operating system with the highest-certainty fingerprint is listed.
Asset OS Version	This is the fingerprinted version number of the scanned asset's operating system. Only the version with the highest-certainty fingerprint is listed.
Asset Risk Score	This is the overall risk score of the scanned asset when the vulnerability test was run. Note that this is different from the vulnerability risk score, which is the specific risk score associated with the vulnerability.
Exploit Count	This is the number of exploits associated with the vulnerability.

Attribute name	Description
Exploit Minimum Skill	This is the minimum skill level required to exploit the vulnerability.
Exploit URLs	These are the URLs for all exploits as published by Metasploit or the Exploit Database.
Malware Kit Names	These are the malware kits associated with the vulnerability. Multiple kits are separated by commas.
Malware Kit Count	This is the number of malware kits associated with the vulnerability.
Scan ID	This is the ID for the scan during which the vulnerability test was performed as displayed in a site's scan history. It is the last scan during which the asset was scanned. Different assets within the same site may point to different scan IDs as of individual asset scans (as opposed to site scans).
Scan Template	This is the name of the scan template currently applied to the scanned asset's site. It may or may not be the template used for the scan during which the vulnerability was discovered, since a user could have changed the template since the scan was last run.
Service Name	This is the fingerprinted service type of the port on which the vulnerability was tested. Examples: HTTP, CIFS, SSHIn the case of operating system checks, the service name is listed as *System*.
Service Port	This is the port on which the vulnerability was found. For example, all HTTP-related vulnerabilities are mapped to the port on which the Web server was found.In the case of operating system checks, the port number is 0.
Service Product	This is the fingerprinted product that was running the scanned service on the port where the vulnerability was found.In the case of operating system checks, this column is blank.
Service Protocol	This is the network protocol of the scanned port. Examples: TCP, UDP

Attribute name	Description
Site Importance	This is the site importance according to the current site configuration at the time of the CSV export. See *Getting started: Info & Security* on page 61.
Site Name	This is the name of the site to which the scanned asset belongs.
Vulnerability Additional URLs	There are the URLs that provide information about the vulnerability in addition to those cited as Vulnerability Reference URLs. They appear in *References* table of vulnerability details page, labeled as *URL*. Multiple URLs are separated by commas.
Vulnerability Age	This is the number of days since the vulnerability was first discovered on the scanned asset.
Vulnerability CVE IDs	These are the Common Vulnerabilities and Exposure (CVE) IDs associated with the vulnerability. If the vulnerability has multiple CVE IDs, the 10 most recent IDs are listed. For multiple values, each value is separated by a comma and space.
Vulnerability CVE URLs	This is the URL of the CVE's entry in the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). For multiple values, each value is separated by a comma and space.
Vulnerability CVSS Score	This is the vulnerability's Common Vulnerability Scoring System (CVSS) score according to CVSS 2.0 specification.
Vulnerability CVSS Vector	This is the vulnerability's Common Vulnerability Scoring System (CVSS) vector according to CVSS 2.0 specification.
Vulnerability Description	This is useful information about the vulnerability as displayed in the vulnerability details page. Descriptions can include a substantial amount of text. You may need to expand the column in the spreadsheet program for better reading. This value can include line breaks and appears in double quotation marks.
Vulnerability ID	This is the unique identifier for the vulnerability as assigned by Nexpose.

Attribute name	Description
Vulnerability PCI Compliance Status	This is the PCI status if the asset is found to be vulnerable.If an asset is not found to be vulnerable, the PCI severity level is not calculated, and the value is Not Applicable.If an asset is found to be vulnerable, the PCI severity is calculated, and the value is either Pass or Fail.If the vulnerability instance on the asset is excluded, the value is Pass.
Vulnerability Proof	This is the method used to prove that the vulnerability exists or doesn't exist as reported by Scan Engine. Proofs can include a substantial amount of text. You may need to expand the column in the spreadsheet program for better reading. This value can include line breaks and appears in double quotation marks.
Vulnerability Published Date	This is the date when information about the vulnerability was first released.
Vulnerability Reference IDs	These are reference identifiers of the vulnerability, typically assigned by vendors such as Microsoft, Apple, and Redhat or security groups such as Secunia; SysAdmin, Audit, Network, Security (SANS) Institute; Computer Emergency Readiness Team (CERT); and SecurityFocus. These appear in the *References* table of the vulnerability details page. The format of this attribute is Source:Identifier. Multiple values are separated by commas and spaces.Example: BID:4241, CALDERA:CSSA-2002-012.0, CONECTIVA:CLA-2002:467, DEBIAN:DSA-119, MANDRAKE:MDKSA-2002:019, NETBSD:NetBSD-SA2002-004, OSVDB:730, REDHAT:RHSA-2002:043, SANS-02:U3, XF:openssh-channel-error(8383)
Vulnerability Reference URLs	These are reference URLs for information about the vulnerability. They appear in the *References* table of the vulnerability details page. Multiple values separated by commas.Example: http://www.securityfocus.com/bid/29179, http://www.cert.org/advisories/TA08-137A.html, http://www.kb.cert.org/vuls/id/925211, http://www.debian.org/security/DSA-/DSA-1571, http://www.debian.org/security/DSA-/DSA-1576, http://secunia.com/advisories/30136/, http://secunia.com/advisories/30220/

Attribute name	Description
Vulnerability Risk Score	This is the risk score assigned to the vulnerability. Note that this is different from the asset risk score, which is the overall risk score of the asset.
Vulnerable Since	This is the date when the vulnerability was first discovered on the scanned asset.
Vulnerability Solution	This is the solution for remediating the vulnerability. Currently, a solution is exported even if the vulnerability test result was negative. Solutions can include a substantial amount of text. You may need to expand the column in the spreadsheet program for better reading. This value can include line breaks and appears in double quotation marks.
Vulnerability Tags	These are tags assigned by Nexposefor the vulnerability.
Vulnerability Test Result Description	This is the word or phrase describing the vulnerability test result. See *Vulnerability result codes* on page 560.
Vulnerability Test Date	This is the date when the vulnerability test was run. It is the same as the last date that asset was scanned. Format: mm/dd/YYYY
Vulnerability Test Result Code	This is the result code for the vulnerability test. See *Vulnerability result codes* on page 560.
Vulnerability Severity Level	This is the vulnerability's numeric severity level assigned byNexpose. Scores range from 1 to 10 and map to severity rankings in the Vulnerability Listing table of the Vulnerabilities page: 1-3=*Moderate*; 4-7=*Severe*; and 8-10=*Critical*. This is not the PCI severity level.
Vulnerability Title	This is the name of the vulnerability.

Glossary

API (application programming interface)

An API is a function that a developer can integrate with another software application by using program calls. The term *API* also refers to one of two sets of XML APIs, each with its own included operations: API v1.1 and Extended API v1.2. To learn about each API, see the API documentation, which you can download from the *Support* page in Help.

Appliance

An Appliance is a set of Nexpose components shipped as a dedicated hardware/software unit. Appliance configurations include a Security Console/Scan Engine combination and an Scan Engine-only version.

Asset

An asset is a single device on a network that the application discovers during a scan. In the Web interface and API, an asset may also be referred to as a *device*. See *Managed asset* on page 724 and *Unmanaged asset* on page 732. An asset's data has been integrated into the scan database, so it can be listed in sites and asset groups. In this regard, it differs from a *node*. See *Node* on page 725.

Asset group

An asset group is a logical collection of managed assets to which specific members have access for creating or viewing reports or tracking remediation tickets. An asset group may contain assets that belong to multiple sites or other asset groups. An asset group is either static or dynamic. An asset group is not a site. See *Site* on page 730, *Dynamic asset group* on page 722, and *Static asset group* on page 730.

Asset Owner

Asset Owner is one of the preset roles. A user with this role can view data about discovered assets, run manual scans, and create and run reports in accessible sites and asset groups.

Asset Report Format (ARF)

The Asset Report Format is an XML-based report template that provides asset information based on connection type, host name, and IP address. This template is required for submitting reports of policy scan results to the U.S. government for SCAP certification.

Asset search filter

An asset search filter is a set of criteria with which a user can refine a search for assets to include in a dynamic asset group. An asset search filter is different from a *Dynamic Discovery filter* on page 722.

Authentication

Authentication is the process of a security application verifying the logon credentials of a client or user that is attempting to gain access. By default the application authenticates users with an internal process, but you can configure it to authenticate users with an external LDAP or Kerberos source.

Average risk

Average risk is a setting in risk trend report configuration. It is based on a calculation of your risk scores on assets over a report date range. For example, average risk gives you an overview of how vulnerable your assets might be to exploits whether it's high or low or unchanged. Some assets have higher risk scores than others. Calculating the average score provides a high-level view of how vulnerable your assets might be to exploits.

Benchmark

In the context of scanning for FDCC policy compliance, a benchmark is a combination of policies that share the same source data. Each policy in the Policy Manager contains some or all of the rules that are contained within its respective benchmark. See *Federal Desktop Core Configuration (FDCC)* on page 723 and *United States Government Configuration Baseline (USGCB)* on page 731.

Breadth

Breadth refers to the total number of assets within the scope of a scan.

Category

In the context of scanning for FDCC policy compliance, a category is a grouping of policies in the Policy Manager configuration for a scan template. A policy's category is based on its source, purpose, and other criteria. See*Policy Manager* on page 726, *Federal Desktop Core Configuration (FDCC)* on page 723, and *United States Government Configuration Baseline (USGCB)* on page 731.

Check type

A check type is a specific kind of check to be run during a scan. Examples: The Unsafe check type includes aggressive vulnerability testing methods that could result in Denial of Service on target

assets; the Policy check type is used for verifying compliance with policies. The check type setting is used in scan template configurations to refine the scope of a scan.

Center for Internet Security (CIS)

Center for Internet Security (CIS) is a not-for-profit organization that improves global security posture by providing a valued and trusted environment for bridging the public and private sectors. CIS serves a leadership role in the shaping of key security policies and decisions at the national and international levels. The Policy Manager provides checks for compliance with CIS benchmarks including technical control rules and values for hardening network devices, operating systems, and middleware and software applications. Performing these checks requires a license that enables the Policy Manager feature and CIS scanning. See *Policy Manager* on page 726.

Command console

The command console is a page in the Security Console Web interface for entering commands to run certain operations. When you use this tool, you can see real-time diagnostics and a behind-the-scenes view of Security Console activity. To access the command console page, click the **Run console commands** link next to the *Troubleshooting* item on the *Administration* page.

Common Configuration Enumeration (CCE)

Common Configuration Enumeration (CCE) is a standard for assigning unique identifiers known as CCEs to configuration controls to allow consistent identification of these controls in different environments. CCE is implemented as part of its compliance with SCAP criteria for an Unauthenticated Scanner product.

Common Platform Enumeration (CPE)

Common Platform Enumeration (CPE) is a method for identifying operating systems and software applications. Its naming scheme is based on the generic syntax for Uniform Resource Identifiers (URI). CCE is implemented as part of its compliance with SCAP criteria for an Unauthenticated Scanner product.

Common Vulnerabilities and Exposures (CVE)

The Common Vulnerabilities and Exposures (CVE) standard prescribes how the application should identify vulnerabilities, making it easier for security products to exchange vulnerability data. CVE is implemented as part of its compliance with SCAP criteria for an Unauthenticated Scanner product.

Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System (CVSS) is an open framework for calculating vulnerability risk scores. CVSS is implemented as part of its compliance with SCAP criteria for an Unauthenticated Scanner product.

Compliance

Compliance is the condition of meeting standards specified by a government or respected industry entity. The application tests assets for compliance with a number of different security standards, such as those mandated by the Payment Card Industry (PCI) and those defined by the National Institute of Standards and Technology (NIST) for Federal Desktop Core Configuration (FDCC).

Continuous scan

A continuous scan starts over from the beginning if it completes its coverage of site assets within its scheduled window. This is a site configuration setting.

Coverage

Coverage indicates the scope of vulnerability checks. A coverage improvement listed on the News page for a release indicates that vulnerability checks have been added or existing checks have been improved for accuracy or other criteria.

Criticality

Criticality is a value that you can apply to an asset with a RealContext tag to indicate its importance to your business. Criticality levels range from *Very Low* to *Very High*. You can use applied criticality levels to alter asset risk scores. See *Criticality-adjusted risk*.

Criticality-adjusted risk

or

Context-driven risk

Criticality-adjusted risk is a process for assigning numbers to criticality levels and using those numbers to multiply risk scores.

Custom tag

With a custom tag you can identify assets by according to any criteria that might be meaningful to your business.

Depth

Depth indicates how thorough or comprehensive a scan will be. Depth refers to level to which the application will probe an individual asset for system information and vulnerabilities.

Discovery (scan phase)

Discovery is the first phase of a scan, in which the application finds potential scan targets on a network. Discovery as a scan phase is different from *Dynamic Discovery* on page 722.

Document report template

Document templates are designed for human-readable reports that contain asset and vulnerability information. Some of the formats available for this template type—Text, PDF, RTF, and HTML—are convenient for sharing information to be read by stakeholders in your organization, such as executives or security team members tasked with performing remediation.

Dynamic asset group

A dynamic asset group contains scanned assets that meet a specific set of search criteria. You define these criteria with asset search filters, such as IP address range or operating systems. The list of assets in a dynamic group is subject to change with every scan or when vulnerability exceptions are created. In this regard, a dynamic asset group differs from a static asset group. See *Asset group* on page 718 and *Static asset group* on page 730.

Dynamic Discovery

Dynamic Discovery is a process by which the application automatically discovers assets through a connection with a server that manages these assets. You can refine or limit asset discovery with criteria filters. Dynamic discovery is different from *Discovery (scan phase)* on page 722.

Dynamic Discovery filter

A Dynamic Discovery filter is a set of criteria refining or limiting Dynamic Discovery results. This type of filter is different from an *Asset search filter* on page 719.

Dynamic Scan Pool

The Dynamic Scan Pool feature allows you to use Scan Engine pools to enhance the consistency of your scan coverage. A Scan Engine pool is a group of shared Scan Engines that can be bound to a site so that the load is distributed evenly across the shared Scan Engines. You can configure scan pools using the Extended API v1.2.

Dynamic site

A dynamic site is a collection of assets that are targeted for scanning and that have been discovered through vAsset discovery. Asset membership in a dynamic site is subject to change if the discovery connection changes or if filter criteria for asset discovery change. See *Static site* on page 731, *Site* on page 730, and *Dynamic Discovery* on page 722.

Exploit

An exploit is an attempt to penetrate a network or gain access to a computer through a security flaw, or vulnerability. Malicious exploits can result in system disruptions or theft of data. Penetration testers use benign exploits only to verify that vulnerabilities exist. The Metasploit product is a tool for performing benign exploits. See *Metasploit* on page 725 and *Published exploit* on page 727.

Export report template

Export templates are designed for integrating scan information into external systems. The formats available for this type include various XML formats, Database Export, and CSV.

Exposure

An exposure is a vulnerability, especially one that makes an asset susceptible to attack via malware or a known exploit.

Extensible Configuration Checklist Description Format (XCCDF)

As defined by the National Institute of Standards and Technology (NIST), Extensible Configuration Checklist Description Format (XCCDF) “is a specification language for writing security checklists, benchmarks, and related documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring.” Policy Manager checks for FDCC policy compliance are written in this format.

False positive

A false positive is an instance in which the application flags a vulnerability that doesn’t exist. A false negative is an instance in which the application fails to flag a vulnerability that does exist.

Federal Desktop Core Configuration (FDCC)

The Federal Desktop Core Configuration (FDCC) is a grouping of configuration security settings recommended by the National Institute of Standards and Technology (NIST) for computers that are connected directly to the network of a United States government agency. The Policy

Manager provides checks for compliance with these policies in scan templates. Performing these checks requires a license that enables the Policy Manager feature and FDCC scanning.

Fingerprinting

Fingerprinting is a method of identifying the operating system of a scan target or detecting a specific version of an application.

Global Administrator

Global Administrator is one of the preset roles. A user with this role can perform all operations that are available in the application and they have access to all sites and asset groups.

Host

A host is a physical or virtual server that provides computing resources to a guest virtual machine. In a high-availability virtual environment, a host may also be referred to as a node. The term *node* has a different context in the application. See *Node* on page 725.

Latency

Latency is the delay interval between the time when a computer sends data over a network and another computer receives it. Low latency means short delays.

Locations tag

With a *Locations* tag you can identify assets by their physical or geographic locations.

Malware

Malware is software designed to disrupt or deny a target systems's operation, steal or compromise data, gain unauthorized access to resources, or perform other similar types of abuse. The application can determine if a vulnerability renders an asset susceptible to malware attacks.

Malware kit

Also known as an exploit kit, a malware kit is a software bundle that makes it easy for malicious parties to write and deploy code for attacking target systems through vulnerabilities.

Managed asset

A managed asset is a network device that has been discovered during a scan and added to a site's target list, either automatically or manually. Only managed assets can be checked for vulnerabilities and tracked over time. Once an asset becomes a managed asset, it counts against the maximum number of assets that can be scanned, according to your license.

Manual scan

A manual scan is one that you start at any time, even if it is scheduled to run automatically at other times. Synonyms include *ad-hoc scan* and *unscheduled scan*.

Metasploit

Metasploit is a product that performs benign exploits to verify vulnerabilities. See *Exploit* on page 723.

MITRE

The MITRE Corporation is a body that defines standards for enumerating security-related concepts and languages for security development initiatives. Examples of MITRE-defined enumerations include Common Configuration Enumeration (CCE) and Common Vulnerability Enumeration (CVE). Examples of MITRE-defined languages include Open Vulnerability and Assessment Language (OVAL). A number of MITRE standards are implemented, especially in verification of FDCC compliance.

National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce. The agency mandates and manages a number of security initiatives, including Security Content Automation Protocol (SCAP). See *Security Content Automation Protocol (SCAP)* on page 729.

Node

A node is a device on a network that the application discovers during a scan. After the application integrates its data into the scan database, the device is regarded as an *asset* that can be listed in sites and asset groups. See *Asset* on page 718.

Open Vulnerability and Assessment Language (OVAL)

Open Vulnerability and Assessment Language (OVAL) is a development standard for gathering and sharing security-related data, such as FDCC policy checks. In compliance with an FDCC requirement, each OVAL file that the application imports during configuration policy checks is available for download from the *SCAP* page in the Security Console Web interface.

Override

An override is a change made by a user to the result of a check for compliance with a configuration policy rule. For example, a user may override a Fail result with a Pass result.

Payment Card Industry (PCI)

The Payment Card Industry (PCI) is a council that manages and enforces the PCI Data Security Standard for all merchants who perform credit card transactions. The application includes a scan template and report templates that are used by Approved Scanning Vendors (ASVs) in official merchant audits for PCI compliance.

Permission

A permission is the ability to perform one or more specific operations. Some permissions only apply to sites or asset groups to which an assigned user has access. Others are not subject to this kind of access.

Policy

A policy is a set of primarily security-related configuration guidelines for a computer, operating system, software application, or database. Two general types of polices are identified in the application for scanning purposes: *Policy Manager* policies and *standard* policies. The application's Policy Manager (a license-enabled feature) scans assets to verify compliance with policies encompassed in the United States Government Configuration Baseline (USGCB), the Federal Desktop Core Configuration (FDCC), Center for Internet Security (CIS), and Defense Information Systems Agency (DISA) standards and benchmarks, as well as user-configured custom policies based on these policies. See *Policy Manager* on page 726, *Federal Desktop Core Configuration (FDCC)* on page 723, *United States Government Configuration Baseline (USGCB)* on page 731, and *Scan* on page 728. The application also scans assets to verify compliance with standard policies. See *Scan* on page 728 and *Standard policy* on page 730.

Policy Manager

Policy Manager is a license-enabled scanning feature that performs checks for compliance with Federal Desktop Core Configuration (FDCC), United States Government Configuration Baseline (USGCB), and other configuration policies. Policy Manager results appear on the *Policies* page, which you can access by clicking the **Policies** tab in the Web interface. They also appear in the *Policy Listing* table for any asset that was scanned with Policy Manager checks. Policy Manager policies are different from standard policies, which can be scanned with a basic license. See *Policy* on page 726 and *Standard policy* on page 730.

Policy Result

In the context of FDCC policy scanning, a result is a state of compliance or non-compliance with a rule or policy. Possible results include *Pass*, *Fail*, or *Not Applicable*.

Policy Rule

A rule is one of a set of specific guidelines that make up an FDCC configuration policy. See *Federal Desktop Core Configuration (FDCC)* on page 723, *United States Government Configuration Baseline (USGCB)* on page 731, and *Policy* on page 726.

Potential vulnerability

A potential vulnerability is one of three positive vulnerability check result types. The application reports a potential vulnerability during a scan under two conditions: First, potential vulnerability checks are enabled in the template for the scan. Second, the application determines that a target is running a vulnerable software version but it is unable to verify that a patch or other type of remediation has been applied. For example, an asset is running version 1.1.1 of a database. The vendor publishes a security advisory indicating that version 1.1.1 is vulnerable. Although a patch is installed on the asset, the version remains 1.1.1. In this case, if the application is running checks for potential vulnerabilities, it can only flag the host asset as being potentially vulnerable. The code for a potential vulnerability in XML and CSV reports is *vp* (vulnerable, potential). For other positive result types, see *Vulnerability check* on page 733.

Published exploit

In the context of the application, a published exploit is one that has been developed in Metasploit or listed in the Exploit Database. See *Exploit* on page 723.

RealContext

RealContext is a feature that enables you to tag assets according to how they affect your business. You can use tags to specify the criticality, location, or ownership. You can also use custom tags to identify assets according any criteria that is meaningful to your organization.

Real Risk strategy

Real Risk is one of the built-in strategies for assessing and analyzing risk. It is also the recommended strategy because it applies unique exploit and malware exposure metrics for each vulnerability to Common Vulnerability Scoring System (CVSS) base metrics for likelihood (access vector, access complexity, and authentication requirements) and impact to affected assets (confidentiality, integrity, and availability). See *Risk strategy* on page 728.

Report template

Each report is based on a template, whether it is one of the templates that is included with the product or a customized template created for your organization. See *Document report template* on page 722 and *Export report template* on page 723.

Risk

In the context of vulnerability assessment, risk reflects the likelihood that a network or computer environment will be compromised, and it characterizes the anticipated consequences of the compromise, including theft or corruption of data and disruption to service. Implicitly, risk also reflects the potential damage to a compromised entity's financial well-being and reputation.

Risk score

A risk score is a rating that the application calculates for every asset and vulnerability. The score indicates the potential danger posed to network and business security in the event of a malicious exploit. You can configure the application to rate risk according to one of several built-in risk strategies, or you can create custom risk strategies.

Risk strategy

A risk strategy is a method for calculating vulnerability risk scores. Each strategy emphasizes certain risk factors and perspectives. Four built-in strategies are available: *Real Risk strategy* on page 727, *TemporalPlus risk strategy* on page 731, *Temporal risk strategy* on page 731, and *Weighted risk strategy* on page 733. You can also create custom risk strategies.

Risk trend

A risk trend graph illustrates a long-term view of your assets' probability and potential impact of compromise that may change over time. Risk trends can be based on average or total risk scores. The highest-risk graphs in your report demonstrate the biggest contributors to your risk on the site, group, or asset level. Tracking risk trends helps you assess threats to your organization's standings in these areas and determine if your vulnerability management efforts are satisfactorily maintaining risk at acceptable levels or reducing risk over time. See *Average risk* on page 719 and *Total risk* on page 731.

Role

A role is a set of permissions. Five preset roles are available. You also can create custom roles by manually selecting permissions. See *Asset Owner* on page 718, *Security Manager* on page 730, *Global Administrator* on page 724, *Site Owner* on page 730, and *User* on page 732.

Scan

A scan is a process by which the application discovers network assets and checks them for vulnerabilities. See *Exploit* on page 723 and *Vulnerability check* on page 733.

Scan credentials

Scan credentials are the user name and password that the application submits to target assets for authentication to gain access and perform deep checks. Many different authentication mechanisms are supported for a wide variety of platforms. See *Shared scan credentials* on page 730 and *Site-specific scan credentials* on page 730.

Scan Engine

The Scan Engine is one of two major application components. It performs asset discovery and vulnerability detection operations. Scan engines can be *distributed* within or outside a firewall for varied coverage. Each installation of the Security Console also includes a local engine, which can be used for scans within the console's network perimeter.

Scan template

A scan template is a set of parameters for defining how assets are scanned. Various preset scan templates are available for different scanning scenarios. You also can create custom scan templates. Parameters of scan templates include the following:

- methods for discovering assets and services
- types of vulnerability checks, including safe and unsafe
- Web application scanning properties
- verification of compliance with policies and standards for various platforms

Scheduled scan

A scheduled scan starts automatically at predetermined points in time. The scheduling of a scan is an optional setting in site configuration. It is also possible to start any scan manually at any time.

Security Console

The Security Console is one of two major application components. It controls Scan Engines and retrieves scan data from them. It also controls all operations and provides a Web-based user interface.

Security Content Automation Protocol (SCAP)

Security Content Automation Protocol (SCAP) is a collection of standards for expressing and manipulating security data. It is mandated by the U.S. government and maintained by the National Institute of Standards and Technology (NIST). The application complies with SCAP criteria for an Unauthenticated Scanner product.

Security Manager

Security Manager is one of the preset roles. A user with this role can configure and run scans, create reports, and view asset data in accessible sites and asset groups.

Shared scan credentials

One of two types of credentials that can be used for authenticating scans, shared scan credentials are created by Global Administrators or users with the Manage Site permission. Shared credentials can be applied to multiple assets in any number of sites. See *Site-specific scan credentials* on page 730.

Site

A site is a collection of assets that are targeted for a scan. Each site is associated with a list of target assets, a scan template, one or more Scan Engines, and other scan-related settings. See *Dynamic site* on page 723 and *Static site* on page 731. A site is not an asset group. See *Asset group* on page 718.

Site-specific scan credentials

One of two types of credentials that can be used for authenticating scans, a set of single-instance credentials is created for an individual site configuration and can only be used in that site. See *Scan credentials* on page 729 and *Shared scan credentials* on page 730.

Site Owner

Site Owner is one of the preset roles. A user with this role can configure and run scans, create reports, and view asset data in accessible sites.

Standard policy

A standard policy is one of several that the application can scan with a basic license, unlike with a Policy Manager policy. Standard policy scanning is available to verify certain configuration settings on Oracle, Lotus Domino, AS/400, Unix, and Windows systems. Standard policies are displayed in scan templates when you include policies in the scope of a scan. Standard policy scan results appear in the *Advanced Policy Listing* table for any asset that was scanned for compliance with these policies. See *Policy* on page 726.

Static asset group

A static asset group contains assets that meet a set of criteria that you define according to your organization's needs. Unlike with a dynamic asset group, the list of assets in a static group does not change unless you alter it manually. See *Dynamic asset group* on page 722.

Static site

A static site is a collection of assets that are targeted for scanning and that have been manually selected. Asset membership in a static site does not change unless a user changes the asset list in the site configuration. For more information, see *Dynamic site* on page 723 and *Site* on page 730.

Temporal risk strategy

One of the built-in risk strategies, Temporal indicates how time continuously increases likelihood of compromise. The calculation applies the age of each vulnerability, based on its date of public disclosure, as a multiplier of CVSS base metrics for likelihood (access vector, access complexity, and authentication requirements) and asset impact (confidentiality, integrity, and availability). Temporal risk scores will be lower than TemporalPlus scores because Temporal limits the risk contribution of partial impact vectors. See *Risk strategy* on page 728.

TemporalPlus risk strategy

One of the built-in risk strategies, TemporalPlus provides a more granular analysis of vulnerability impact, while indicating how time continuously increases likelihood of compromise. It applies a vulnerability's age as a multiplier of CVSS base metrics for likelihood (access vector, access complexity, and authentication requirements) and asset impact (confidentiality, integrity, and availability). TemporalPlus risk scores will be higher than Temporal scores because TemporalPlus expands the risk contribution of partial impact vectors. See *Risk strategy* on page 728.

Total risk

Total risk is a setting in risk trend report configuration. It is an aggregated score of vulnerabilities on assets over a specified period.

United States Government Configuration Baseline (USGCB)

The United States Government Configuration Baseline (USGCB) is an initiative to create security configuration baselines for information technology products deployed across U.S. government agencies. USGCB evolved from FDCC, which it replaces as the configuration security mandate in the U.S. government. The Policy Manager provides checks for Microsoft Windows 7, Windows 7 Firewall, and Internet Explorer for compliance with USGCB baselines. Performing these checks requires a license that enables the Policy Manager feature and USGCB scanning. See *Policy Manager* on page 726 and *Federal Desktop Core Configuration (FDCC)* on page 723.

Unmanaged asset

An unmanaged asset is a device that has been discovered during a scan but not correlated against a managed asset or added to a site's target list. The application is designed to provide sufficient information about unmanaged assets so that you can decide whether to manage them. An unmanaged asset does not count against the maximum number of assets that can be scanned according to your license.

Unsafe check

An unsafe check is a test for a vulnerability that can cause a denial of service on a target system. Be aware that the check itself can cause a denial of service, as well. It is recommended that you only perform unsafe checks on test systems that are not in production.

Update

An update is a released set of changes to the application. By default, two types of updates are automatically downloaded and applied:

Content updates include new checks for vulnerabilities, patch verification, and security policy compliance. Content updates always occur automatically when they are available.

Product updates include performance improvements, bug fixes, and new product features. Unlike content updates, it is possible to disable automatic product updates and update the product manually.

User

User is one of the preset roles. An individual with this role can view asset data and run reports in accessible sites and asset groups.

Validated vulnerability

A validated vulnerability is a vulnerability that has had its existence proven by an integrated Metasploit exploit. See *Exploit* on page 723.

Vulnerable version

Vulnerable version is one of three positive vulnerability check result types. The application reports a vulnerable version during a scan if it determines that a target is running a vulnerable software version and it can verify that a patch or other type of remediation has not been applied. The code for a vulnerable version in XML and CSV reports is *vv* (vulnerable, version check). For other positive result types, see *Vulnerability check* on page 733.

Vulnerability

A vulnerability is a security flaw in a network or computer.

Vulnerability category

A vulnerability category is a set of vulnerability checks with shared criteria. For example, the Adobe category includes checks for vulnerabilities that affect Adobe applications. There are also categories for specific Adobe products, such as *Air*, *Flash*, and *Acrobat/Reader*. Vulnerability check categories are used to refine scope in scan templates. Vulnerability check results can also be filtered according category for refining the scope of reports. Categories that are named for manufacturers, such as *Microsoft*, can serve as supersets of categories that are named for their products. For example, if you filter by the *Microsoft* category, you inherently include all Microsoft product categories, such as *Microsoft Path* and *Microsoft Windows*. This applies to other "company" categories, such as *Adobe*, *Apple*, and *Mozilla*.

Vulnerability check

A vulnerability check is a series of operations that are performed to determine whether a security flaw exists on a target asset. Check results are either negative (no vulnerability found) or positive. A positive result is qualified one of three ways: See *Vulnerability found* on page 733, *Vulnerable version* on page 732, and *Potential vulnerability* on page 727. You can see positive check result types in XML or CSV export reports. Also, in a site configuration, you can set up alerts for when a scan reports different positive results types.

Vulnerability exception

A vulnerability exception is the removal of a vulnerability from a report and from any asset listing table. Excluded vulnerabilities also are not considered in the computation of risk scores.

Vulnerability found

Vulnerability found is one of three positive vulnerability check result types. The application reports a vulnerability found during a scan if it verified the flaw with asset-specific vulnerability tests, such as an exploit. The code for a vulnerability found in XML and CSV reports is ve (vulnerable, exploited). For other positive result types, see *Vulnerability check* on page 733.

Weighted risk strategy

One of the built-in risk strategies, Weighted is based primarily on asset data and vulnerability types, and it takes into account the level of importance, or weight, that you assign to a site when you configure it. See *Risk strategy* on page 728.