RAPID7

Nexpose

Deployment & MVM Migration Utility Guide

Product version: 6.0

Contents

Pre-Deployment & Deployment

Thank you for choosing Rapid7 as your vulnerability management partner. The following sections will help you plan and prepare your Nexpose Deployment.

Initial Setup

For customers who purchased hardware appliances:

- Rack and cable then power-on the appliances.
- Obtain and statically assign an IP address for each appliance.

For customers who purchased virtual appliances:

- Download the virtual appliance OVA file. See the VA Console and VA Engine download page.
- Import the virtual appliance OVA into your VMware environment.
- Obtain and statically assign an IP address for each virtual appliance. See the Virtual Appliance Getting Started Guide and Virtual Appliance Deployment Guide.

For customers who purchased software licenses only (customer provisioned hardware):

- Build out the server and operating system infrastructure according to the documented system requirements or specifications provided by your sales engineer.
- Obtain and statically assign an IP address for each server.
- Disable any solutions that whitelist (e.g., Bit9 or other executable-blocking products).
- Obtain the latest Nexpose installer (optional) for Linux or Windows.
- The following products need to be removed or disabled on the servers hosting the console and engine(s):
    - Anti-virus/Malware
    - Host-based IDS
    - Personal firewalls
    - Any solutions that whitelists executables (e.g., Bit9 or other executable-blocking products)
    - SELinux (for Linux platforms)
- Ensure availability of resources to support mitigation on issues surrounding any of the products or product types listed above.

For all deployments:

- Configure DNS on the console and engines for internal and external name resolution.
- Validate network connectivity
- Apply firewall rules where necessary, in accordance to the Firewall Rules table.
- Validate Internet connectivity to:
  - port 443 at https://support.rapid7.com
  - port 80 at http://updates.rapid7.com
  - If a proxy server is in place, proxy settings will be set in Nexpose. Please have the proxy address and credentials (if necessary) provisioned for the engagement.
  - If the proxy is using content filtering or advanced protocol inspection (i.e. Bluecoat, Ironport, Websense), please whitelist traffic to and from the Nexpose Console and the addresses above.

For customers that purchased shared hosted scan engines:

- Open port 40814 outbound to 208.118.237.0/24 on your perimeter firewall from the Nexpose Console.
- Note that external scans will originate from the following IP source range 208.118.237.0/24.

Planning your Nexpose

Infrastructure Build Out

To get the most out of the deployment, we recommend building out the necessary infrastructure prior to the scheduled deployment engagement. The following information attempts to answer many of the questions you may have.

Supported Operating Systems

Nexpose supports the operating system platforms listed at the Officially Supported Systems page.

Physical vs. Virtual Infrastructure

The Nexpose console and scan engines may be installed on physical or virtual infrastructure. The choice of which platform to deploy is typically a matter of customer preference. Rapid7 provides customers access to virtual appliances, for the console and scan engines, to make the deployment process in a virtual environment easier. These appliances are configured on a hardened Ubuntu Linux image. Though Rapid7 offers these appliances, the operating system configuration is not supported by Rapid7 support. The customer is responsible for maintaining/supporting the appliance operating system (i.e. resizing partitions, configuring systems management, applying operating system updates).

If you have a virtual infrastructure in place near your target assets, it is generally recommendation is to deploy virtual scan engines for that environment.

Nexpose is currently only supported on ESXi 5.0-5.5. Other hypervisors may work, but have not been formally tested or certified by Rapid7, and therefore are not supported by Rapid7.

Vulnerability scanning is a resource intensive process. Both the Nexpose Console and Engines will utilize all the CPU and memory resources that are allocated to it. It is recommended to place these components on a hypervisor host with plenty of resources available and not to oversubscribe the hypervisor host.

Database

Nexpose utilizes its own instance of a PostgreSQL 9.4 database. The database instance will be installed along with the application. No other database platforms are currently supported.

The Nexpose database can be read/write intensive. The former for report generation, and the latter for the integration of scan results into the console for analysis and reporting. Choose your storage location carefully, in some instances, remote storage, such as SAN or NAS, may limit

performance. This is more of a concern where scan data volumes are high and scan intervals are frequent (i.e. 100K+ IPs scanned daily and 100 reports generated daily).

Partitioning

The application/database architecture does not support being split out over multiple partitions. For example, application on one partition and database on another, or database on one partition and transaction logs on another.

The default installation path is /opt/Rapid7/Nexpose, on Linux; and C:\Program Files\Rapid7\Nexpose, on Windows. You may choose an alternate install path during the install process; however, all Nexpose components must be on the same logical partition.

Networking

To achieve the best results, leverage your core network architecture and place the console and engines where there is highest bandwidth and least network latency.

For scanning assets across low band-width WAN connections, you may either:

1. Deploy an engine on the far end of the WAN link. This is ideal when there is a high volume of assets to scan or scanning is frequent (i.e. daily). OR
2. Tune the scan template to prevent saturation of the WAN link. This is ideal when there is a low volume of assets to scan or scanning is infrequent (i.e. monthly).

Nexpose currently supports one network interface per console and scan engine. For optimal results, ensure your console and engines Ethernet interfaces are set to 1Gb full-duplex.

Nexpose does not support 802.1q VLAN tagging within the application. If you wish to utilize 802.1q, you must already have VLAN-aware switches and configure 802.1q at the OS level of your console. This will vary based on the underlying operating system platform. Refer to your operating systems documentation for further information.

Opening and verifying firewall rules

The table below outlines the necessary communication requirements for Nexpose to operate. Assess your environment and determine where firewall or access control changes will need to be made.

Source	Destination	Port
Nexpose Admin/User (Workstation)	Nexpose Console (NSC)	3780
Nexpose Console (NSC)	Remote Scan Engines (NSE)	40814
Nexpose Console (NSC)	Shared Hosted Scan Engines (208.118.237.0/24)	40814
Nexpose Console (NSC)	Dedicated Hosted Scan Engine (Please reach out to your Customer Success Manager or Rapid7 Support for address information)	40814
Nexpose Console (NSC)	Assets/Network that will be scanned from the Console/Local Scan Engine	TCP 1-65535, UDP 1-65535
Nexpose Console (NSC)	updates.rapid7.com	80
Nexpose Console (NSC)	support.rapid7.com	443
Nexpose Console (NSC)	sonar.labs.rapid7.com	443
Nexpose Console (NSC)	vCenter (for vAsset Discovery)	443 (may be custom)
Nexpose Remote Scan Engines (NSE)	Nexpose Console (NSC) - Optional	40815
Nexpose Remote Scan Engines (NSE)	Assets/Networks that will be scanned from the Remote Scan Engine	TCP 1-65535, UDP 1-65535

Hardware and resource requirements

There are a number of factors to consider when sizing your Nexpose Deployment, such as:

- The total number of assets you will be scanning
- The frequency in which you will be scanning (daily, weekly, monthly, quarterly). More frequent scanning will require more hardware resources.
- Timeframes in which scans will be allowed to run (i.e. Scan/Maintenance Windows). Shorter scan windows will require the ability to scan more assets in parallel, which will consume more hardware resources.
- Number of reports that will be generated
- Scan data retention requirements

The below table is a general sizing guideline, based on Rapid7's hardware appliances, to ensuring your allocated hardware and resource requirements will achieve your deployments needs.

Nexpose Scan Console

Memory and storage are the main resources to focus on. Memory is impacted by engines transmitting scan logs for integration into the Nexpose database for analysis. Reporting is another factor for additional memory, as is whether or not you are utilizing the integrated scan engine. For mid-sized to large enterprise deployments, it is not recommended to utilize the integrated scan engine and off-load to a dedicated engine.

Storage needs will vary, from customer-to-customer. A majority of the storage consumption is the database, reports and any backups you may perform. The number of IP's and the frequency of scanning, as well as the number and frequency of running reports, and data retention requirements, will impact storage needs. Virtual deployments have the benefit of being able to provision additional storage as it is needed, rather than upfront.

Nexpose Scan Engine:

Scan engines are the workhorse of Nexpose and perform the actual scans against your assets. When sizing engines, it is generally recommended to favor many smaller engines over fewer larger engines, as the scale is not necessarily linear. Engines can also be placed in engine pools, allowing for fault tolerance and better resource allocation.

Though there is no exact formula for sizing your deployment, the following metrics should give you some general ballparks.

Scan Duration

Credentialed scan duration averages 8-12 minutes, per asset

- Un-credentialed scan duration averages 4-8 minutes, per asset
- Note: assets can be scanned in parallel. The more memory allocated to the engine, the more assets that can be scanned in parallel.

Memory Utilization

- Memory is a critical resource in efficiently and effectively scanning assets. The following formula can be used to estimate memory consumption per scan.
- The key factor is whether the below functions are enabled in the scan template, as memory will be allocated upon scan initialization.
- 1GB +(Concurrent Assets x 100MB) + (Credential Scan? x Threads x 100MB) + (WebApp Scanning? x Threads x 100MB) + (Policy Scanning? x Threads x 100MB)
- True = 1; False = 0
- Example: 1GB +(10 x 100MB) + (1 x 10 x 100MB) + (1 x 10 x 100MB) + (0 x 10 x 100MB) = 4GB
- Add the results to the minimum requirements of the OS.
- If planning to run concurrent scans, calculate the results of each scan and add them together.

Network Bandwidth Utilization

- Network bandwidth utilization averages 1.8Mbps for scanning 10 simultaneous assets.
- Peak bandwidth averages at about 4Mbps.

Disk Utilization

- Average disk usage per asset per scan 50k remote (un-credentialed)
- Average disk usage per asset per scan 500k remote (credentialed)
- Example: 10,000 assets scanned with credentials on a weekly basis = (10,000 x 500k) x 52 = 250GB

• Factor in additional disk space for reports, OS, etc.

Scan Engine Placement

When determining number of scan engines needed, first identify all your network segments and ranges and consider the following:

- Firewalls, ACLs and IPSs will restrict traffic from the scan engine to targets. It is preferable to place an engine behind these devices rather than attempt to scan through them for both accuracy and security concerns. If you scan through one of these devices, ensure to completely whitelist the traffic from the engine. Please note that vulnerability scanning has the potential to exhaust a firewalls connection state table on some firewalls and cause instability.
- Load balancers can also impact performance and accuracy. It is preferable to scan from behind these and only scan the physical IP of the device, not the virtual IP.
- VPNs and low bandwidth connections are performance limiting. A scan engine should be placed on the far end of these connections so only scan results, not the actual scan traffic, are traversing the limited bandwidth network segment.
- It is extremely time consuming to scan empty IP space. If possible, identify an authoritative source of routable network ranges that are currently alive in your environment and only scan populated network segments.

Installing the application

Installation requirements

Make sure that your host hardware and network support Nexpose operations.

Hardware requirements

See the Rapid7 Web site for hardware requirements:

http://www.rapid7.com/products/nexpose/system-requirements.jsp.

It is recommended that you install Nexpose on a computer that does not have an Intrusion Detection System (IDS), an Intrusion Prevention System (IPS), or a firewall enabled. These devices block critical operations that are dependent on network communication.

The 64-bit configuration is recommended for enterprise-scale deployments

System component	Requirement
server	dedicated server with no IPS or IDS
processor	2 GHz
RAM	8 GB
disk space	80 GB + for Security Console with local Scan Engine 10 GB + for distributed Scan Engines
network interface card (NIC)	100 Mbps

Network activities and requirements

The Security Console communicates over the network to perform four major activities:

Activity	Type of communication
manage scan activity on Scan Engines and pull scan data from them	outbound; Scan Engines listen on 40814
download vulnerability checks and feature updates from a server at updates.rapid7.com	outbound; server listens on port 80
upload PGP-encrypted diagnostic information to a server at support.rapid7.com	outbound; server listens on port 443

Activity	Type of communication
provide Web interface access to users	inbound; Security Console accepts HTTPS requests over port 3780

Scan Engines contact target assets using TCP, UDP, and ICMP to perform scans. They do not initiate outbound communication with the Security Console.

Ideally there should be no firewalls or similar devices between a Scan Engine and its target assets. Also, scanning may also require some flexibility in security policies. For more information, see the *administrator's guide*.

Supported platforms

Windows

- Windows Server 2012, Standard, Enterprise 64-bit
- Windows Server 2008 (R2 SP1), Standard, Enterprise 64-bit
- Windows 8 Professional, Enterprise 64-bit

Scanning over IPv6 networks is not supported from a Scan Engine installed on Windows 2003. Also, if your Security Console is installed on Windows 2003, you will not be able to access it over an IPv6 network.

Windows

- Windows Server 2012, Standard, Enterprise 64-bit
- Windows Server 2008 (R2 SP1), Standard, Enterprise 64-bit
- Windows 8 Professional, Enterprise 64-bit
- Windows 7 Professional (RTM and SP1), Ultimate, Enterprise 64-bit *
- Windows 7 Professional (RTM and SP1), Ultimate, Enterprise 32-bit*

**This platform is only supported for the Security Console.*

Scanning over IPv6 networks is not supported from a Scan Engine installed on Windows 2003. Also, if your Security Console is installed on Windows 2003, you will not be able to access it over an IPv6 network.

Linux

- RHEL Server 5.x 64-bit
- RHEL Server 6.x 64-bit

Linux

- RHEL Server 5.x 64-bit
- RHEL Server 6.x 64-bit
- Ubuntu 8.04 LTS 64-bit
- Ubuntu 10.04 LTS 64-bit
- Ubuntu 12.04 LTS 64-bit

Virtual machines

- VMware ESX 4.x
- VMware ESXi 4.x
- VMware ESXi 5.x

Making sure you have necessary items

Make sure you have all of the following items before you begin the installation process:

- installers (32-bit and 64-bit versions) for all supported environments (.bin files for Linux and .exe files for Windows)
- the md5sum, which helps to ensure that installers are not corrupted during download
- documentation, including this guide
- a product key, which you need to activate your license when you log on

If you do not have any of these items, contact your account representative.

If you have not done so yet, download the correct installer for your system, the corresponding hash, and any documentation you need.

Installing in Windows environments

This section describes how to install NexposeSymantec CCS Vulnerability Manager on a Windows host. It also describes options that are available to you during the installation.

During the installation, the installer runs a system check and identifies any system components or settings that meet the minimum requirements but not the recommended requirements. If any items are identified, you can continue the installation, but you should consider modifying your system after the installation to ensure optimal performance. For example, if your system does not have the recommended the amount of RAM, you may encounter performance issues with RAM-intensive operations, such as running scans or reports. To prevent this, you should consider adding RAM to your system.

Uninstalling a previously installed copy

Installing and using multiple copies of the software on the same server is not supported. If you install multiple copies on the same server, the application will not function properly.

Each copy of the software must be installed from scratch. This means that if you already have a copy installed, you must uninstall it before you install the new copy you downloaded.

Use the procedure in the section Running the Windows uninstaller on page 1 to uninstall any previously installed copies.

Creating an account during installation

When you install the application, you create a default Global Administrator account. You will use the account to log onto the application after you complete the installation.

Recovery of credentials is not supported. If you forget your user name or password, you will have to reinstall the program. Credentials are case-sensitive.

As you enter credentials, the complexity requirements are displayed to ensure that you create strong (secure) credentials. Even if your password meets the requirements, it is recommended that you make your password as strong as possible for better security. A “heat bar” is displayed that gradually changes color from red to green as you make your password stronger.

A Global Administrator can create and modify accounts after installation. See *Managing users and authentication* in Help or the administrator’s guide.

Installation choices

During the installation, you will make several choices, including the following:

- Select the component(s) you want to install and where to install them.
- Enable the application to initialize during the installation and start automatically after installation.

Selection of components

You can either install a Security Console with a local Scan Engine or you can install a distributed Scan Engine. If you install the latter, you must have a Security Console running in your environment before you can use the Scan Engine. The Security Console controls all Scan Engine activity.

Application initialization and automatic start option

You can choose to have the application initialize during installation and automatically start once you finish the installation. By default, this option is enabled. If you do not want initialization to occur during installation, you must disable it.

You can only leave this option enabled if you install both components (the Scan Engine and Security Console). If you choose to install only the Scan Engine, this option is not available.

The benefit to leaving the option enabled is that you can start using the application immediately after the installation is complete. This is because the initialization process prepares the application for use by updating the database of vulnerability checks and performing the initial configuration.

Because the time required for the initialization process ranges from 10 to 30 minutes, leaving the option enabled increases the total installation time by 10 to 30 minutes. Although disabling the option shortens the installation time, it takes longer to start the application because it has to initialize before you can begin using it.

Tips for using the installation wizard

The pages of the wizard are listed in the left page of the wizard, and the current page is highlighted. You can use the list to check your progress.

Each page of the wizard has a **Previous** button and a **Cancel** button. Use the **Previous** button to go to a previous page if you need to review or change an installation setting. Use the **Cancel** button only if you need to cancel the installation. If you cancel at any point in during the installation process, no files are installed and you need to go back to the beginning of the installation process.

Before you begin

Confirm the following items:

- You are logged onto Windows as an administrator.
- Your system meets the minimum installation requirements. See Installation requirements on page 1 for details.
- You have all of the items you need to complete the installation. See Making sure you have necessary items on page 1 for details.
- You have uninstalled any previously installed copies of the application. See Running the Windows uninstaller on page 1 for details.

Running the Windows installer

To install the application in Windows, take the following steps:

1. Double-click the **installer icon**.

   The installer displays a message that it is preparing the wizard to guide you through the installation. Then the *Welcome* page of the wizard is displayed.

   Command-line windows open once you begin the installation. Although you do not need them, do not close them.

   Note: The installation will stop if you close the command line interface windows.

   Click **Next**.

2. Read the agreement and select the **I accept the agreement** option. If you do not accept it, you cannot continue the installation.
3. Click **Next**.

   The *Type and destination* page is displayed.

4. Select the components you want to install by doing one of the following:
   - Select the **Security Console with local Scan Engine** option. If you do not install the Security Console, the application cannot initialize during installation.
   - Select the **Scan Engine only** option. If you install only the Scan Engine, you must install the Security Console before you can use the Scan Engine.
     - Select a communication direction. Which option is preferred depends on your network configuration:
       - Engine to Console: The Scan Engine will actively inform the Security Console that it is available for communication. This configuration allows a console that is behind a firewall and is configured to allow inbound connections to establish a communication channel.
       - Console to Engine: The Scan Engine will listen for communication from the Security Console. This configuration is most effective when the engine and console are on the same area of the network.

5. Select where you want to install the components by doing one of the following:

   - Click **Next** to accept the default directory. Go to **step 10**.
   - Change the installation directory by doing one of the following:
     - Enter the preferred installation directory path in **Destination directory** box, then click **Next**.
     - Click **Change** to open the *Select Directory* dialog and select or create the preferred directory, then click OK.

     Note: If your hard drive is partitioned and you select a location on a different partition, make sure that partition has sufficient space.

2. Click **Next**.

   The installer displays the *System check* page.

3. Review the page to make sure your system meets the installation requirements and do one of the following:

   - Click **Next** to continue.

     The installer displays the end-user license agreement.

   - Click **Finish** to end the installation, modify your system as needed, then go back to the beginning of the installation process.

   The installer displays the *User details* page.

6. Enter your first name, last name, and company name in the appropriate boxes.
7. Click **Next**.If you have a product key select the **I already have a product key** option and click **Next**.

   The *Database port* page is displayed. Go to **step 8** to continue.

   If you do not have a product key leave the **I would like to register for a product key** option selected and click **Next**.

   The registration form is displayed.

   a. Enter or select all requested information into the form (all fields are required).

      The phone number must include an area code.

      The e-mail address must be for a valid account that is not associated with a free e-mail service, such as Gmail, Hotmail, or Yahoo!.

   b. Click **Next**. The registration form is submitted. You should receive an e-mail from Rapid7 within 5 minutes that contains the product key.

8. The database port shows in the Database port page. The default port is 5432. You can change it if your network configuration requires it. Click **Next**.

   The *Account details* page is displayed.

9. In the *Account details* page, enter a user name and password. Enter the password again for confirmation, and click **Next**.

   The installer displays the *Shortcut location* page.

10. To choose to have the shortcut, do one of the following:
    - If you do not want to create a shortcut, clear the check box for creating a **Start Menu** folder. Click **Next**. Go to **step 12**.
    - To create a shortcut, leave the check box selected for creating a **Start Menu** folder. Choose the location of the shortcut, do one of the following:
      - To accept the default location (a folder named NexposeSymantec CCS Vulnerability Manager), do not change the location shown in the text box, then click **Next**.
      - To create the shortcut in a different folder, enter the **name of the folder** in the text box or select one of the listed folders, then click **Next**.
      - To make the shortcut to available to all users on the host system, leave the appropriate check box selected. Otherwise, clear it. Then click **Next.**

The *Confirm selections* page is displayed. It lists a summary of your installation settings and provides other several options.

11. Review your settings and do one of the following:
    - If you do not need to change any settings, Go to **step 13**.
    - To change any settings, click **Previous** to go to the desired page, make the changes, then return to the *Confirm selections* page.

12. To create a desktop icon you can double-click to start the program after installation, leave the appropriate check box selected. Otherwise, clear it.
13. Choose whether you want the application to initialize during installation by doing one the following:
    - Accept the default setting for this option to have the application initialize.
    - Clear the check box for this option if you do not want the application to initialize (this disables the option).

    Note: If you want to enable FIPS mode, disable this option. FIPS mode must be enabled before the application starts for the first time.

14. Click **Next**.

    The installer displays the *Installation progress* page with a status bar and message indicating that it is extracting installation files. In the pane below the status bar, you can view information about Nexpose and related products.

    The installer displays the *Installation progress* page with a status bar and message indicating that it is extracting installation files.

    If you chose to have the application initialize during installation, the *Initialization* page is displayed, showing a status bar and messages about initialization processes.

15. To exit the *Initialization* page and go to the final installation page, click **Exit**. This does *not* stop the initialization process.

    Once the initialization process is complete, the *Installation success* page is displayed.

    At this point, the application files are installed.

    - If you only installed the Scan Engine, complete step **17** and **18** to finish the installation.
    - If you installed the Security Console, complete step **19**, **20**, and **21** to finish the installation.

Scan Engine

17. The *Pair with Console* page is displayed. Specify the IP address or domain name for the Security Console.
18. If necessary for your network configuration, you can change the console TCP port. The default is 40815.
19. Specify the Shared Secret. Global Administrators can generate a Shared Secret in the Administration section of the Security Console. Select **manage** next to *Engines*, click **Generate** next to *Shared Secret*, and copy and paste the Shared Secret into the Installation Wizard.
20. Test the connection. A successful test is required in order to proceed.

    Note: Only the connection between the engine and console is tested. The Shared Secret is not tested.
21. It is possible to skip the Scan Engine pairing if you do not have all the information available, or if the test was unsuccessful and you need to perform further troubleshooting later. To do so, click **Skip Scan Engine Pairing**.
22. Click **Next**.
23. Start the Scan Engine (See *Enabling FIPS mode* on page 1).

Security Console

24. Read the instructions for getting started with the product.
25. Do one of the following:
    - If you disabled the initialization option, you must start the application manually (*Enabling FIPS mode* on page 1).
    - If you left the initialization option enabled, click the URL for logging onto the application.

    A browser displays the logon box page for the Security Console if it has initialized and started.
26. Click **Finish**. See *Getting Started* on page 1 for information on getting started using the application.

Installing in Linux environments

See the instructions for your specific supported Linux distribution.

Uninstalling a previously installed copy

Installing and using multiple copies of the software on the same server is not supported. If you install multiple copies on the same server, the application will not function properly.

Each copy of the software must be installed from scratch. This means that if you already have a copy installed, you must uninstall it before you install the new copy you downloaded.

Use the procedure in the topic *Running the Linux uninstaller* on page 1 to uninstall any previously installed copies.

Do I need to disable SELinux?

SELinux is a security-related feature that must be disabled before you can install the application.

Tip: Later versions of Ubuntu do not include SELinux, or it is automatically set to `permissive`. It is recommended that you check the status before you start the installation.

To disable SELinux, take these steps:

1. Open the SELinux configuration file in your preferred text editor.

   Example: `$ vi /etc/selinux/config`

2. Go the line that begins with `SELINUX=`.

   If the setting is `enforcing`, change it to `disabled`: `SELINUX=disabled`

3. Save and close the file.
4. Restart the server for the change to take effect: `$ shutdown -r now`

At this point you can check the installer file to make sure it is not corrupted or begin the installation. It is recommended that you check the installer file before you begin the installation.

Ensuring that the installer file is not corrupted

This procedure shows you how to check the installer file you downloaded to make sure it is not corrupted. This helps to prevent installation problems.

Make sure that you downloaded the installation file and the md5sum file. See *Installing the application* on page 1 for details.

To check the installer file, take these steps:

1. Go to the directory that contains the installer and the md5sum file. If you have not changed any settings, this will be `Downloads`.
2. Run the md5sum program with the -c option to check the MD5 checksum:

```
$ md5sum -c [installer_file_name].md5sum
```

   - If this command returns an `OK` message, the file is valid.
   - If it returns a "FAILED" message, download the installer and md5sum file again, and repeat this procedure.

Installing in Ubuntu

These steps apply to Ubuntu 8.04. There may be some variation on other versions of Ubuntu.

Make sure that:

- You have downloaded all items necessary for installation. See*Installing the application* on page 1 for details.
- You have root-level access.
- (Recommended) You check the installer file to make sure it was not corrupted during the download. See *Ensuring that the installer file is not corrupted* on page 27.

Manually installing necessary packages in Ubuntu

If sudo is active in your environment, and if your account is listed in the sudoers file, you can use sudo -i to run the commands.

Tip: Rapid7 recommends using apt-get to install packages on Ubuntu.

To install the necessary packages:

1. To verify that you have apt-get, run:

```
$ apt-get -v
```

2. To determine if you have a required package and install it if necessary, run:

```
$ apt-get install [package_name]
```

The following package must be installed:

- screen

Next Steps

Run the Linux installer. See "Running the Linux installer" below.

Installing in Red Hat

You must have root-level access to run the installation. If sudo is active in your environment, and if your account is listed in the sudoers file, you can use sudo -i to run the commands.

These steps apply to Red Hat 5.4. There may be some variation on other versions of Red Hat.

Make sure that:

- You have downloaded all items necessary for installation. See *Installing the application* on page 1 for details.
- You have yum and RPM, which you need to install packages on Red Hat.
- You have a Red Hat Enterprise Linux license.
- (Recommended) You check the installer file to make sure it was not corrupted during the download. See *Ensuring that the installer file is not corrupted* on page 27.

Manually installing necessary packages in Red Hat

You need yum and RPM to install packages on Red Hat.

1. To verify that you have yum and RPM, run: `$ yum --version`
2. To determine if you have a required package and install it as necessary, run:

   ```
   $ yum install [package_name]
   ```

The following package must be installed: `screen`.

Running the Linux installer

This procedure shows you how to install the application in a Linux environment.

If you are using a graphical user interface

If you are using an interface such as KDE or Gnome, omit the `-c flag` in step 3 of the procedure. The installer opens a wizard to guide you through the installation (similar to the Windows

installation wizard (see *Installing in Windows environments* on page 1). The rest of the steps in this procedure reflect installation using the command line interface.

Before you begin

Make sure that:

- Your system meets the minimum installation requirements.
- You have all of the items you need to complete the installation. See *Installing in Windows environments* on page 1.
- You have disabled SELinux (if necessary). See *Do I need to disable SELinux?* on page 27.
- (Recommended) You check the installer file to make sure it was not corrupted during the download. See *Ensuring that the installer file is not corrupted* on page 27.
- You have installed the required packages for your Linux platform.
- You have uninstalled any previously installed copies. See *Running the Linux uninstaller* on page 1.

Warning: The installation will fail if you do not install all necessary packages.

To install the application, take these steps:

1. Go to the directory that contains the installer.
2. Change the permissions for the installation file to make it executable:

   ```
   $ chmod +x [installation_file_name]
   ```

3. Start the installer:

   ```
   $ ./[installation_file_name] -c
   ```

   The installer displays information about the application.

4. Enter **y** and press <**ENTER**>.

   The installer displays system check results. This indicates whether your system meets each of the installation requirements.

5. Review the results and do one of the following:
   - Enter **y** and press <**ENTER**> to continue.

     The end-user license agreement is displayed.

   - Press <**ENTER**> to cancel the installation, modify your system as needed, then go back to the beginning of the installation process.

6. Read the end-user license agreement. Enter **y** and press <**ENTER**> to go to the next screen.
7. At the final screen of the agreement, if you agree with the terms, enter **1** to accept it and continue. If you do not accept it, you cannot continue the installation.

   A prompt is displayed requesting your name and company name (they are required).

8. Enter your name and company name by doing the following:
   - Enter your **first name** and press <**ENTER**>.
   - Enter your **last name** and press <**ENTER**>.
   - Enter your **company name** and press <**ENTER**>.

9. Select the components you want to install by doing one of the following:
   - Select the **Security Console with local Scan Engine** option. If you do not install the Security Console, the application cannot initialize during installation.
   - Select the **Scan Engine only** option. If you install only the Scan Engine, you must install the Security Console before you can use the Scan Engine.
     - Select a communication direction. Which option is preferred depends on your network configuration:
       - Engine to Console: The Scan Engine will actively inform the Security Console that it is available for communication. This configuration allows a console that is behind a firewall and is configured to allow inbound connections to establish a communication channel.
       - Console to Engine: The Scan Engine will listen for communication from the Security Console. This configuration is most effective when the engine and console are on the same area of the network.

10. Select the installation directory by doing one of the following:
    - Press **<ENTER**> to accept the default installation directory (displayed in square brackets).
    - Enter a **different directory path**, then press <**ENTER**>.

Note: If your hard drive is partitioned and you select a location on a different partition, make sure that partition has sufficient space.

A prompt is displayed to select the components you want to install.

Tip: : To view a description of a component, enter an asterisk (*) and the component's number.

11. Select the component (or components) to install by typing the component number and pressing <**ENTER**> for each component. If you do not install the Security Console, the application cannot initialize during installation.

    A prompt is displayed to create a Global Administrator account.

12. To create the Global Administrator account, do the following:
    - Enter a **user name**and press <**ENTER**>.
    - Enter a **password**and press <**ENTER**>.
    - Enter the **password**again for confirmation and press <**ENTER**>.

    Your installation settings are displayed.

13. Review your settings and change them if needed.

    If you are using a graphical user interface an option is displayed for you to create an icon you can use to start the application. The icon in created in the **Applications | Internet** menus enter **y** and press <**ENTER**> to create the icon or enter **n** to decline it.

    An option is displayed to have the application initialize during installation and start automatically after installation.

14. Enter **y** and press <**ENTER**> to accept the option, or enter **n** to decline it. If you want to enable FIPS mode, disable this option. FIPS mode must be enabled before the application starts for the first time.

    The installation progress is displayed. If you chose to install the Security Console and you enabled the initialize and start option, information on the initialization progress is displayed.

    A message that the installation is complete is displayed.

15. Read the additional information.
16. Press <**ENTER**> to exit the installer.

Scan Engine

17. The *Pair with Console* page is displayed. Specify the IP address or domain name for the Security Console.
18. If necessary for your network configuration, you can change the console TCP port. The default is 40815.
19. Specify the Shared Secret. Global Administrators can generate a Shared Secret in the Administration section of the Security Console. Select **manage** next to *Engines*, click **Generate** next to *Shared Secret*, and copy and paste the Shared Secret into the Installation Wizard.
20. Test the connection. A successful test is required in order to proceed.

    Note: Only the connection between the engine and console is tested. The Shared Secret is not tested.
21. It is possible to skip the Scan Engine pairing if you do not have all the information available, or if the test was unsuccessful and you need to perform further troubleshooting later. To do so, click **Skip Scan Engine Pairing**.
22. Click **Next**.
23. Start the Scan Engine (See *Enabling FIPS mode* on page 1).

Security Console

24. Read the instructions for getting started with the product.
25. Do one of the following:
    - If you disabled the initialization option, you must start the application manually (*Enabling FIPS mode* on page 1).
    - If you left the initialization option enabled, click the URL for logging onto the application.

    A browser displays the logon box page for the Security Console if it has initialized and started.
26. Click **Finish**. See *Getting Started* on page 1 for information on getting started using the application.

Running the application

Manually starting or stopping in Windows

NexposeSymantec CCS Vulnerability Manager 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 NexposeSymantec CCS Vulnerability Managerin 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

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 *Managing versions, updates and licenses*.

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.If you do not have a product key, read the instructions to request one. 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.

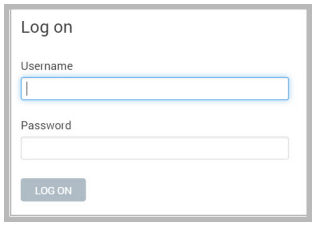
   Your browser displays the *Logon* window.

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*Changing the Security Console Web server default settings*.

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 *Running in maintenance mode*.

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

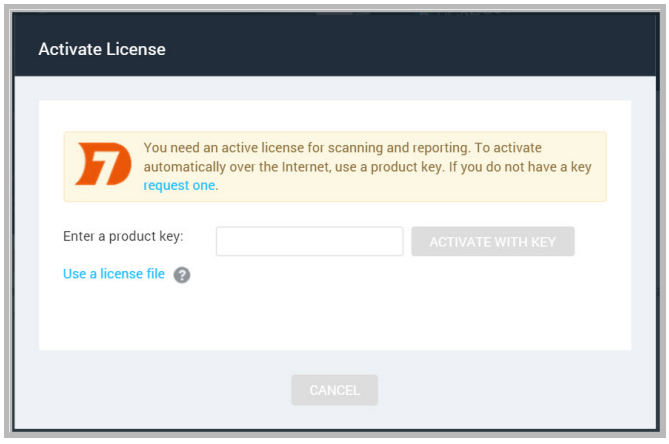
   User names and passwords are case-sensitive and non-recoverable.



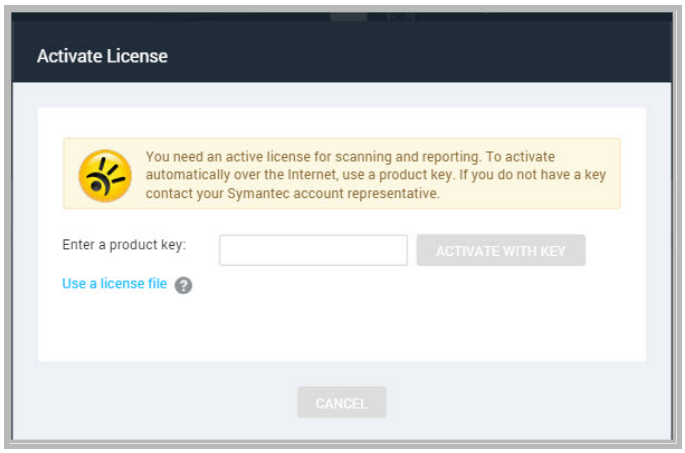
Logon window

3. Click the **Logon** icon.

   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



Activate License window

Note: If the Security Console displays a warning that authentication services are unavailable, and your network uses an external authentication source, have your Global Administrator verify that the source is online and correctly configured. See *Using external sources for user authentication* in the administrator's guide *Using external sources for user authentication*.

4. Click **Activate** to complete this step.
5. Click the **Home**icon to view the Security Console *Home* page.
6. Click the **Help** icon 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 under the **Help** icon dropdown. The **Help** icon can be found near the top right corner of every page of the console interface.

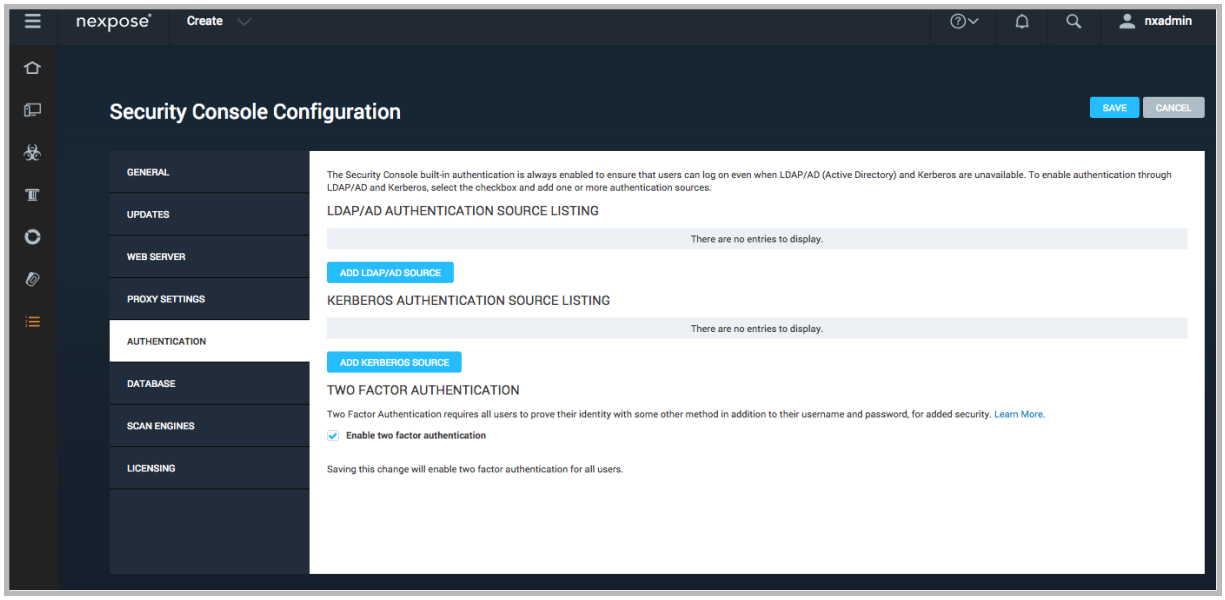
Enabling Two Factor Authentication

For organizations that want additional security upon login, the product supports Two Factor Authentication. Two Factor Authentication requires the use of a time-based one-time password application such as Google Authenticator.

Two Factor Authentication can only be enabled by a Global Administrator on the *Security Console*.

To enable Two Factor Authentication:

1. As a Global Administrator, go to the **Administration** tab.
2. Click the **Administer** link in the *Global and Console Settings* section.
3. Select **Enable two factor authentication**.

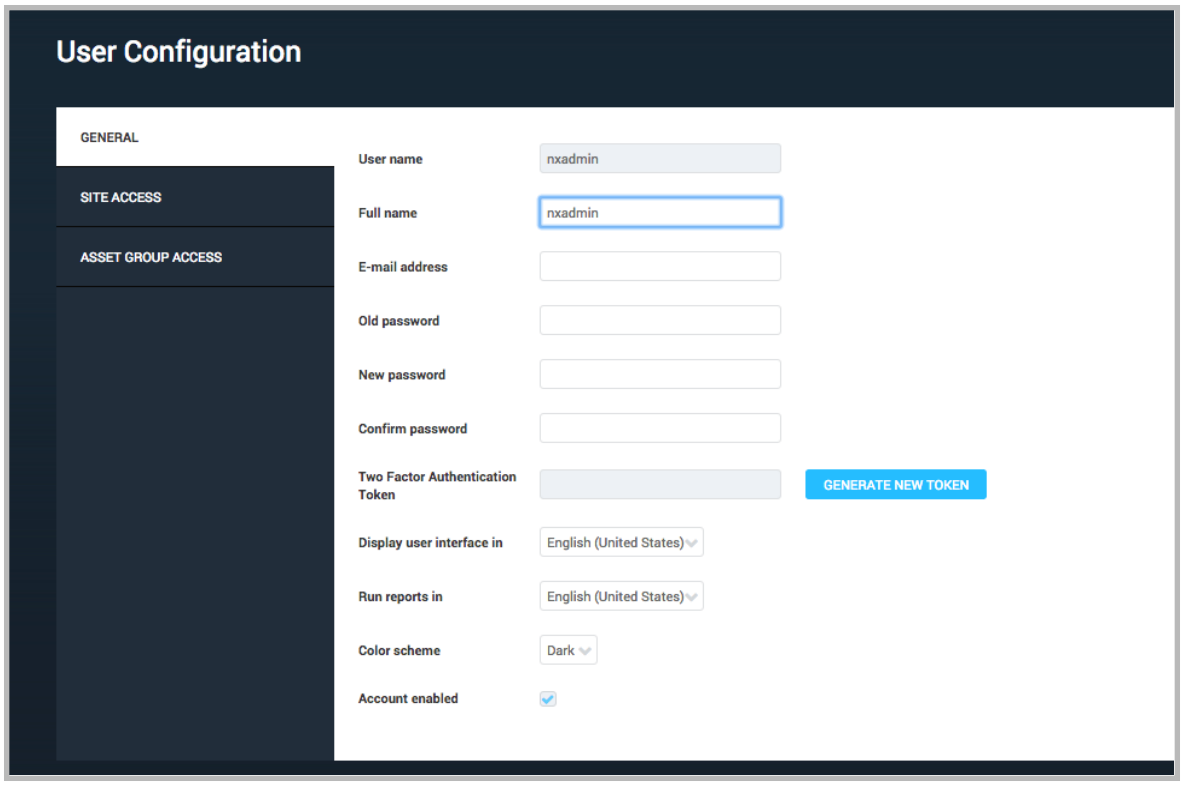


The next step is to generate a token for each user. The users can generate their own tokens, or you can generate tokens for them that they then change. In either case, you should communicate with them about the upcoming changes.

Method 1: Tokens created by users

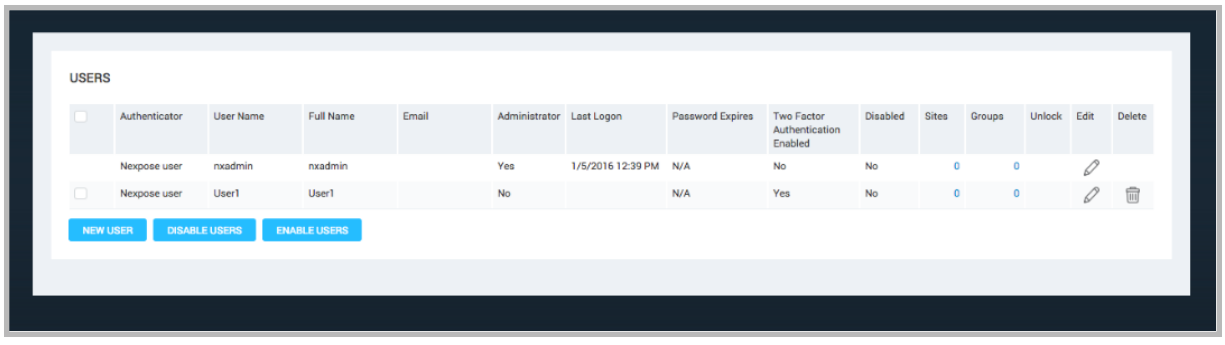
Once Two Factor Authentication is enabled, when a user logs on, they will see a field where they can enter an access code. For the first time, they should log in without specifying an access code.

Once the user logs in, they can generate a token in the *User Preferences* page.



The user should then open their time-based one-time password application such as Google Authenticator. They should enter the token as the key in the password application. The password application will then generate a new code that should be used as the user's access code when logging in.

A Global Administrator can check whether users have completed the Two Factor Authentication on the *Manage Users* page. The *Manage Users* page can be reached by going to the *Administration* tab and clicking the **Manage** link in the *Users* section. A new field, **Two Factor Authentication Enabled**, will appear in the table and let the administrator know which users have enabled this feature.



If the user doesn't create a token, they will still be able to log in without an access code. In this case, you may need to take steps to enforce enablement.

Method 2: Generating tokens for users

You can enforce that all users log in with a token by disabling the accounts of any users who have not completed the process, or by creating tokens for them and emailing them their tokens.

To disable users:

1. Go to the *Manage users* page by going to the **Administration** tab and clicking the **Manage** link in the Users section.
2. Select the checkbox next to each user for whom the Two Factor Authentication Enabled column shows No.
3. Select **Disable users**.

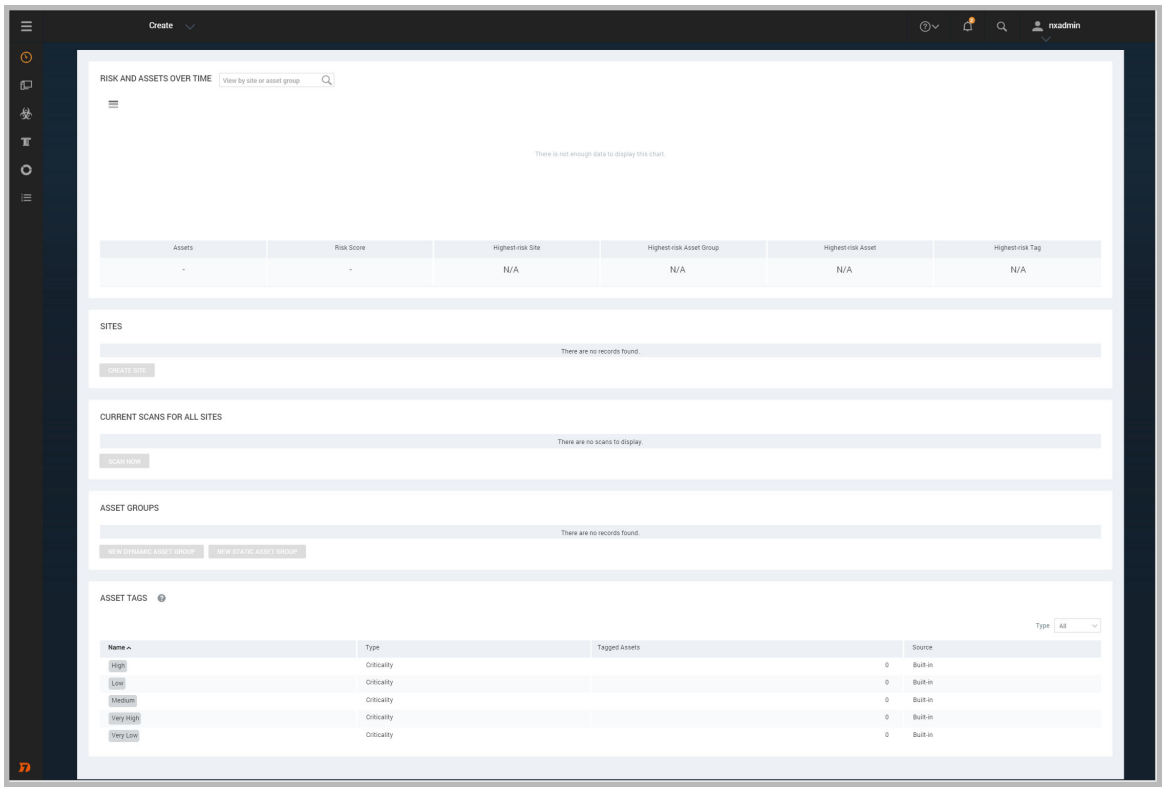
To generate a token for a user:

1. Go to the *Manage users* page by going to the **Administration** tab and clicking the **Manage** link in the *Users* section.
2. Select **Edit** for that user.
3. Generate a token for that user.
4. Provide the user with the token.
5. Once the user logs in with their access code, they can change their token if they would like in the *User preferences* page.

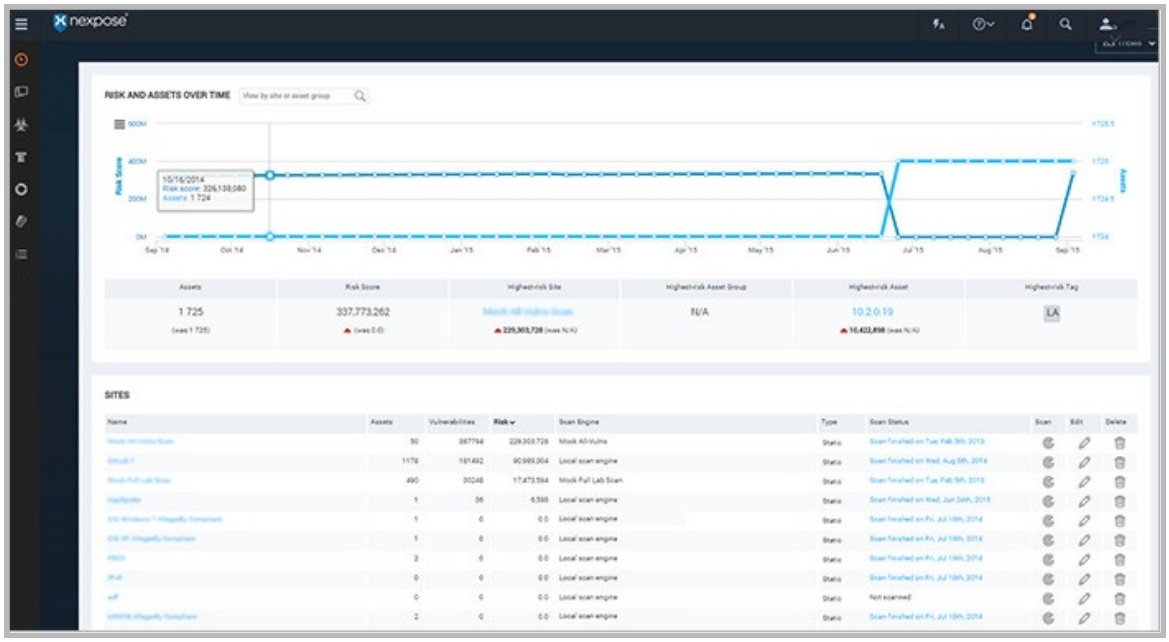
Navigating the Security Console Web interface

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.

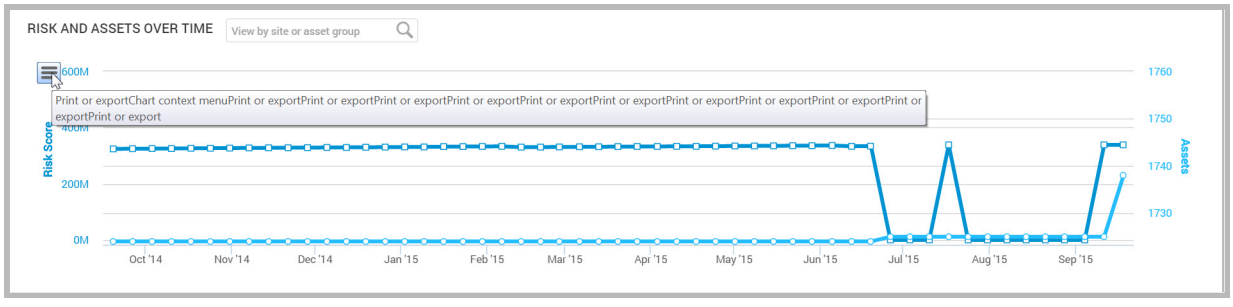
The *Home* page also displays a chart that shows trends of risk score over time. As you add assets to your environment your level of risk can increase because the more assets you have, the more potential there is for vulnerabilities.

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

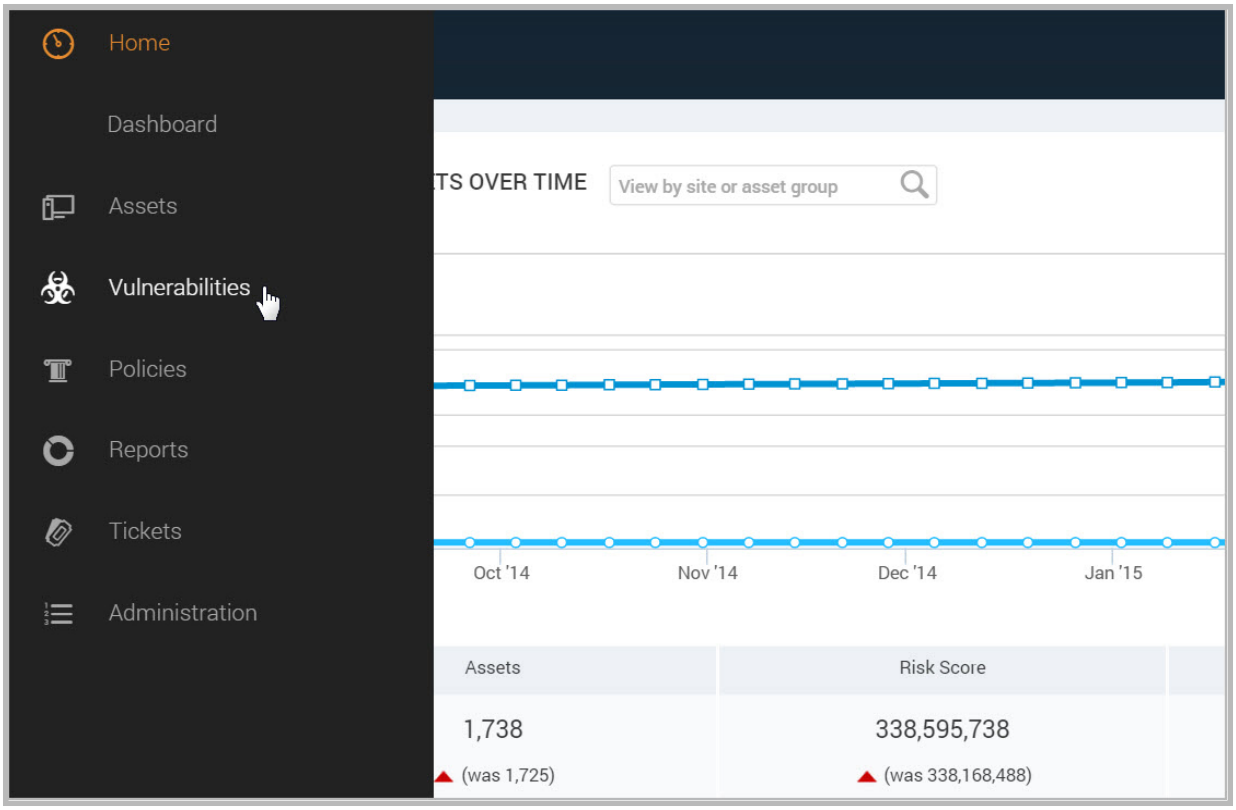
On the *Site Listing* pane, you can click controls to view and edit site information, run scans, and start to create a new site, depending on your role and permissions.

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 menu appears on the left side of the *Home* page, as well as every page of the Security Console. Mouse over the icons to see their labels, and use these icons to navigate to the main pages for each area.



Icon menu

The *Home* page links to the initial page you land on in the Security Console.

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 icon.

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* in the user's guide *Creating a basic report* on page 1 *Creating a basic report*.

Using icons and other controls

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

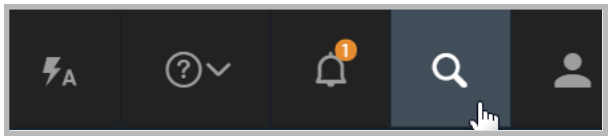
Control	Description	Control	Description
▼	Minimize any pane so that only its title bar appears.		Add items to your dashboard.
▲	Expand a minimized pane.		Copy a built-in report template to create a customized version.
x	Close a pane.		Edit properties for a site, report, or a user account.
ITEMS	Click to display a list of closed panes and open any of the listed panes.		View a preview of a report template.
	Export data to a comma-separated value (CSV) file.		Delete a site, report, or user account.
	Start a manual scan.		Exclude a vulnerability from a report.
	Pause a scan.	?	View Help. View the Support page to search FAQ pages and contact Technical Support. View the *News* page which lists all updates.
	Resume a scan.	Product logo	Click the product logo in the upper-left area to return to the *Home* page.
	Stop 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.
	Initiate a filtered search for assets to create a dynamic asset group.	**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.
Create	Expand a drop-down list of options to create sites, asset groups, tags, or reports.		

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

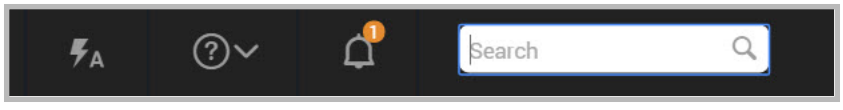
Access the **Search** box on any a page of the Security Console interface by clicking the magnifying glass icon near the top right of the page.



Clicking the Search icon

Enter your search criteria into the **Search** box and then click the magnifying glass icon again. 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.

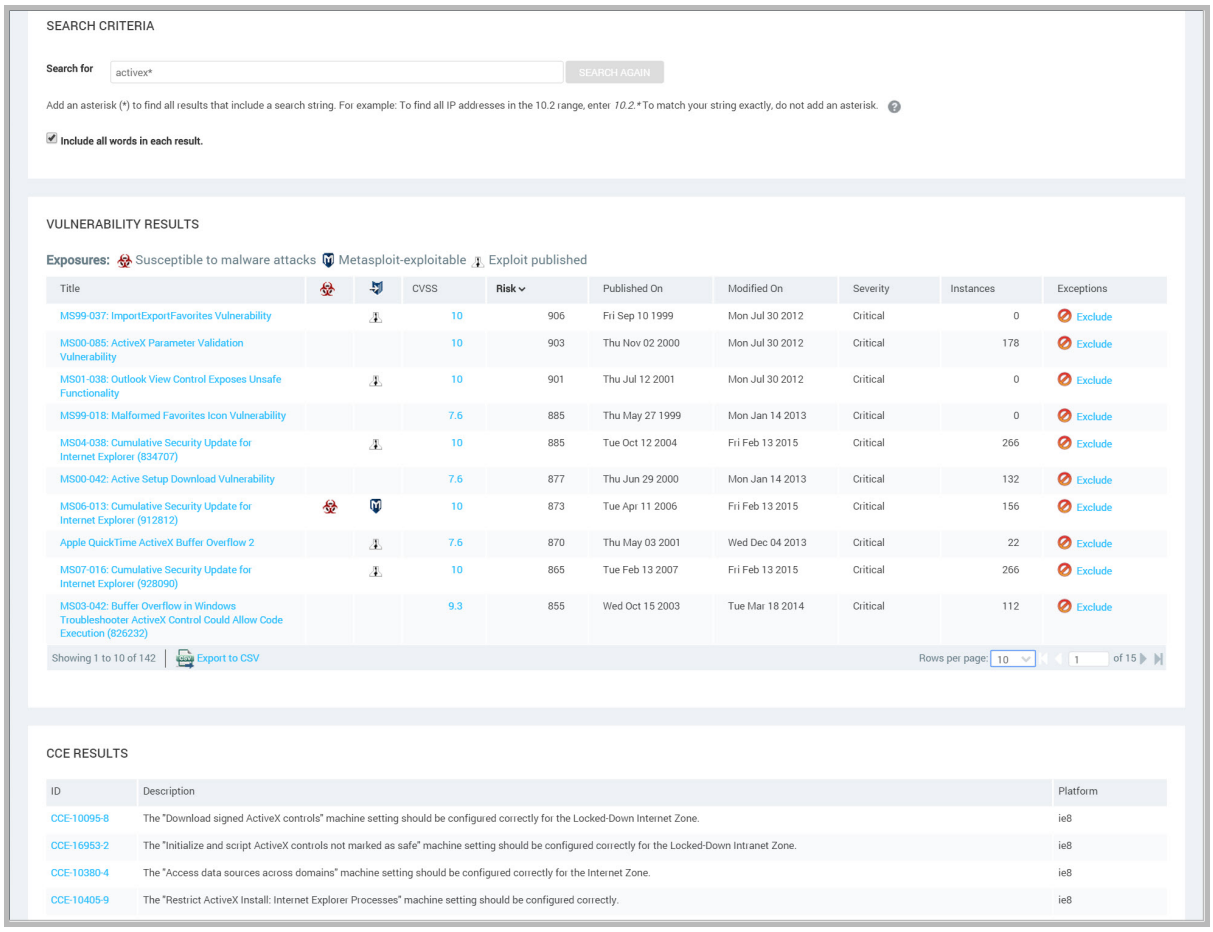
For example, if you want to search for discovered instances of the vulnerabilities that affect assets running ActiveX, enter ActiveX or activex in the **Search** text box. The search is not case-sensitive.



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

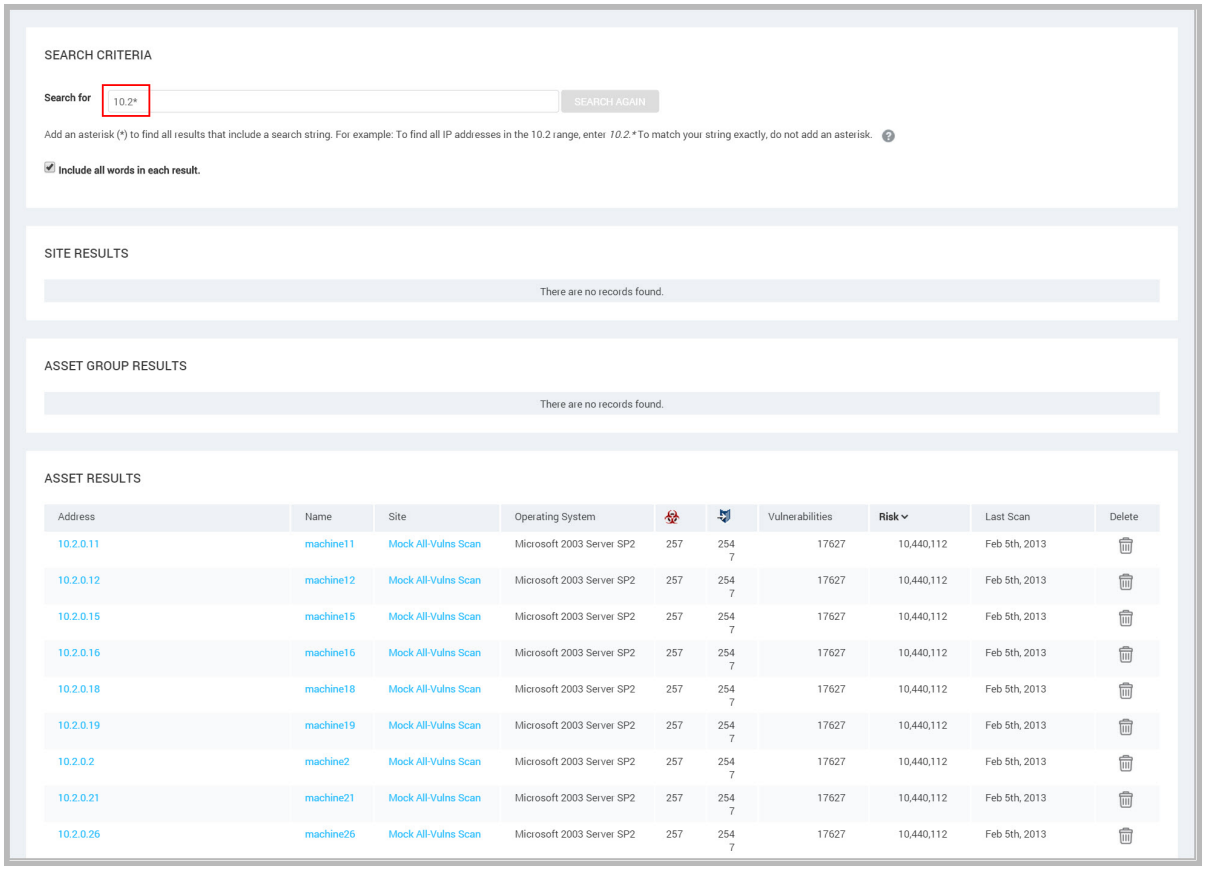
In the *Search Criteria* pane, you can refine and repeat the search. You can change the search phrase and choose whether to allow partial word matches and to specify that all words in the phrase appear in each result. After refining the criteria, click the **Search Again** button.

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.



Searching with a partial string

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:

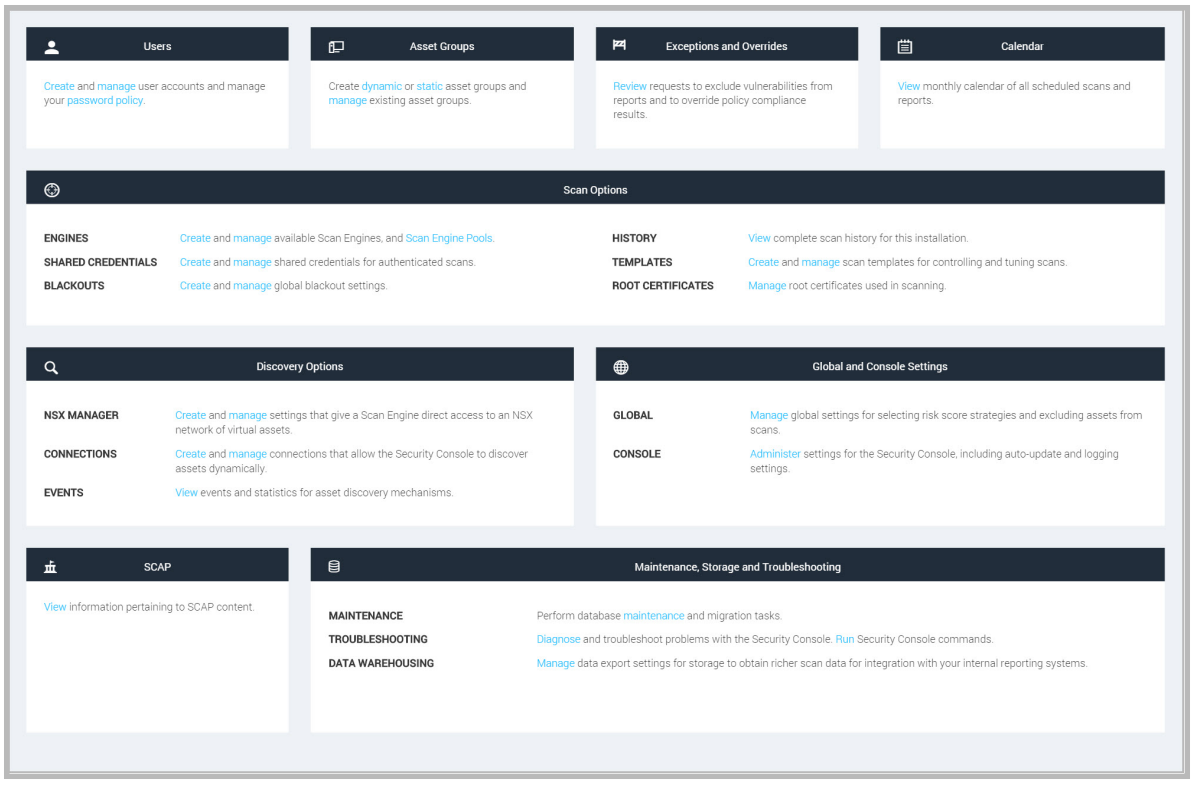
a	about	above	after	again	against	all	am	an	and
any	are	as	at	be	because	been	being	below	before
between	both	but	by	can	did	do	doing	don	does
down	during	each	few	for	from	further	had	has	have
having	he	her	here	hers	herself	him	himself	his	how
i	if	in	into	it	is	its	itself	just	me
more	most	my	myself	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** icon. 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

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

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 *Changing the Security Console Web server default settings*.

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.

Activating the license

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 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.

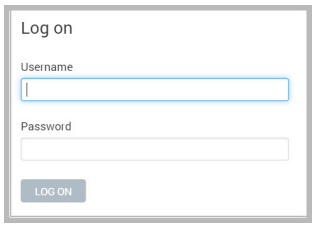
   Your browser displays the *Logon* window.

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.

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.

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

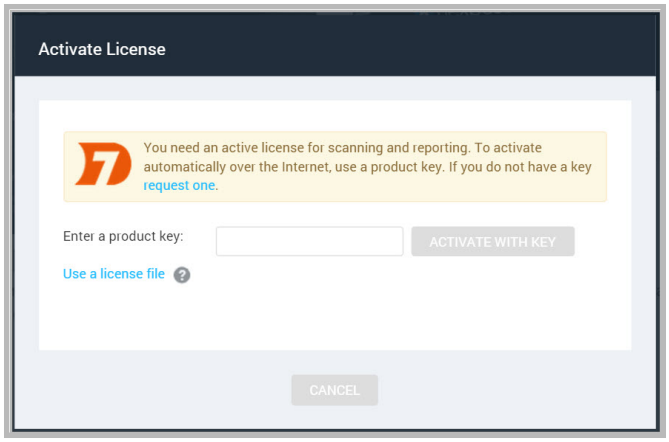
   User names and passwords are case-sensitive and non-recoverable.



Logon window

3. Click the **Logon** icon.

   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

Note: If the Security Console displays a warning that authentication services are unavailable, and your network uses an external authentication source, have your Global Administrator verify that the source is online and correctly configured.

4. Click **Activate** to complete this step.
5. Click the **Home**icon to view the Security Console *Home* page.
6. Click the **Help** icon 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 under the **Help**

icon dropdown. The **Help** icon can be found near the top right corner of every page of the console interface.

Setting up the proxy in the console

If the Security Console does not have direct Internet access, you can use a proxy server for downloading updates. In most cases, Technical Support will advise if you need to change this setting. This topic covers configuring proxy settings for updates.

Note: For information on configuring updates for an Appliance, see the *Appliance Guide* which you can download from the *Support* page of *Help*.

To configure proxy settings for updates:

1. Click the **Administration** tab.

   The *Administration* page appears.

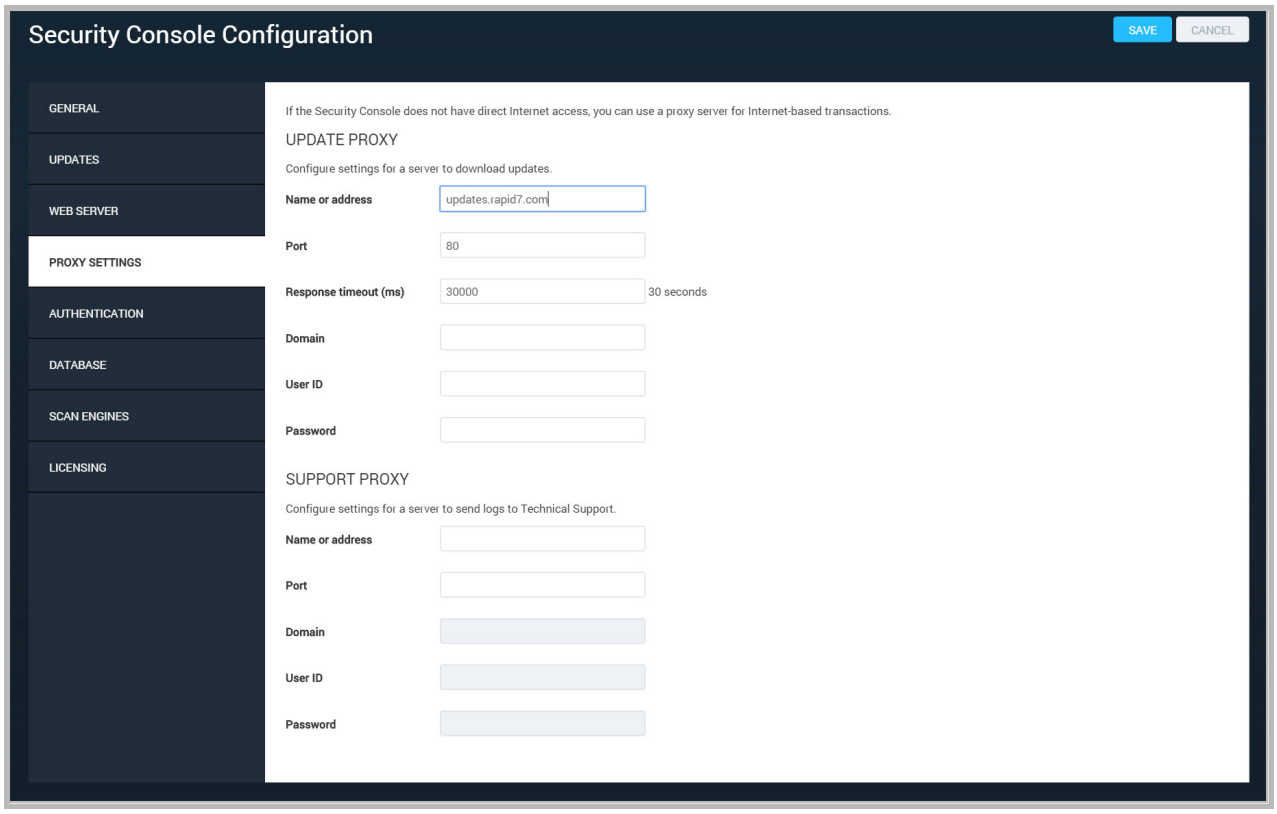
2. On the *Administration* page, click the **Manage** link for *Security Console*.

   The *Security Console Configuration* panel appears.

3. Go to the *Proxy Settings* page.

4. Enter the information for the proxy server in the appropriate fields:
   - The **Name or address** field is set to *updates.rapid.7.com* by default, which means that the Security Console is configured to contact the update server directly. If you want to use a proxy, enter the name or IP address of the proxy server.
   - The **Port** field is set to *80* by default because the Security Console contacts the update server on that port. If you want to use a proxy, and if it uses a different port number for communication with the Security Console, enter that port number.
   - The **Response timeout** field sets the interval that the Security Console will wait to receive a requested package before initiating a timeout of the transfer. The default setting is 30,000 ms, or 30 seconds. The minimum setting is 1,000 ms, and the maximum is 2,147,483,647 ms. A proxy server may not relay an entire requested package to the Security Console until it downloads and analyzes the package in its entirety. Larger packages require more time. To determine how long to allow for a response interval, see the following topic: *Determining a response timeout interval for the proxy*.
   - The Security Console uses the information in the **Domain**, **User name**, and **Password** fields to be authenticated on a proxy server. If you want to use a proxy server, enter required values for those fields.

   After you enter the information, click **Save**.



Security Console Configuration panel - Proxy Settings page

Determining a response timeout interval for the proxy

To determine a timeout interval for the proxy server, find out how much time the Security Console requires to download a certain number of megabytes. You can, for example, locate the downloaded .JAR archive for a recent update and learn from the log file how long it took for the Security Console to download a file of that size.

Open the nsc.log file, located in the [installation_directory]/nsc directory. Look for a sequence of lines that reference the download of an update, such as the following:

```
2013-06-05T00:04:10 [INFO] [Thread: Security Console] Downloading update ID
1602503.

2013-06-05T00:04:12 [INFO] [Thread: Security Console] Response via 1.1
proxy.example.com.

2013-06-05T00:05:05 [INFO] [Thread: Security Console] Response via 1.1
proxy.example.com.
```

```
2013-06-05T00:05:07 [INFO] [Thread: Security Console] Acknowledging receipt
of update ID 1602503.
```

Note the time elapsed between the first entry (`Downloading update ID`...) and the last entry (`Acknowledging receipt of update`...).

Then go to the directory on the Security Console host where the .JAR archives for updates are stored: [installation_directory]/updates/packages. Locate the file with the update ID referenced in the log entries and note its size. Using the time required for the download and the size of the file, you can estimate the timeout interval required for downloading future updates. It is helpful to use a larger update file for the estimate.

Tip: In most cases, a timeout interval of 5 minutes (300,000 ms) is generally sufficient for most update file sizes.

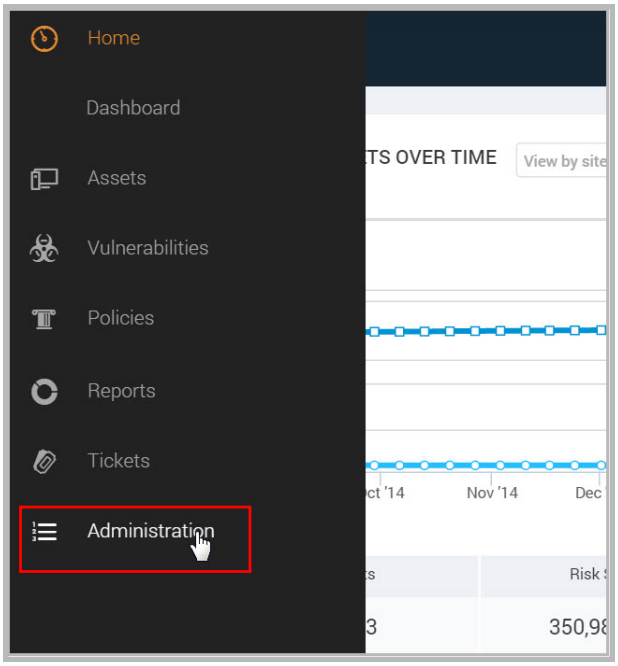
Updating the console

Viewing version and update information

It is important to keep track of updates and to know which version of the application you are running. For example, a new vulnerability check may require the latest product update in order to work. If you are not seeing expected results for that check, you may want to verify that the application has installed the latest product update. Also, if you contact Technical Support with an issue, the support engineer may ask you which version and update of the application you are running.

1. Click the **Administration** tab of the Security Console interface.

   The Security Console displays the *Administration* page.



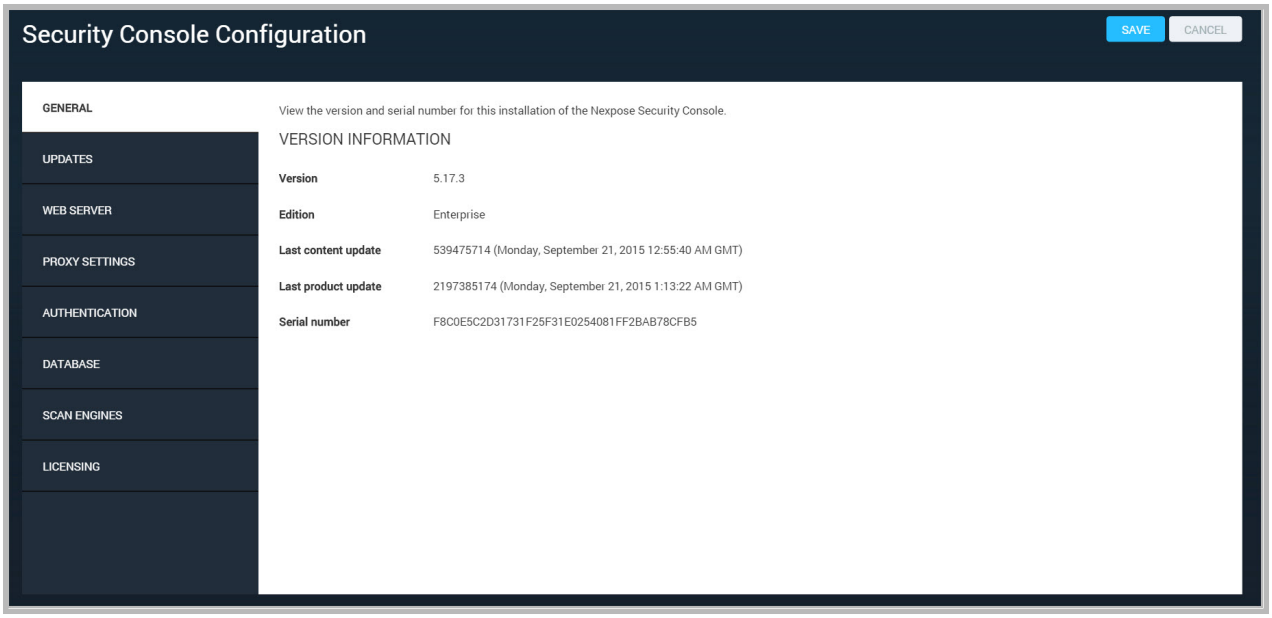
Administration tab

2. Click **Manage** settings for the Security Console, including auto-update and logging settings.

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

   On this page you can view the current version of the application. You can also view the dates and update IDs for the current product and content updates. Release announcements

always include update IDs, so you can match the IDs displayed on the Security Console page with those in the announcement to verify that you are running the latest updates.



The General page of the Security Console Configuration panel

Managing updates with an Internet connection

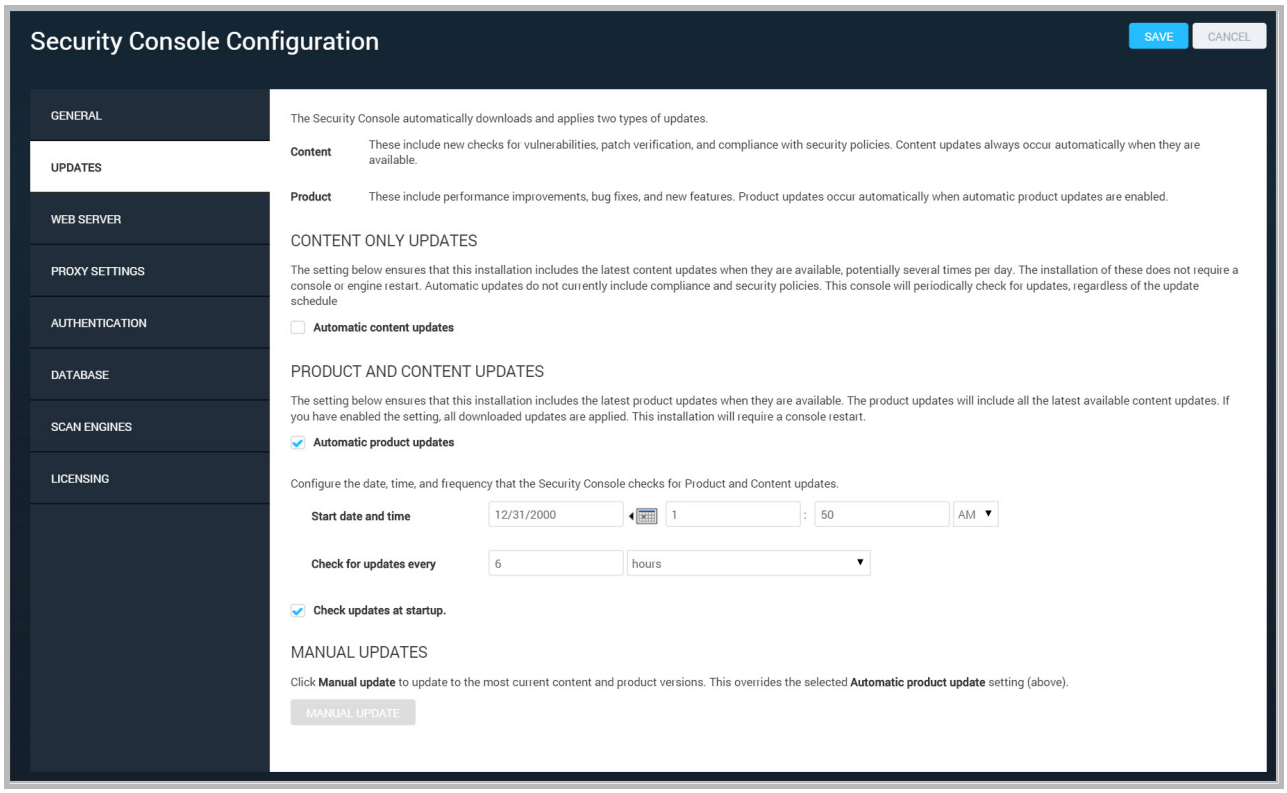
By default, the Security Console automatically downloads and applies two types of updates.

Content updates

Content updates include new checks for vulnerabilities, patch verification, and security policy compliance. Content updates always occur automatically when they are available.

Product updates

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.



The Security Console Updates page

Disabling automatic product updates

You can disable automatic product updates and initiate one-time product updates on an as-needed basis. This gives your organization the time and flexibility to train staff or otherwise prepare for updates that might cause changes in workflow. For example, a new feature may streamline a particular workflow by eliminating certain steps.

Note: Some new vulnerability and policy checks, which are included in content updates, require concurrent product updates in order to work properly.

To disable automatic product updates:

1. Click the **Administration** tab.
2. Click **manage** next to *Security Console*.

   The *Security Console Configuration* panel appears.
3. Select **Updates** from the menu on the left-hand side.
4. Clear the checkbox labeled **Enable automatic product updates**.

   A warning dialog box appears about the risks of disabling automatic product updates.

Click **Disable automatic product updates** to confirm that you want to turn off this feature.

Or click **Cancel** to leave automatic product updates enabled.

5. Click **Save**.

   Whenever you change this setting and click **Save**, the application downloads any available product updates. If you have disabled the setting, it does not apply any downloaded product updates.

Enabling automatic product updates

Note: Your PostgreSQL database must be version 9. Otherwise, the application will not apply product updates. If you are using an earlier version of PostgreSQL, see *Migrating the database* on page 1 *Migrating the database*.

Enabling automatic product updates ensures that you are always running the most current version of the application.

To enable automatic product updates after they have been previously disabled:

1. Go to the **Administration** tab.
2. Click **manage** next to *Security Console*.

   The *Security Console Configuration* panel appears.

3. Select **Updates** from the left navigation pane.
4. Select the **Enable automatic product updates** check box.
5. Click **Save**.

   Whenever you change this setting and click **Save**, the application downloads any available product updates. If you have enabled the setting, it also applies any downloaded product updates and restarts.

Manual product updates

When automatic product updates have been disabled, you can manually download product updates.

Note: By using this one-time update feature, you are not enabling future automatic product updates if they are not currently enabled.

To manually download a new product update:

1. Go to the *Administration*page.
2. Click **manage** next to *Security Console*.

   The *Security Console Configuration* screen appears.
3. Select **Updates**from the left navigation pane.

   Current available updates appear on the *Updates*page.
4. Click **Manual Update** to install them.

   A warning dialog box appears, indicating that the time to update will vary depending on the number and complexity of updates, and that future automatic product updates will remain disabled.
5. Click **Complete this one-time update** to perform the update.
6. (Optional) Click **Cancel** if you do not want to perform the update.

Scheduling automatic updates

By default the Security Console queries the update server for updates every six hours. If an update is available, the console downloads and applies the update and then restarts. You can schedule updates to recur at specfic times that are convenient for your business operations. For example, you may want updates to only occur during non-business hours or at times when they won't coincide with and disrupt scans.

Note: Content updates are always applied according to the schedule, and product updates are applied according to the schedule only if they are enabled.

To schedule updates:

1. Go to the *Administration*page.
2. Click **manage** next to *Security Console*.

   The *Security Console Configuration* screen appears.
3. Select **Updates**from the left navigation pane.

   The *Updates*page appears.

4. If you want to prevent the Security Console from applying any available updates whenever it starts up, clear the appropriate checkbox. Disabling this default setting allows you to resume normal operations after an unscheduled restart instead of delaying these operations until any updates are applied.
5. Select a date and time to start your update schedule.
6. Select how frequently you want the Security Console to apply any available updates once the schedule is in effect.
7. Click **Save**.

Tuning your Nexpose Database

The following table lists PostgreSQL configuration parameters, their descriptions, default settings, and their recommended “tuned” settings. The table continues on the following page.

The file to be edited is located in *[installation_directory]/nsc/nxpgsql/nxpdata/postgresql.conf*.

The *Recommended midrange settings* are intended to work with a Nexpose 64-bit Appliance running on 8 GB of RAM, or equivalent hardware. 64-bit hardware running on 8GB of RAM.

The *Recommended enterprise business settings* are intended to work in a higher-scan-capacity environment in which the application is installed on high-end hardware with 72 GB of RAM. See *Selecting a Security Console host for an enterprise deployment* on page 1*Selecting a Security Console host for an enterprise deployment*

Parameter	Description	Default value	Recommended midrange settings	Recommended enterprise settings
shared_ buffers	This is the amount of memory that is dedicated to PostgreSQL for caching data in RAM. PostgreSQL sets the default when initializing the database based on the hardware capacity available, which may not be optimal for the application. Enterprise configurations will benefit from a much larger setting for shared_buffers. Midrange configurations should retain the default that PostgreSQL allocates on first installation. **Note:** Increasing the default value may prevent the database from starting due to kernel limitations. To ensure that PostgreSQL starts, see *Increasing the shmmax kernel parameter* on page 71*Increasing the shmmax kernel parameter*	This value is set on PostgreSQL startup based on operating system settings.	24 MB	1950 MB
max_ connections	This is the maximum number of concurrent connections to the database server. Increase this value if you anticipate a significant rise in the number of users and concurrent scans. Note that increasing this value requires approximately 400 bytes of shared memory per connection slot.	100	200	300
work_mem	This is the amount of memory that internal sort operations and hash tables use before switching to temporary disk files.	1 MB	32 MB	32 MB

Parameter	Description	Default value	Recommended midrange settings	Recommended enterprise settings
checkpoint_ segments	PostgreSQL writes new transactions to the database in files known as write ahead log (WAL) segments, which are 16 MB in size. These entries trigger checkpoints, or points in the transaction log sequence at which all data files have been updated to reflect the content of the log. The checkpoint_ segments setting is the maximum distance between automatic checkpoints. At the default setting of 3, checkpoints can be can be resource intensive, producing 48 MB (16 MB multiplied by 3) and potentially causing performance bottlenecks. Increasing the setting value can mitigate this problem.	3	3	32
effective_ cache_size	This setting reflects assumptions about the effective portion of disk cache that is available for a single query. It is factored into estimates of the cost of using an index. A higher value makes an index scan more likely. A lower value makes sequential scans more likely.	128 MB	4 GB (For configurations with more than 16 GB of RAM, use half of the available RAM as the setting.)	32 GB

Parameter	Description	Default value	Recommended midrange settings	Recommended enterprise settings
logging: log_ min_error_ statement	This setting controls whether or not the SQL statement that causes an error condition will be recorded in the server log. The current SQL statement is included in the log entry for any message of the specified severity or higher. Each value corresponds to one of the following severity levels in ascending order: DEBUG5, DEBUG4, DEBUG3, DEBUG2, DEBUG1, INFO, NOTICE, WARNING, ERROR, LOG, FATAL, and PANIC. The default value is ERROR, which means statements causing errors or more severe events will be logged. Increasing the log level can slow the performance of the application since it requires more data to be logged.	ERROR	ERROR	ERROR
logging: log_ min_ duration_ statement	This setting causes the duration of each completed statement to be logged if the statement ran for at least the specified number of milliseconds. For example: A value of 5000 will cause all queries with an execution time longer than 5000 ms to be logged. The default value of -1 means logging is disabled. To enable logging, change the value to 0. This will increase page response time by approximately 5 percent, so it is recommended that you enable logging only if it is required. For example, if you find a particular page is taking a long time to load, you may need to investigate which queries may be taking a long time to complete.	-1	-1 (Set recommended value to 0 only if required for debugging)	-1 (Set recommended value to 0 only if required for debugging)

Parameter	Description	Default value	Recommended midrange settings	Recommended enterprise settings
wal_buffers	This is the amount of memory used in shared memory for write ahead log (WAL) data. This setting does not affect select/update-only performance in any way. So, for an application in which the select/update ratio is very high, wal_buffers is almost an irrelevant optimization.	64 KB	64 KB	8 MB
maintenance_work_mem	This setting specifies the maximum amount of memory to be used by maintenance operations, such as VACUUM, CREATE INDEX, and ALTER TABLE ADD FOREIGN KEY.	16 MB	16 MB	512 MB

Increasing the shmmax kernel parameter

If you increase the shared_buffers setting as part of tuning PostgreSQL, check the shmmax kernel parameter to make sure that the existing setting for a shared memory segment is greater than the PostgreSQL setting. Increase the parameter if it is less than the `PostgreSQL setting`. This ensures that the database will start.

1. Determine the maximum size of a shared memory segment:

```
# cat /proc/sys/kernel/shmmax
```

2. Change the default shared memory limit in the proc file system.

```
# echo [new_kernel_size_in_bytes] > /proc/sys/kernel/shmmax
```

It is unnecessary to restart the system.

Alternatively, you can use sysctl(8) to configure the shmax parameters at runtime:

```
# sysctl -w kernel.shmmax=[new_kernel_size_in_bytes]
```

Note: If you do not make this change permanent, the setting will not persist after a system restart.

To make the change permanent, add a line to the /etc/sysctl.conf utilities file, which the host system uses during the startup process. Actual command settings may vary from the following example:

```
# echo "kernel.shmmax=[new_kernel_size_in_bytes]" >> /etc/sysctl.conf
```

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 73*Adding an engine* on page 73
- *Pairing the Scan Engine with the Security Console* on page 75*Pairing the Scan Engine with the Security Console* on page 75
- *Configuring distributed Scan Engines* on page 73 *Configuring distributed Scan Engines*

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*Support: Technical Support and Customer CareSupport, Documents, and FAQs*.
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.

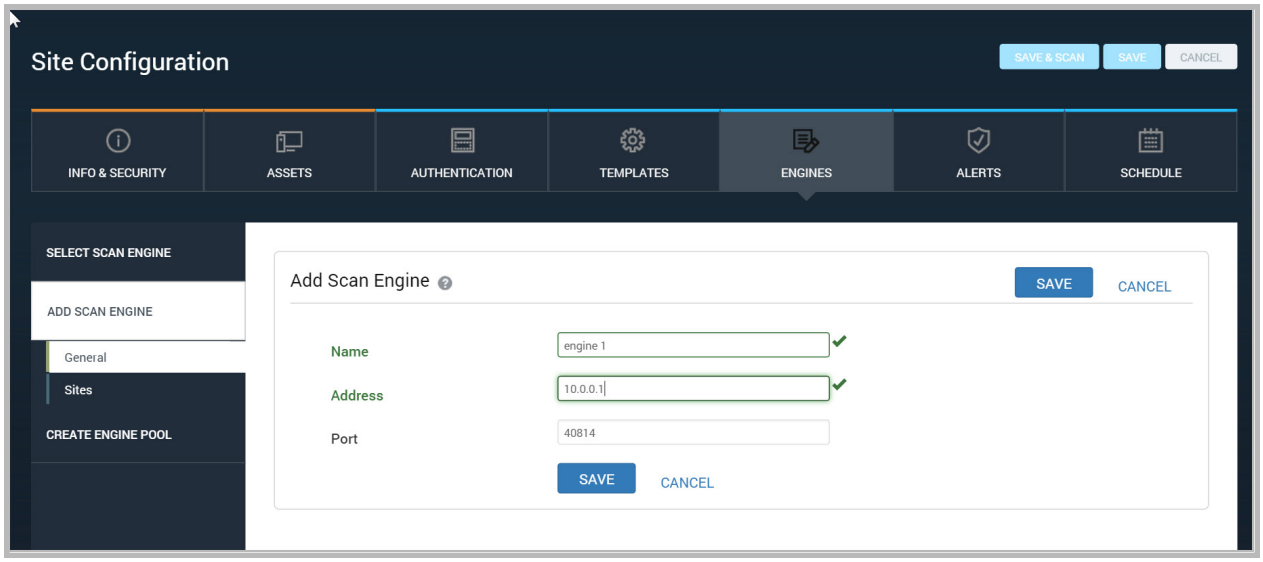
Adding an engine

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** icon.
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**.

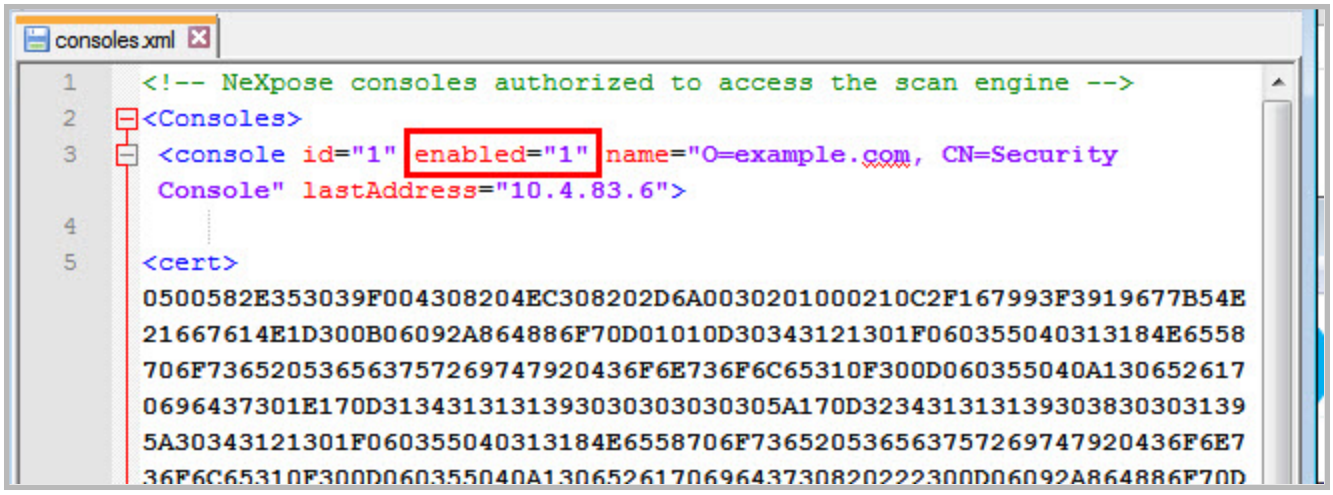
After you add the engine, the Security Console creates the *consoles.xml* file. You will need to edit this file in the pairing process.

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:

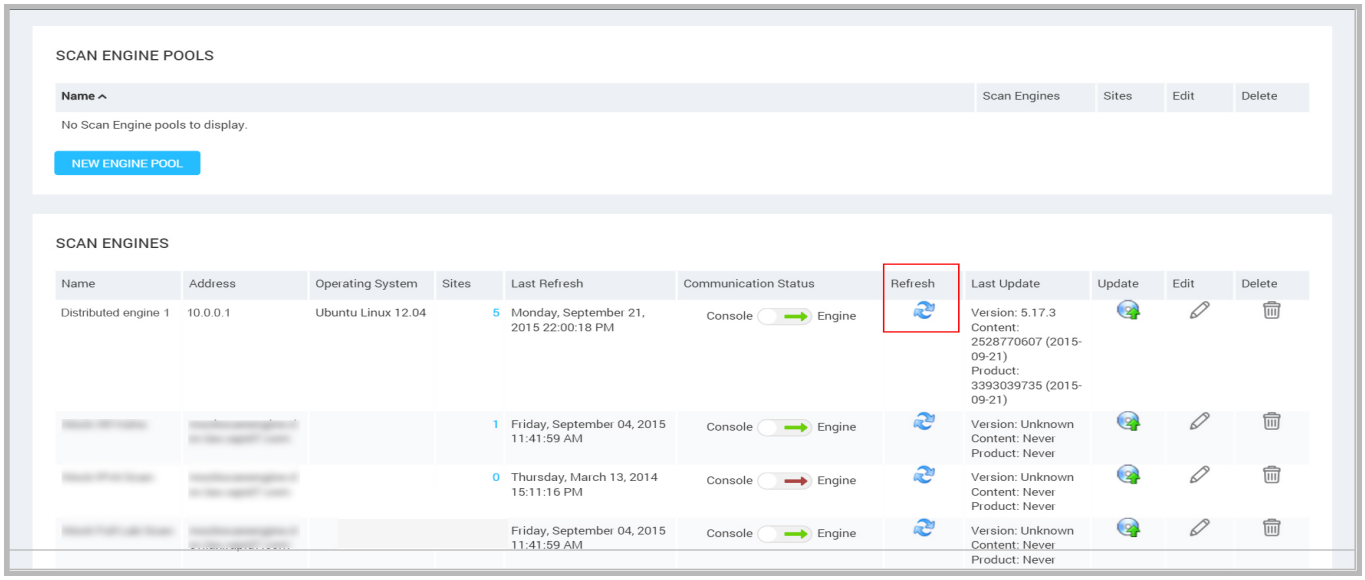
1. Click the **Administration** icon.
2. On the *Administration* page, click **Manage** to the right of *Scan Engines*.
3. On the *Scan Engines* page, locate the Scan Engine that you added.

   Note that the status for the engine is *Unknown*.

4. Click the **Refresh** icon for the engine.

   The Status column indicates with a color-coded arrow whether the Security Console or a Scan Engine is initiating communication in each pairing. The color of the arrow indicates the status of the communication. A green arrow indicates *Active* status, which means you can now assign a site to this Scan Engine and run a scan with it.

   For more information on communication status, see *Managing the Security Console* on page 1*Changing Scan Engine communication direction in the Console*.



*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 *Using the command console*.

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 *Changing default Scan Engine settings*.

Pairing hosted scan engines

You can create a pairing from a Scan Engine to a Security Console by creating a trusted connection between with them. A shared secret is a piece of data used so the console will recognize and trust the incoming communication from the engine.

Note: Each generated shared secret can be used by multiple engines. A shared secret is valid for 60 minutes from when it was generated. After 60 minutes, you will need to generate a new Shared Secret if you want to create additional trusted pairings.

To create a trusted pairing:

1. Ensure that no network-based or host-based firewall is blocking access to port 40815 on your Nexpose Security Console. If you want to use a port other than 40815, change this line in your console's nsc.xml file (*[installation directory]*\nsc\conf\nsc.xml) to the port you want to use:

   ```
   <EngineListener port="40815"/>
   ```

   Restart your Security Console.

2. Generate a shared secret on the Security Console. To do so, go to the *Administration* page and click **manage** next to *Engines*. Under *Generate Scan Engine Shared Secret*, click **Generate**. Copy the Shared Secret to a text file.
3. Log on to the host where the Scan Engine is running and access the command line interface. For Windows hosts, you can use Remote Desktop Protocol. For Unix and related hosts, you can use SSH. For Linux, access the engine's console by using the command:

   ```
   screen -r
   ```
4. Add the Security Console on your engine using the IP address or the hostname of the machine hosting the Security Console. Example:

   ```
   add console 10.1.1.4
   ```
5. Find the ID of the Security Console by typing

   ```
   show consoles
   ```
6. Connect to the Security Console using the ID you just found. Example:

   ```
   connect to console 2
   ```
7. Verify that the connection was successful. Type:

   ```
   show consoles
   ```
   For the console ID you just connected, the value of *connectTo* should be 1.

8. Add the shared secret to that Security Console on the engine. Example:

   ```
   add shared secret 2
   ```

At the prompt, paste in the shared secret you copied from the Security Console.

You will see a verification message if the shared secret has been applied successfully.

9. Enable the console on the engine. Example:

   ```
   enable console 2
   ```
   You will see many lines logged as the pairing takes place.

10. Return to the Scan Engines page on the Security Console Web interface. Click **Refresh displayed Engines**. Verify that the Scan Engine you just paired has been added. Click the Refresh icon for that Scan Engine to confirm that the Security Console can query it.

    By default, when you have created a trusted pairing with this method, the comunication direction will be from Engine to Console.

Setting up LDAP/AD authentication sources

LDAP (including Microsoft Active Directory): Active Directory (AD) is an LDAP-supportive Microsoft technology that automates centralized, secure management of an entire network's users, services, and resources.

You can integrate Nexpose with external authentication sources like LDAP/AD. If you use one of these sources, leveraging your existing infrastructure will make it easier for you to manage user accounts.

Before you can create externally authenticated user accounts you must define external authentication sources.

To define external authentication sources:

1. Go to the *Authentication* page in the *Security Console Configuration* panel.
2. Click **Add...** in the area labelled *LDAP/AD authentication sources* to add an LDAP/Active Directory authentication source

   The Security Console displays a box labeled *LDAP/AD Configuration*.
3. Click the check box labeled **Enable authentication source**.
4. Enter the name, address or fully qualified domain name, and port of the LDAP server that you wish to use for authentication.

   Note: It is recommended that you enter **a fully qualified domain name in all capital letters** for the LDAP server configuration. Example: SERVER.DOMAIN.EXAMPLE.COM

   Default LDAP port numbers are 389 or 636, the latter being for SSL. Default port numbers for Microsoft AD with Global Catalog are 3268 or 3269, the latter being for SSL.
5. (*Optional*) Select the appropriate check box to require secure connections over SSL.
6. (*Optional*) Specify permitted authentication methods, enter them in the appropriate text field. Separate multiple methods with commas (,), semicolons (;), or spaces.

   Note: It is not recommended that you use PLAIN for non-SSL LDAP connections.

   Simple Authentication and Security Layer (SASL) authentication methods for permitting LDAP user authentication are defined by the Internet Engineering Task Force in document *RFC 2222* (http://www.ietf.org/rfc/rfc2222.txt). The application supports the use of GSSAPI, CRAM-MD5, DIGEST-MD5, SIMPLE, and PLAIN methods.
7. Click the checkbox labeled **Follow LDAP referrals** if desired.

As the application attempts to authenticate a user, it queries the target LDAP server. The LDAP and AD directories on this server may contain information about other directory servers capable of handling requests for contexts that are not defined in the target directory. If so, the target server will return a referral message to the application, which can then contact these additional LDAP servers. For information on LDAP referrals, see the document *LDAPv3 RFC 2251* (http://www.ietf.org/rfc/rfc2251.txt).

8. Enter the base context for performing an LDAP search if desired. You can initiate LDAP searches at many different levels within the directory.

   To force the application to search within a specific part of the tree, specify a search base, such as CN=sales,DC=acme,DC=com.

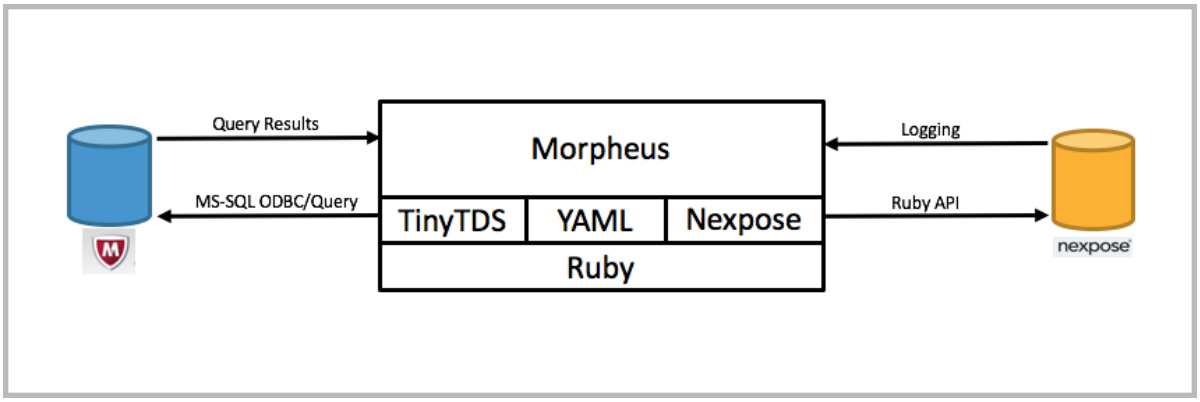
9. Click one of the three buttons for LDAP attributes mappings, which control how LDAP attribute names equate, or map, to attribute names.

   Your attribute mapping selection will affect which default values appear in the three fields below. For example, the LDAP attribute Login ID maps to the user's login ID. If you select AD mappings, the default value is sAMAccountName. If you select AD Global Catalog mappings, the default value is userPrincipalName. If you select Common LDAP mappings, the default value is uid.

10. Click **Save**.

    The Security Console displays the *Authentication* page with the LDAP/AD authentication source listed.

MVM, Nexpose parity, and concept mapping



Migration utility functionality

The MVM Migration Utility is a series of command-line Ruby scripts that connect to the MVM SQL database and extracts relevant configuration and asset information to be later imported into Nexpose.

The utility will export and import the following components:

- Scan Configurations
- Asset Groups
- Asset Tags
- Asset Inventory
- Scan Credentials
- Users

The Migration Utility will import the exported configurations using the Nexpose Ruby Gem and associated API.

Planning your migration to Nexpose

This section will assist with planning your migration to Nexpose.

Using the Migration Tool

These instructions will walk you through installing, configuring and testing the Migration Utility. These instructions are based on an Ubuntu 14.04.4, however, can be easily adapted for other platforms.

You may also download and deploy a virtual appliance OVA with the migration utility already installed. If using the Migration Virtual Appliance, skip to Configuring the MVM Database for Migration section of this guide. You may download the Migration Utility OVA from the Rapid7 Customer Care Portal. Your Customer Success Manager can assist you.

Preparing the MVM Database for migration

The Migration Utility will need to query the MVM SQL Server Database directly to extract the necessary information for the migration. To do this, we need to configure SQL Server to:

- Allow remote connections to the database.
- Assign a static listening port.
- Create a user to the MVM faultline database, with read-only access.
- Configure Windows Firewall or other end-point protection to allow inbound access to SQL Server.

Note: Depending on your environment, some or all of these perquisites may already be completed.

Allow Remote Connections to the Database

SQL Server 2005

1. From the MVM Database Server, open the SQL Server Surface Area Configuration utility.
2. On the SQL Server 2005 Surface Area Configuration page, click Surface Area Configuration for Services and Connections.
3. On the Surface Area Configuration for Services and Connections page, expand Database Engine, click Remote Connections, click Local and remote connections, click the appropriate protocol to enable for your environment, and then click Apply.

   Note: Click OK when you receive the message reading *Changes to Connection Settings will not take effect until you restart the Database Engine service*.
4. On the Surface Area Configuration for Services and Connections page, expand Database Engine, click Service, click Stop. wait until the MSSQLSERVER service stops, and then click Start to restart the MSSQLSERVER service.

SQL Server Express/Standard/Enterprise 2008/2008R2/2012

1. From the MVM Database Server, open up the SQL Server Configuration Manager.
2. Expand the SQL Server Network Configuration node and select the Protocols for SQLEXPRESS (or whatever your instance of SQL Server is called).
3. Enable TCP/IP and NAMED PIPES by right-clicking the respective protocols > Properties and selecting Enable.
4. Click on the SQL Server Services node and in the right panel right-click your SQL Server and select restart to restart the service.
5. Right-click on the SQL Server Browser and select start to start the browser service if it isn't started already. This will allow you to access the SQL Express instance by the computer name.

Assign a Static Listening Port to SQL Server

SQL Server Express/Standard/Enterprise 2005/2008/2008R2/2012

1. In SQL Server Configuration Manager, in the console pane, expand SQL Server Network Configuration, expand Protocols for <instance name>, and then double-click TCP/IP.
2. In the TCP/IP Properties dialog box, on the IP Addresses tab, several IP addresses appear in the format IP1, IP2, up to IPAll. Select IPAll.
3. If the TCP Dynamic Ports dialog box contains 0, indicating the Database Engine is listening on dynamic ports, delete the 0.
4. In the IPAll Properties area box, in the TCP Port box, type the port number you want this IP address to listen on and then click OK. Generally, this is port 1433, but can be whatever you want as long as it does not conflict with another service.
5. In the console pane, click SQL Server Services.
6. In the details pane, right-click SQL Server (<instance name>) and then click Restart, to stop and restart SQL Server.

Create a Read-only User to the faultline Database

SQL Server Express/Standard/Enterprise 2005/2008/2008R2/2012:

1. Open up SQL Server Management Studio as a SQL Server Administrator.
2. In the Object Explorer under the Security node, add a new user for the account that will be connecting by right-clicking and selecting "New User". This opens the Login Properties page. If you're on a domain then use Windows Authentication. To enable SQL logins you need to first right-click on the SQL Express instance at the top, select Properties and under Security select "SQL Server and Windows Authentication mode".
3. Select User Mapping on the Login Properties and check off the database you want to connect to. In this case ‘faultline’.

Allow Local Firewall Connectivity to SQL Server

If Windows Firewall is running and enabled. Open up Windows Firewall and select Change Settings, select the Exceptions Tab and click Add Program. You'll need to select the SQLservr.exe in Program Files\Microsoft SQL Server\MSSQL10.SQLEXPRESS\MSSQL\Binn\ and the SQLBrowser.exe in Program Files\Microsoft SQL Server\90\Shared\. Then select Properties for each of them and select the "Change Scope" button. Then select the proper scope.

Note: If you are running another end-point protection solution, please refer to the products documentation to allow inbound and outbound access to SQL Server.

Installing the migration utility

Download the Migration Utility Virtual

The MVM Migration Virtual Appliance contains the MVM Migration Utility and all necessary requirements preinstalled on an Ubuntu 14.04 Linux platform. You may download the Virtual Appliance from the Rapid7 Customer Care Portal.

The Virtual Appliance is in OVA format and will install on any hypervisor that accepts the OVA/OVF format.

The default username and password to the appliance is:

Username: migrate

Password: mvm

The migration utility is installed in the /opt/morpheus-exporter directory.

If you are using the preconfigured MVM Virtual Appliance, proceed to the section titled Configure FreeTDS, as the preceding sections will have been completed for you.

Install the Latest Version of the Migration Utility

1. Obtain the latest version of the Migration Utility from your Rapid7 Customer Success Manager.

2. Change directories and change the properties of bin/morpheus.rb file to allow execute:

```
user:@host:~/morpheus-exporter$ chmod +x bin/morpheus
```

Install Ruby Version Manager (RVM) and Ruby =>2.2.2

1. Before any other step install mpapis public key (might need gpg2):

```
user:@host:~$ gpg --keyserver hkp://keys.gnupg.net --recv-keys
409B6B1796C275462A1703113804BB82D39DC0E3
```

2. Install RVM stable with Ruby 2.2.2 (must be 2.2.2 or higher):

```
user:@host:~$ sudo \curl -sSL https://get.rvm.io | bash -s stable --
ruby=2.2.2
```

3. Execute the following command to enable Ruby:

```
user:@host:~$ source /home/migrate/.rvm/scripts/rvm
```

4. Verify Ruby version, should be 2.2.2 or higher:

```
user:@host:~$ ruby -v
ruby 2.2.2p95 (2015-04-13 revision 50295) [x86_64-linux]
```

5. If you're running multiple versions of Ruby, set the default Ruby version in RVM:

```
user:@host:~$ sudo rvm --default use 2.2.2
Using /usr/local/rvm/gems/ruby-2.2.2
```

Install the Git Utility

```
user:@host:~$ sudo apt-get install git
```

Install the Bundler Ruby Gem

1. Install the bundler gem:

```
user:@host:~$ gem install bundler
```

2. Run the bundler installer from the morpheus-exporter directory (do not run as root):

```
user:@host:~/morpheus-exporter$ bundle install
Fetching git://github.com/rails-sqlserver/tiny_tds.git
Fetching gem metadata from https://rubygems.org/.....
Fetching version metadata from https://rubygems.org/..
Resolving dependencies...
Installing builder 3.2.2
Installing mini_portile2 2.0.0
Installing byebug 8.2.2 with native extensions
Installing coderay 1.1.1
Installing rack 1.6.4
Installing systemu 2.6.5
Installing method_source 0.8.2
Installing nexpose 3.2.0
Installing nori 2.6.0
Installing slop 3.6.0
Installing thor 0.19.1
Using bundler 1.11.2
Installing gyoku 1.3.1
Installing nokogiri 1.6.7.2 with native extensions
Using tiny_tds 0.9.5.rc.3 from git://github.com/rails-sqlserver/tiny_tds.git
(at master@82edfd5)
Installing httpi 2.4.1
Installing macaddr 1.7.1
Installing pry 0.10.3
Installing akami 1.3.1
Installing wasabi 3.5.0
Installing uuid 2.3.8
Installing pry-byebug 3.3.0
Installing savon 2.10.1
Bundle complete! 6 Gemfile dependencies, 23 gems now installed.
Use `bundle show [gemname]` to see where a bundled gem is installed.
```

3. If you get an error, Gem::Ext::BuildError: ERROR: Failed to build gem native extension, install the following libraries and then re-run step 3:

```
user:@host:~$ sudo apt-get install libgmp3-dev
```

Install FreeTDS (Ubuntu 12.04 / 14.04)

```
user:@host:~$ sudo apt-get install freetds-bin
```

Configure FreeTDS

FreeTDS is a database utility that we will use to verify we have properly configured the MVM SQL Server Database to accept remote connections.

1. Obtain the location of the freetds.conf file:

```
user:@host:~$ tsql -C
Compile-time settings (established with the "configure" script)
                         Version: freetds v0.91
             freetds.conf directory: /etc/freetds
     MS db-lib source compatibility: no
        Sybase binary compatibility: yes
                    Thread safety: yes
                    iconv library: yes
                      TDS version: 4.2
                            iODBC: no
                        unixodbc: yes
              SSPI "trusted" logins: no
                        Kerberos: yes
```

2. Edit /etc/freetds/freetds.conf:

```
user:@host:~$ sudo nano /etc/freetds/freetds.conf
```

3. Modify the [global] section of the freetds.conf and uncomment and change the TDS protocol version to reflect the following:

```
# TDS protocol version
tds version = 8.0
```

4. Add the following section to the end of the file:

```
[mvm]
        host = MSSQL_SERVER_HOSTNAME -OR- IP_ADDRESS
        port = 1433
        tds version = 8.0
```

Testing Database Connectivity with FreeTDS

If we are unable to connect and query the MVM database using FreeTDS, we will not be able to connect with the Migration Utility. Perform the following steps to verify connectivity to the MVM database.

1. Test the configuration with the hostname with the following:

```
user:@host:~$ tsql -H [[MSSQL_SERVER]] -U username -P password -p 1433 -D
faultline
```

A successful connection will look like this:

```
user:@host:~$ tsql -H [[MSSQL_SERVER]] -U username -P password -p 1433 -D
faultline
locale is "en_US.UTF-8"
locale charset is "UTF-8"
using default charset "UTF-8"
1>
```

2. Test the configuration with freetds.conf configuration with the following:

```
user:@host:~$ tsql -S mvm -U nxadmin -P nxadmin -D faultline
```

A successful connection will look like this:

```
user:@host:~$ tsql -S mvm -U nxadmin -P nxadmin -D faultline
locale is "en_US.UTF-8"
locale charset is "UTF-8"
using default charset "UTF-8"
1>
```

3. Validate the ability to query the database:

```
user:@host:~$ tsql -S mvm -U nxadmin -P nxadmin -D faultline
locale is "C"
locale charset is "ANSI_X3.4-1968"
using default charset "ISO-8859-1"
1> SELECT * FROM Job.Detail
2> GO
```

Testing the Migration Utility

Test Morpheus to ensure it is working properly:

```
user:@host:~/morpheus-exporter$ bundle exec bin/morpheus mvm dry_run --
host=[[MSSQL_SERVER_HOSTNAME]] --user=[[DATABASE_USERNAME]] --
pwd=[[PASSWORD]] --database=faultline
```

Note: The default database name for MVM is *faultline*.

Using the Migration Utility

The MVM Migration Utility is a command line utility that will allow the export of certain configuration settings and data from MVM and allow import into Nexpose. The elements of MVM that can be exported are:

- Scan Configurations
- Asset Inventory (Hostname, IP Address)
- Most Recent Asset Scan Data (Vulnerabilities, Ports, Services, OS)
- Asset Groups
- Asset Tags
- User Accounts
- Credentials (Credential Name, Username, Service)

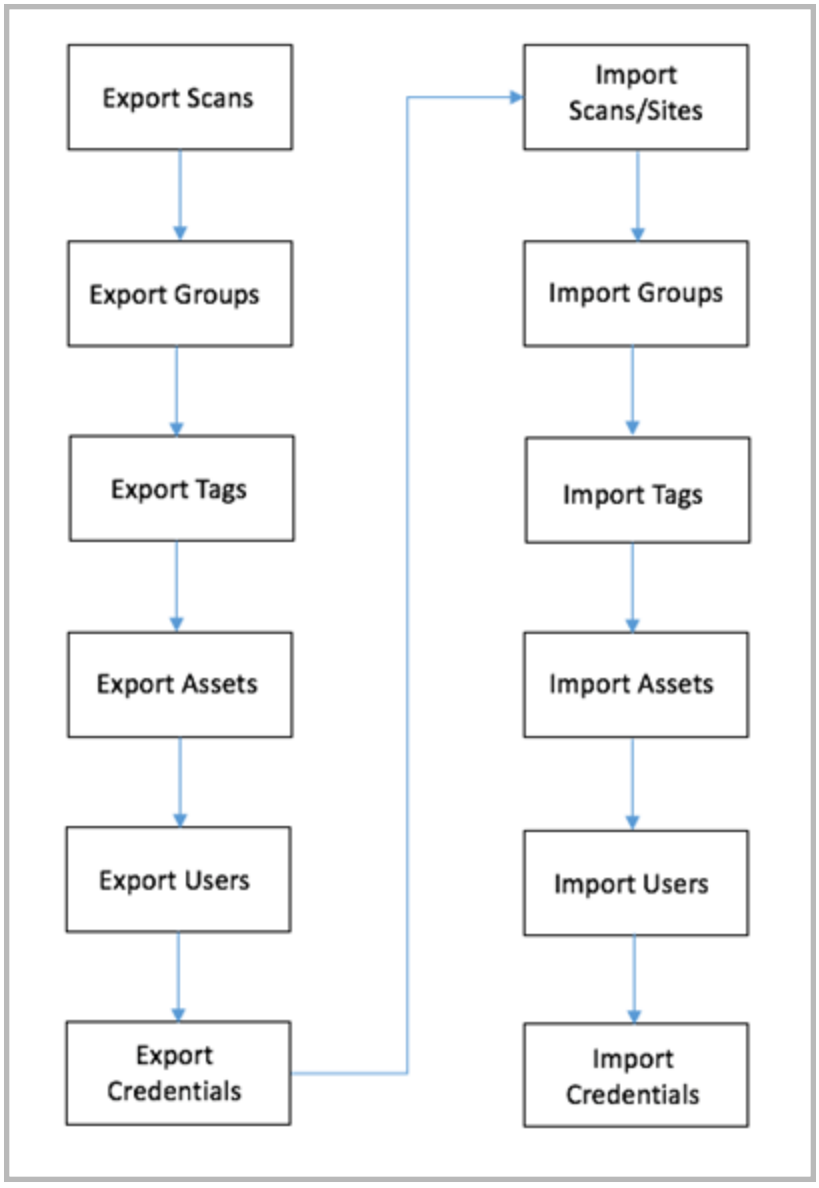
The Migration Utility will write the exported data to the output directory. The contents will look like the following:

```
output
├── groups
│   └── 2 (MVM Group ID)
│   ├── assets
│   │   └── 1.yaml (Asset Data)
│   └── group.yaml (Group Configuration)
├── sites
│   ├── 60 (MVM Site ID)
│   │   ├── assets
│   │   │   └── 1.yaml (Asset Data for Scan)
│   │   └── scan.yaml (Scan Configuration)
│   ├── 66
│   │   ├── assets
```

```
│   │   │   └── 1.yaml
│   │   └── scan.yaml
│   └── 67
│   ├── assets
│   │   └── 1.yaml
│   └── scan.yaml
├── tags
│   └── 18
│   ├── assets
│   │   └── 1.yaml (Asset Data for Tag)
│   └── tag.yaml (Tag Data)
└── users
    ├── 2.yaml (User Data)
    ├── 3.yaml
    └── 4.yaml
└── Credentials
└── Service_CredSet_Username.yaml (Credential Data)
```

Where each folder under ‘sites’ is the id of the MVM scan. The Assets folder under each scan contains the Nexpose external representation of an MVM asset.

MVM Migration Utility Workflow



Exporting from MVM

The Migration Utility is a command-line utility that is broken into two major functions: exporting configuration data from MVM and importing the exported MVM configuration data into Nexpose. Each of these functions will be performed independently, and the resultant exported data will be saved to disk.

To List the Main Morpheus Commands:

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus
Commands:
  morpheus help [COMMAND]  # Describe available commands or one specific command
  morpheus mvm <command>   # MVM related commands.
  morpheus nex <command>   # Nexpose related commands.
```

Exporting

To List the MVM Sub-commands:

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus help mvm
Commands:
  morpheus mvm dry_run HOST USER PWD DATABASE
# List the counts of scans, users...
  morpheus mvm export_asset_groups HOST USER PWD DATABASE ORG
# Exports all asset groups in the...
  morpheus mvm export_assets HOST USER PWD DATABASE ORG SCAN TAG GROUP --type=TYPE
# Exports all assets in a given s...
  morpheus mvm export_scans HOST USER PWD DATABASE ORG
# Exports all scans or specific s...
  morpheus mvm export_tags HOST USER PWD DATABASE ORG
# Exports all tags in the given org
  morpheus mvm export_users HOST USER PWD DATABASE ORG
# Exports all users in the given org
  morpheus mvm help [COMMAND]
# Describe subcommands or one spe...

Options:
  --host=HOST          # Host where MVM is installed
  --user=USER          # Database user for MVM instance
  --pwd=PWD            # Database user password for MVM instance
  --database=DATABASE  # MVM database instance to export from
  --org=ORG            # MVM Root organization to export from
```

Exporting Scan Configurations

It's best to start the exporting of scan configurations. This will export the Scan Name, Included IP Range, Excluded IP Range and Scan Schedule.

Scan Export Help:

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus mvm help export_scans
Options:
--host=HOST                              # Host where MVM is installed
--user=USER                              # Database user for MVM instance
--pwd=PWD                                # Database user password for MVM instance
--database=DATABASE                      # MVM database instance to export from
--org=ORG                                # MVM Root organization to export from
--scan-ids=1 2 3]                        # Optional list of scan ids to be exported
```

To export all scan configurations from MVM:

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus mvm export_scans --
host=[[MSSQL_SERVER_HOSTNAME]] --user=[[DATABASE_USERNAME]] --pwd=[[PASSWORD]] --
database=faultline --org=[[MVM_ORG_NAME]]
Processing My Network : 57
Processing Test Scan : 55
```

To export specific scan configurations (no asset inventory, no vulnerabilities) from MVM, use '--scan_ids=' option:

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus mvm export_scans --scan_ids=64 56
--host=[[MSSQL_SERVER_HOSTNAME]] --user=[[DATABASE_USERNAME]] --pwd=[[PASSWORD]] --
database=faultline
Processing My Network : 64
Processing Test Scan : 56
```

Note: Scan IDs can be obtained in the MVM URL when editing or viewing a Scan Configuration.

Exporting Asset Groups

MVM Asset Groups can be exported.

Asset Group information will be stored in the output/groups/[[GROUP_ID]]/group.yaml file.

To export Asset Groups from MVM:

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus mvm export_asset_groups --
host=[[MSSQL_SERVER_HOSTNAME]] --user=[[DATABASE_USERNAME]] -pwd=[[PASSWORD]] --
database=faultline -- org=[[MVM_ORG_NAME]]
```

Exporting Asset Tags

MVM Asset Tags can be exported.

Asset Tag information will be stored in the output/tags/[[TAG_ID]]/tag.yaml file.

To export Asset Tags from MVM:

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus mvm export_tags --
host=[[MSSQL_SERVER_HOSTNAME]] --user=[[DATABASE_USERNAME]] -pwd=[[PASSWORD]] --
database=faultline --org=[[MVM_ORG_NAME]]
```

Exporting Assets

Once you've exported your scan configurations, asset groups and tags, you may wish to export the asset inventory associated with those scans/groups/tags. The asset inventory contains the asset host name, IP address, MAC address, service fingerprint (service name, port, protocol), OS fingerprint, and optionally, most recently identified vulnerabilities. Importing assets will also allow you to apply asset tags that where assigned in MVM to the assets in Nexpose.

Use the 'Type' option with the value of SCANS, TAGS or GROUPS to export the assets associated to the respective value. Asset data will be stored in the output/[sites|groups|tags]/[ID] /assets/1.yaml file.

To export assets from MVM:

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus mvm export_all_assets --
host=[[MSSQL_SERVER_HOSTNAME]] --user=[[DATABASE_USERNAME]] -pwd=[[PASSWORD]] --
database=faultline --org=[[MVM_ORG_NAME]] type=[SCANS|TAGS|GROUPS]
```

To export vulnerabilities associated with each exported asset, use the '--with_vulns' option:

Note: On MVM systems with a large number of assets, this can take a while to run.

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus mvm export_all_assets --
host=[[MSSQL_SERVER_HOSTNAME]] --user=[[DATABASE_USERNAME]] -pwd=[[PASSWORD]] -
database=faultline type=[SCANS|TAGS|GROUPS] --with_vulns
```

Exporting Users

MVM users in can be exported.

User information exported will include username, full name, email address.

Exported users will reside in the output/credentials directory.

To export users:

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus mvm export_users --scan_ids=64 56
--host=[[MSSQL_SERVER_HOSTNAME]] --user=[[DATABASE_USERNAME]] --pwd=[[PASSWORD]] --
database=faultline
Processing user Administrator
Processing user user1
Processing user user2
Processed 3 users
```

Exporting Credentials

MVM Credential Set credentials can be exported.

Due to encryption schemes being used in MVM, credential passwords and/or private keys will not export. Passwords must be reentered in Nexpose.

Exported credentials will reside in the output/credentials directory.

To export users:

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus mvm export_credentials --
host=[[MSSQL_SERVER_HOSTNAME]] --user=[[DATABASE_USERNAME]] --pwd=[[PASSWORD]] --
database=faultline --org=[[MVM_ORG_NAME]]
I, [2016-03-07 10:26:48 #5356]  INFO -- : Exported 'Test-Creds_Administrator' credential.
I, [2016-03-07 10:26:48 #5356]  INFO -- : Exported 'Test-Creds_root' credential.
```

Importing to Nexpose

To List the Nexpose Sub-commands:

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus help nex
Commands:
morpheus nex help [COMMAND]             # Describe subcommands or one specific subcommand
morpheus nex import_asset_groups HOST USER PWD PATH  # Import asset_groups into nexpose.
morpheus nex import_sites HOST USER PWD PATH         # Import sites into nexpose.
morpheus nex import_tags HOST USER PWD PATH          # Import tags into nexpose.
morpheus nex import_users HOST USER PWD PATH         # Import users into nexpose.

Options:
  [--host=HOST]
  [--user=USER]
  [--pwd=PWD]
  [--path=PATH]
```

Importing Scans

The import of scan configurations will create the Nexpose equivalent called a Site. A Site contains the asset(s)/range(s) to be scanned, the asset(s)/range(s) to be excluded, the scan template for the scan to use, scan engine for the scan to use, the scan schedule, alerts and access permissions. The importer will default the scan template to 'Full Audit without Web Spider', and the scan engine to 'Local' engine. Access permissions will need to be assigned after all scans and users are imported.

The imported Site name in Nexpose will be in the format, ORG_WORKGROUP_SCAN NAME. This will allow you to easily identify which scans belong to specific MVM Organizations/Workgroups and avoid the potential to have duplicate Site names in Nexpose.

To import scan configs into Nexpose, use the 'import_sites' command. For additional help use the '--help' option.

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus nex import_sites --
host=[[NEXPOSE_CONSOLE]] --user=[[NEXPOSE_ADMIN]] --pwd=[[PASSWORD]] --path output/sites
```

Set the '--path' option to output/sites

Importing Asset Groups

Any asset groups that have been created in MVM will be imported as Static Asset Groups in Nexpose. This portion of the import will just create the groups. We will import assets into the group in a later step.

To Import Asset Groups into Nexpose, use the 'import_asset_groups' command. For additional help use the '--help' option.

Be sure to set the '--path' option to output/groups.

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus nex import_asset_groups --
host=[[NEXPOSE_CONSOLE]] --user=[[NEXPOSE_ADMIN]] --pwd=[[PASSWORD]] --path output/groups
I, [2016-02-17 22:30:48 #11697]  INFO -- : Imported MVM group Group1 to Nexpose group 7
I, [2016-02-17 22:30:49 #11697]  INFO -- : Imported MVM group Group2 to Nexpose group 8
```

Importing Asset Tags

Any asset tags that were created in MVM can be imported into Nexpose. Be aware that the dynamic filters will not migrate to Nexpose from MVM, however, Nexpose does support dynamic tagging of assets based on specified criteria. Any dynamic tags in MVM will be applied as a static tag in Nexpose.

If an assets criticality and/or owner have been set, these will map to the criticality and owner tags in Nexpose. Any other tags that have been applied will be imported as custom tags. Tags will not get applied to assets until assets are imported.

To Import Asset Tags into Nexpose, use the 'import_tags' command. For additional help use the '--help' option.

Be sure to set the '--path' option to output/tags. For additional help use the '--help' option.

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus nex import_tags --
host=[[NEXPOSE_CONSOLE]] --user=[[NEXPOSE_ADMIN]] --pwd=[[PASSWORD]] --path output/tags
I, [2016-02-18 15:33:13 #13027]  INFO -- : Imported MVM tag Paris to Nexpose tag 28
I, [2016-02-18 15:33:14 #13027]  INFO -- : Imported MVM tag Berlin to Nexpose tag 29
I, [2016-02-18 15:33:14 #13027]  INFO -- : Imported MVM tag Moscow to Nexpose tag 30
I, [2016-02-18 15:33:14 #13027]  INFO -- : Imported MVM tag London to Nexpose tag 31
```

Importing Users

Users account created in MVM can be imported into Nexpose. This will import the username, full name, and email address. All users will be imported as a 'user' role in Nexpose, so review the post migration task of assigning user roles and permissions.

The default import setting will configure users to be local users, meaning credentials and authentication will be managed within Nexpose. Imported users will be set with a default password of 'notpassword'.

If Active Directory, LDAP or Kerberos authentication is being used for user authentication, be sure to setup the Authentication Connector in Nexpose prior to importing users, as you will be able to specify the connector name to assign users during the import process.

To Import Users into Nexpose, use the 'import_tags' command. For additional help use the

'--help' option.

To assign an authentication connector during import use the '--use-ldap' and

'--ldap-name=[[CONNECTOR_NAME]]'. The connector name is what you named the connector in the Nexpose Console, under Administration > Console Administration > Authentication.

Be sure to set the '--path' option to output/users.

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus nex import_users
host=[[NEXPOSE_CONSOLE]] --user=[[NEXPOSE_ADMIN]] --pwd=[[PASSWORD]] --path=output/users --
use-ldap --ldap-name=[[CONNECTOR_NAME]]
I, [2016-02-18 15:48:49 #13053]  INFO -- : Processed MVM user OtherAdmin to Nexpose user 8
I, [2016-02-18 15:48:49 #13053]  INFO -- : Processed MVM user GlobalAdmin to Nexpose user 9
I, [2016-02-18 15:48:49 #13053]  INFO -- : Processed MVM user Administrator to Nexpose user
10
I, [2016-02-18 15:48:49 #13053]  INFO -- : Processed MVM user dmorash to Nexpose user 11
W, [2016-02-18 15:48:50 #13053]  WARN -- : failed to process dmorash output/users/6.yaml
NexposeAPI: Action failed: A user with the same login name already exists.
I, [2016-02-18 15:48:50 #13053]  INFO -- : Processed MVM user jblow to Nexpose user 12
```

In MVM, it is possible to have two users with the same username in two different MVM organizations. Duplicate usernames are not allowed in Nexpose. The Importer will only process the first instance of a username and skip any duplicate usernames.

Importing Assets

Now that we have the general structure of the Nexpose configuration migrated from MVM, we can begin to import the asset inventory, and optionally vulnerability data. There are a few things to know about the import process:

1. The import process will import the following asset attributes: Hostname, IP Address, Operating system fingerprint, Identified ports and fingerprinted services, Vulnerability data (optional)
2. The importer will import the last scanned state of an asset. If the asset was last scanned six months ago, its state at that time will be imported.
3. The importer does not import historical scan data. Historical trending of an imported asset will not be available prior to the import date.
4. Nexpose will assign the OS fingerprint in CPE notation, however, this will be replaced with the Nexpose fingerprint upon initial discovery/scan.
5. Vulnerability content is mapped using the CVE ID of vulnerabilities identified in MVM to a corresponding CVE ID in Nexpose. It is possible that there may be multiple vulnerability checks using the same CVE ID. For example, same vulnerability on multiple platforms or versions. Do to this, the importer will map the first instance found with a particular CVE ID. You may find the correct vulnerability, but possibly referencing a different version or platform than the asset. Additionally, both MVM and Nexpose have vulnerability checks that do not have a corresponding CVE ID. In this case, vulnerabilities cannot be mapped and will be omitted. Upon first scan of an asset in Nexpose, the vulnerability results will update and reflect accordingly.
6. To apply asset tags to an asset, you must import the asset tags first, then import the assets.
7. It is imperative that Asset-linking is enabled in the Nexpose Console. This is the default.

Depending on your specific objectives, you may need to run the asset import three times. You may want to run the import_assets against sites, groups and tags to populate asset information respectively.

To Import Assets into Nexpose, use the 'import_assets' command. For additional help use the

'--help' option.

Be sure to set the '--path' option to output/[SITES/GROUPS/TAGS]

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus nex import_assets
host=[[NEXPOSE_CONSOLE]] --user=[[NEXPOSE_ADMIN]] --pwd=[[PASSWORD]] --
path=output/[SITES/GROUPS/TAGS] --type=[SITES/GROUPS/TAGS]
```

To import assets into sites:

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus nex import_assets
host=[[NEXPOSE_CONSOLE]] --user=[[NEXPOSE_ADMIN]] --pwd=[[PASSWORD]] --path=output/sites --
type=sites
```

To import assets into asset groups:

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus nex import_assets
host=[[NEXPOSE_CONSOLE]] --user=[[NEXPOSE_ADMIN]] --pwd=[[PASSWORD]] --path=output/groups --
type=groups
```

Applying tags to assets:

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus nex import_assets
host=[[NEXPOSE_CONSOLE]] --user=[[NEXPOSE_ADMIN]] --pwd=[[PASSWORD]] --path=output/tags –
type=tags
```

Importing Credentials

Exported credentials from MVM can be imported into Nexpose as 'Shared Credentials'. These are credentials that can be used across multiple Nexpose Scan Sites. Similar to MVM Credential Sets.

Depending on the type of credential imported, credentials will map to the appropriate service and populate the username, domain, hostname, privilege escalation, etc. For security purposes, passwords are not exported from MVM and thus not imported into Nexpose. It will be necessary to re-enter the passwords for all your imported scan credentials.

By default, credentials are configured in Nexpose to be applied to all existing and future Scan Sites. You may wish to restrict certain credentials to specific Scan Sites. This can be accomplished in the Nexpose Administration page, under Shared Credentials.

Credentials that were configured as 'Individual' in MVM will migrate into Nexpose with the 'Restriction' configuration set to the IP Address or Hostname that was configured in MVM.

Be sure to set the '--path' option to output/credentials.

```
user:@host:~/morpheus-exporter# bundle exec bin/morpheus nex import_credentials
host=[[NEXPOSE_CONSOLE]] --user=[[NEXPOSE_ADMIN]] --pwd=[[PASSWORD]] --
path=output/credentials
I, [2016-03-07 11:01:57 #5359]  INFO -- : Processed MVM Credential Administrator to Nexpose
Credential true
I, [2016-03-07 11:01:57 #5359]  INFO -- : Processed MVM Credential Administrator to Nexpose
Credential true
I, [2016-03-07 11:01:57 #5359]  INFO -- : Processed MVM Credential root to Nexpose
Credential true
I, [2016-03-07 11:01:57 #5359]  INFO -- : Processed MVM Credential root to Nexpose
Credential true
```

Post Migration

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:

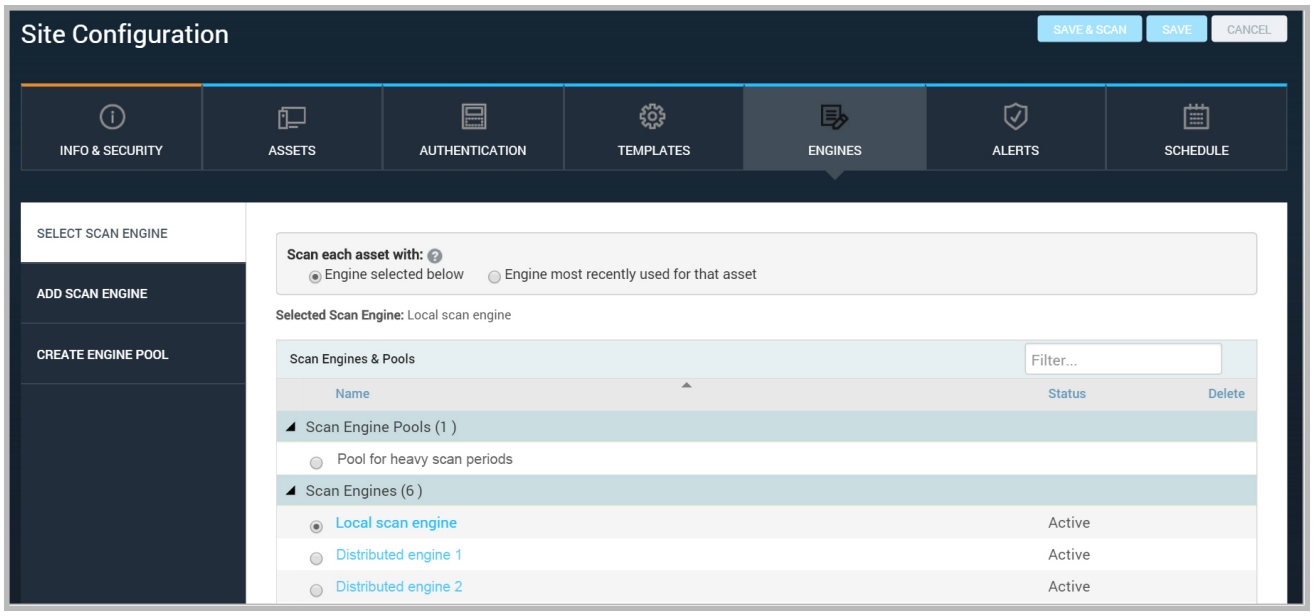
- *Configuring distributed Scan Engines* on page 1 *Configuring distributed Scan Engines*.
- *Working with Scan Engine pools* on page 1 *Working with Scan Engine pools*

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 108 *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:

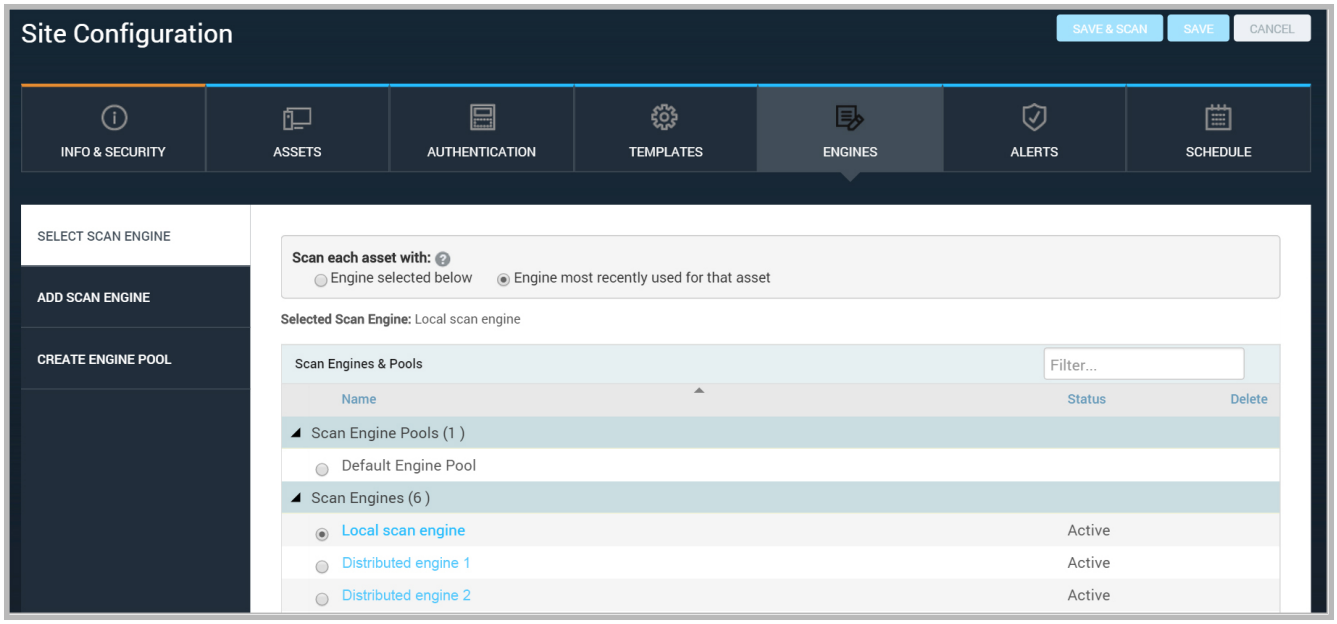
1. In the *Site Configuration*, go to the **Engines** tab.
2. If you want to scan all the assets with the same Scan Engine or Scan Engine Pool, select *Engine selected below*.

   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 1 *Running a manual scan*.

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 112 *Keep the "triangle" in mind when you tune*. 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 111 *Defining your goals for tuning*
- *The primary tuning tool: the scan template* on page 115 *The primary tuning tool: the scan template*

See also the appendix that compares all of our built-in scan templates and their use cases:

- *Scan templates* on page 1 *Scan templates*

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 1*Configuring custom scan templates*

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 1 *Scan templates*. 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 acknowledgment 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.

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 1 *Scan templates*. NexposeSymantec CCS Vulnerability Manager 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 1*Configuring custom scan templates* 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.

Note: For dynamic sites that include mobile devices, the choice of scan template is unimportant because the devices themselves are not scanned. The scan process queries information about the devices from a Windows Active Directory (AD) server.

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.

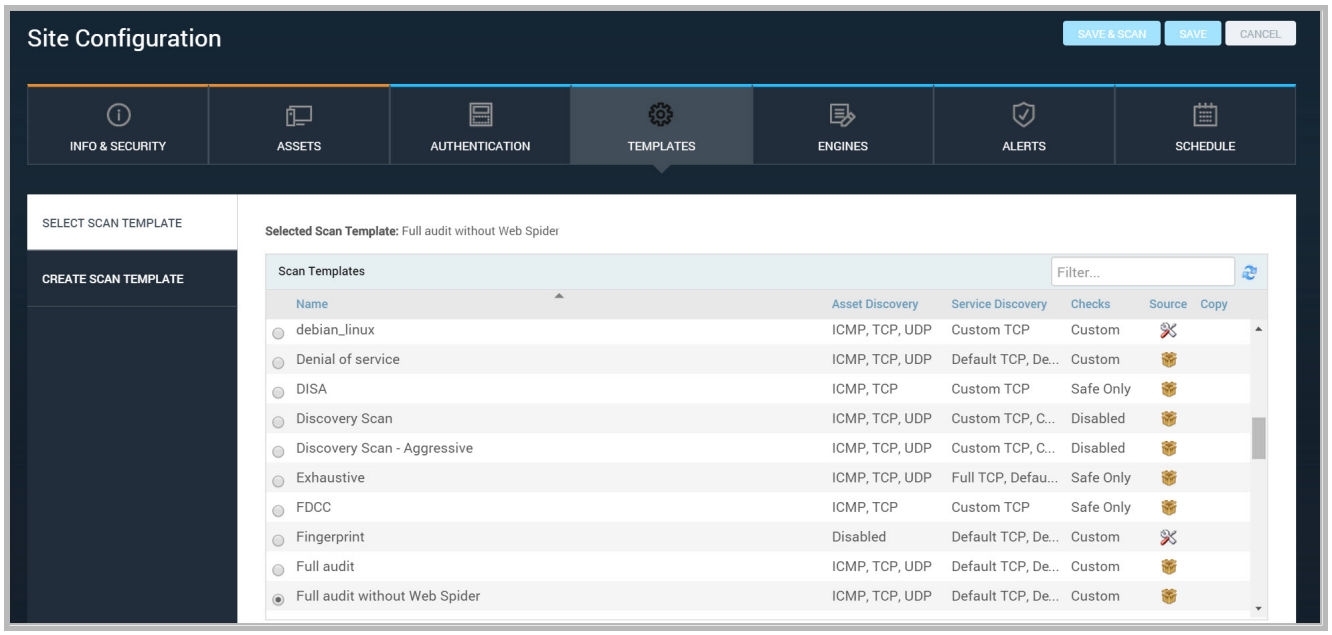
Note: If you created the site through the integration with VMware NSX, you can change the scan template but it will not affect the type of scan or the scan results. See *Integrating NSX network virtualization with scans* on page 1*Integrating NSX network virtualization with scans*.

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.

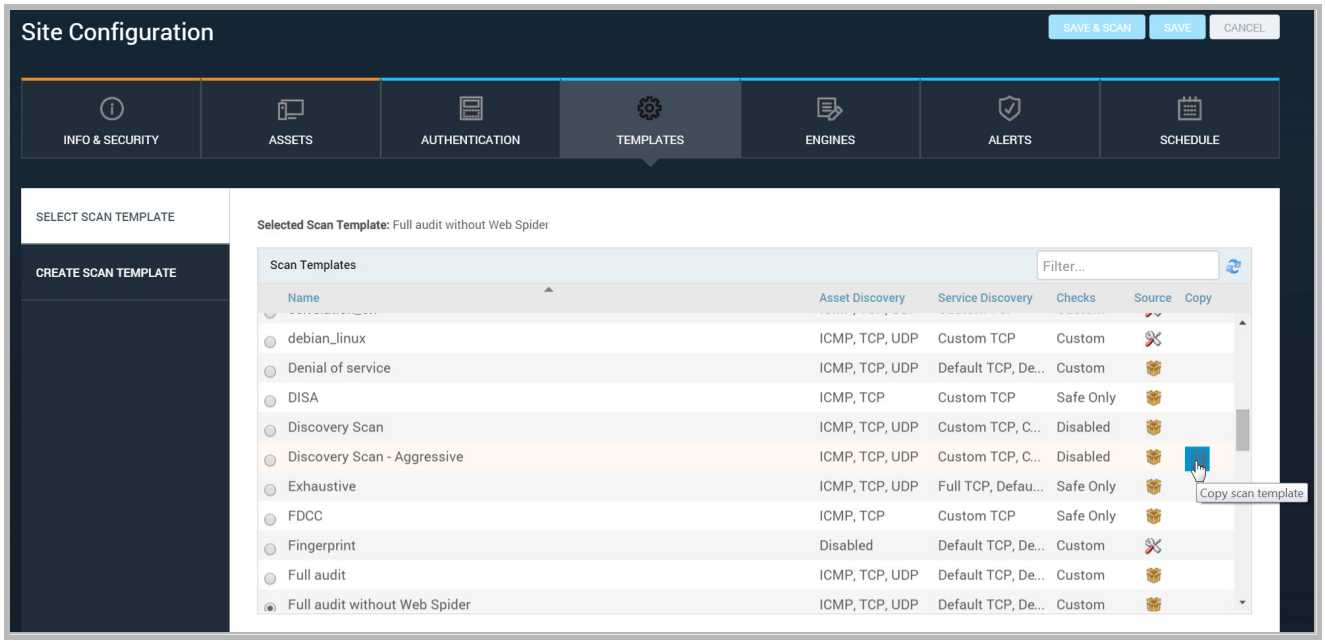
3. Save your changes.



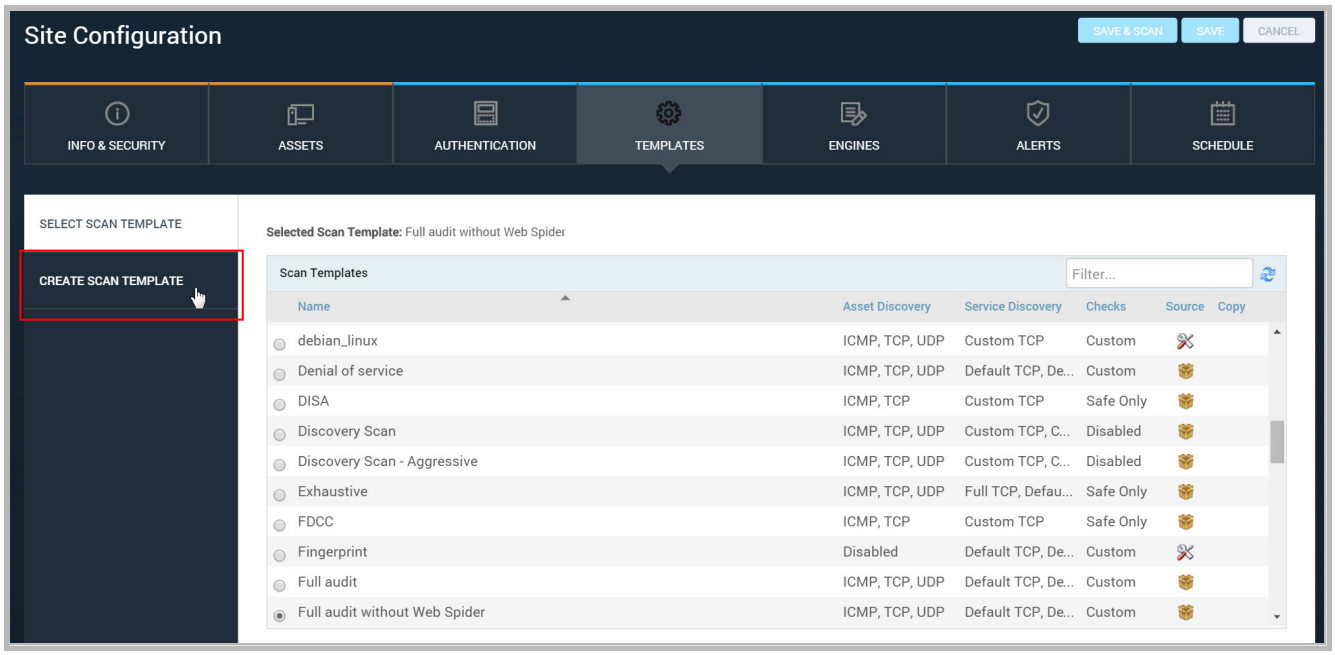
Default scan template selection

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.



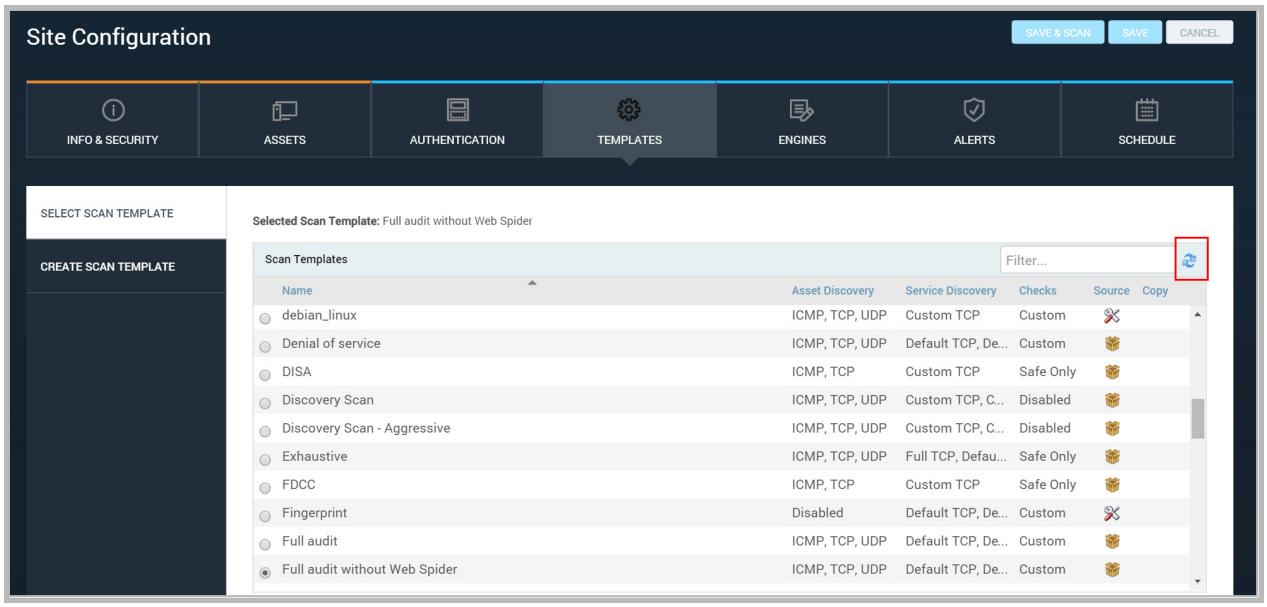
Copying an existing scan template



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 1*Configuring custom scan templates* 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.

Planning your Scan Engine deployment

Your assessment of your security goals and your environment, including your asset inventory, will help you plan how and where to deploy Scan Engines. Keep in mind that if your asset inventory is subject to change on continual basis, you may need to modify your initial Scan Engine deployment over time.

Any deployment includes a Security Console and one or more Scan Engines to detect assets on your network, collect information about them, and test these assets for vulnerabilities. Scan Engines test vulnerabilities in several ways. One method is to check software version numbers, flagging out-of-date versions. Another method is a "safe exploit" by which target systems are probed for conditions that render them vulnerable to attack. The logic built into vulnerability tests mirrors the steps that sophisticated attackers would take in attempting to penetrate your network.

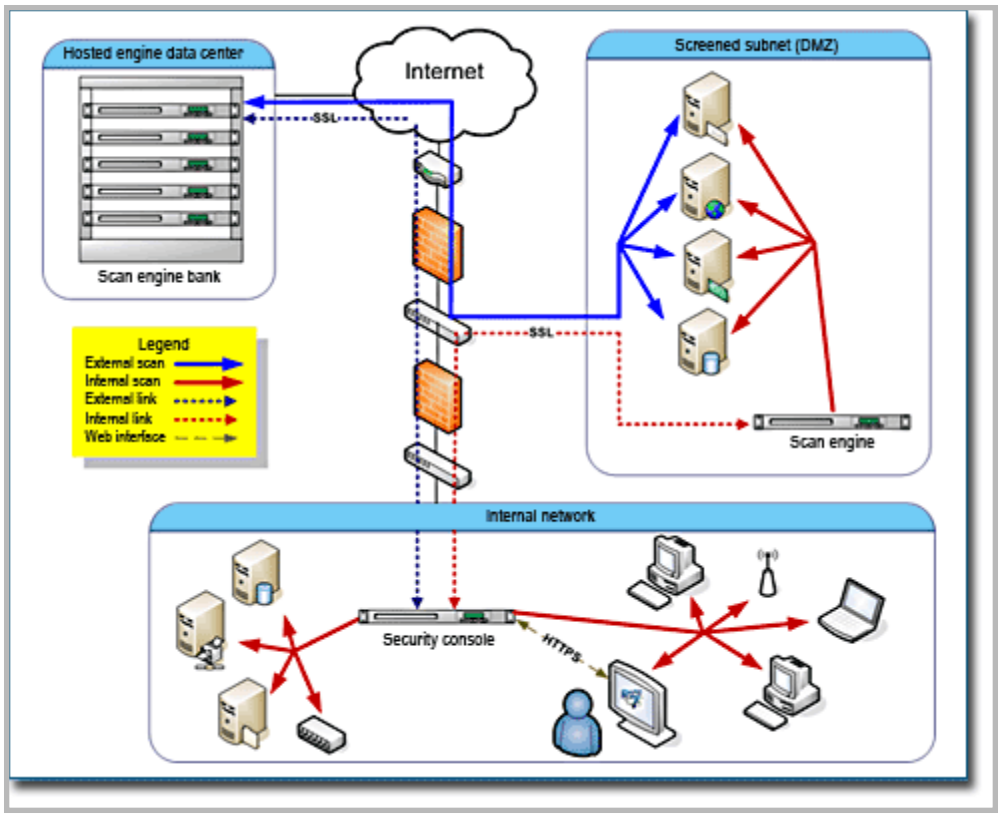
The application is designed to exploit vulnerabilities without causing service disruptions. It does not actually attack target systems.

One way to think of Scan Engines is that they provide strategic views of your network from a hacker's perspective. In deciding how and where to deploy Scan Engines, consider how you would like to "see" your network.

View your network inside-out: hosted vs. distributed Scan Engines

Two types of Scan Engine options are available—hosted and distributed. You can choose to use only one option, or you can use both in a complementary way. It is important to understand how the options differ in order to deploy Scan Engines efficiently. Note that the hosted and distributed Scan Engines are not built differently. They merely have different locations relative to your network. They provide different views of your network.

Hosted Scan Engines allow you to see your network as an external attacker with no access permissions would see it. They scan everything on the periphery of your network, outside the firewall. These are assets that, by necessity, provide unconditional public access, such as Web sites and e-mail servers.



Note: If your organization uses outbound port filtering, you would need to modify your firewall rules to allow hosted Scan Engines to connect to your network assets.

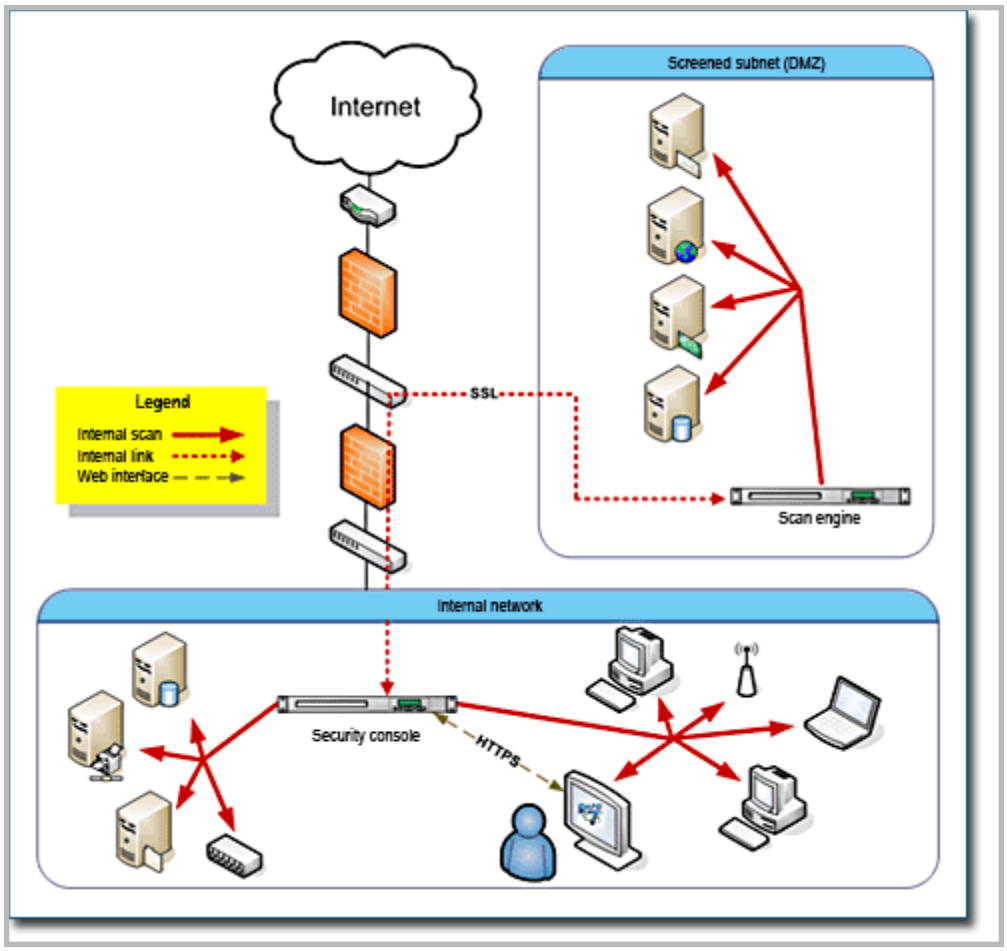
Rapid7 hosts and maintains these Scan Engines, which entails several benefits. You don't have to have to install or manage them. The Scan Engines reside in continuously monitored data centers, ensuring high standards for availability and security.

With these advantages, it might be tempting to deploy hosted Scan Engines exclusively. However, hosted Scan Engines have limitations in certain use cases that warrant deploying distributed Scan Engines.

Distribute Scan Engines strategically

Distributed Scan Engines allow you to inspect your network from the inside. They are ideal for core servers and workstations. You can deploy distributed Scan Engines anywhere on your network to obtain multiple views. This flexibility is especially valuable when it comes to scanning a network with multiple subnetworks, firewalls, and other forms of segmentation.

Note: Scan Engines do not store scan data. Instead, they immediately send the data to the Security Console.



But, how many Scan Engines do you need? The question to ask first is, where you should you put them?

In determining where to put Scan Engines, it's helpful to look at your network topology. What are the areas of separation? And where are the connecting points? If you can answer these questions, you have a pretty good idea of where to put Scan Engines.

It is possible to operate a Scan Engine on the same host computer as the Security Console. While this configuration may be convenient for product evaluation or small-scale production scenarios, it is not appropriate for larger production environments, especially if the Scan Engine is scanning many assets. Scanning is a RAM-intensive process, which can drain resources away from the Security Console.

Following are examples of situations that could call for the placement of a Scan Engine.

Firewalls, IDS, IPS, and NAT devices

You may have a firewall separating two subnetworks. If you have a Scan Engine deployed on one side of this firewall, you will not be able to scan the other subnetwork without opening the firewall. Doing so may violate corporate security policies.

An application-layer firewall may have to inspect every packet before consenting to route it. The firewall has to track state entry for every connection. A typical scan can generate thousands of connection attempts in a short period, which can overload the firewalls state table or state tracking mechanism.

Scanning through an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) can overload the device or generate an excessive number of alerts. Making an IDS or IPS aware that NexposeSymantec CCS Vulnerability Manager is running a vulnerability scan defeats the purpose of the scan because it looks like an attack. Also, an IPS can compromise scan data quality by dropping packets, blocking ports by making them “appear” open, and performing other actions to protect assets. It may be desirable to disable an IDS or IPS for network traffic generated by Scan Engines.

Having a Scan Engine send packets through a network address transition (NAT) device may cause the scan to slow down, since the device may only be able to handle a limited number of packets per second.

In each of these cases, a viable solution would be to place a Scan Engine on either side of the intervening device to maximize bandwidth and minimize latency.

VPNs

Scanning across virtual private networks (VPNs) can also slow things down, regardless of bandwidth. The problem is the workload associated with connection attempts, which turns VPNs into bottlenecks. As a Scan Engine transmits packets within a local VPN endpoint, this VPN has to intercept and decrypt each packet. Then, the remote VPN endpoint has to decrypt each packet. Placing a Scan Engine on either side of the VPN tunnel eliminates these types of bottlenecks, especially for VPNs with many assets.

Subnetworks

The division of a network into subnetworks is often a matter of security. Communication between subnetworks may be severely restricted, resulting in slower scans. Scanning across subnetworks can be frustrating because they are often separated by firewalls or have access control lists (ACLs) that limit which entities can contact internal assets. For both security and performance reasons, assigning a Scan Engine to each subnetwork is a best practice

Perimeter networks (DMZs)

Perimeter networks, which typically include Web servers, e-mail servers, and proxy servers, are “out in the open,” which makes them especially attractive to hackers. Because there are so many possible points of attack, it is a good idea to dedicate as many as three Scan Engines to a perimeter network. A hosted Scan Engine can provide a view from the outside looking in. A local Scan Engine can scan vulnerabilities related to outbound data traffic, since hacked DMZ assets could transmit viruses across the Internet. Another local Scan Engine can provide an interior view of the DMZ.

ACLs

Access Control Lists (ACLs) can create divisions within a network by restricting the availability of certain network assets. Within a certain address space, such as 192.168.1.1/254, NexposeSymantec CCS Vulnerability Manager may only be able to communicate with 10 assets because the other assets are restricted ay an ACL. If modifying the ACL is not an option, it may be a good idea to assign a Scan Engine to ACL-protected assets.

WANs and remote asset locations

Sometimes an asset inventory is distributed over a few hundred or thousand miles. Attempting to scan geographically distant assets across a Wide Area Network (WAN) can tax limited bandwidth. A Scan Engine deployed near remote assets can more easily collect scan data and transfer that data to more centrally located database. It is less taxing on network resources to perform scans locally. Physical location can be a good principle for creating a site. See Configuring scan credentialsSee the topic Configuring scan credentials in the user’s guide. This is relevant because each site is assigned to one Scan Engine.

Other factors that might warrant Scan Engine placement include routers, portals, third-party-hosted assets, outsourced e-mail, and virtual local-area networks.

Deploying Scan Engine Pools

If your license enables Scan Engine pooling, you can use pools to enhance the consistency and speed of your scan coverage. A pool is a group of Scan Engines over which a scan job is distributed. Pools are assigned to sites in the same way that individual Scan Engines are.

Tip: See *Finding out what features your license supports* in Help or the user's guide.

Pooling provides two main benefits:

- Scan load balancing prevents overloading of individual Scan Engines. When a pool is assigned to a site, scan jobs are distributed throughout the pool, reducing the load on any single Scan Engine. This approach can improve overall scan speeds.
- Fault tolerance prevents scans from failing due to operational problems with individual Scan Engines. If the Security Console contacts one pooled Scan Engine to start a scan, but the Scan Engine is offline, the Security Console simply contacts the next pooled Scan Engine. If a Scan Engine fails while scanning a given asset, another engine in that pool will scan the asset. Also, the application monitors how many jobs it has assigned to the pooled engine and does not assign more jobs than the pooled engine can run concurrently based on its memory capacity.

Note: The algorithm for how much memory a job takes is based on the configuration options specified in the scan template.

You can configure and manage pools using the Web interface. See the topic *Working with Scan Engine pools* in Help or the user's guide. You also can use the extended API v1.2. See the *API Guide*.

Best practices for deploying and scaling pools

For optimal performance, make sure that pooled Scan Engines are located within the same network or geographic location. Geographically dispersed pools can slow down scans. For example, if a pool consists of one engine in Toronto and one in Los Angeles, and this pool is used to scan a site of assets located in Los Angeles, part of that load will be distributed to the Toronto engine, which will take longer to scan the assets because of the geographical distance.

To improve the performance of pools, you can add Scan Engines or increase the amount of RAM allocated to each pooled engine. By increasing RAM, you can increase the number of simultaneous sites that can be scanned and increase the number of assets that each engine scans simultaneously, which, in turn, expands the scanning capacity of the pool. See the topic *Tuning performance with simultaneous scan tasks* in Help or the user's guide.

Creating a basic report

Creating a basic report involves the following steps:

- Selecting a report template and format (see Starting a new report configuration)
- 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 see Entering CyberScope information
- Configuring an XCCDF report
- Configuring an ARF report
- Database Export see Distributing, sharing, and exporting reports
- Baseline reports see Selecting a scan as a baseline
- Risk trend reports see Working with risk trends in reports

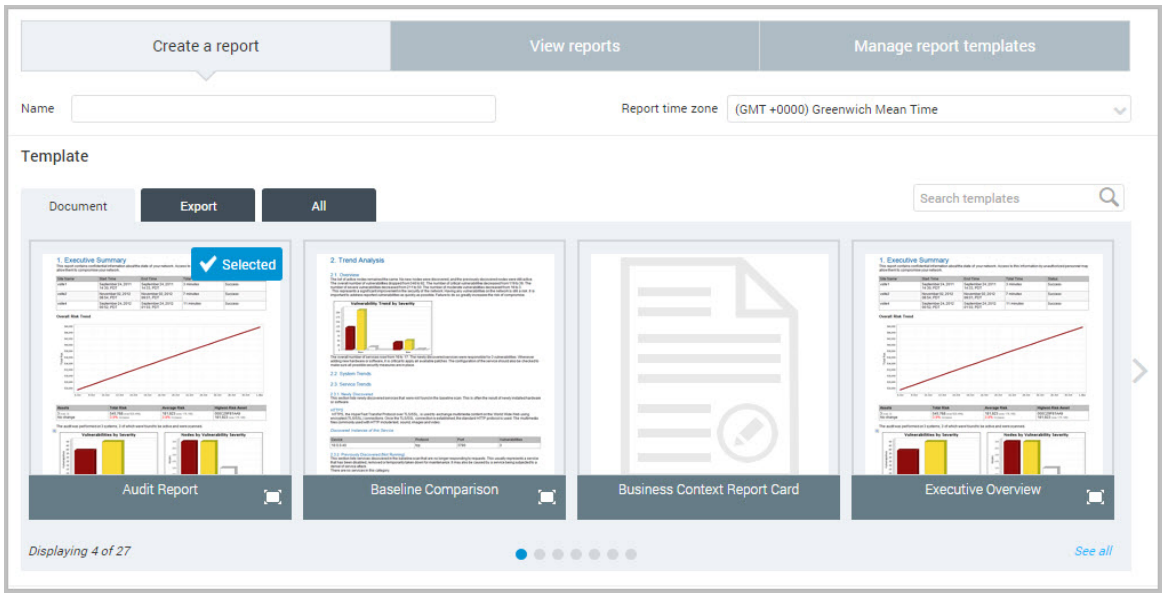
After you complete a basic report configuration, you will have the option to configure additional properties, such as those for distributing the report.

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 1 *Viewing, editing, and running reports* .

Starting a new report configuration

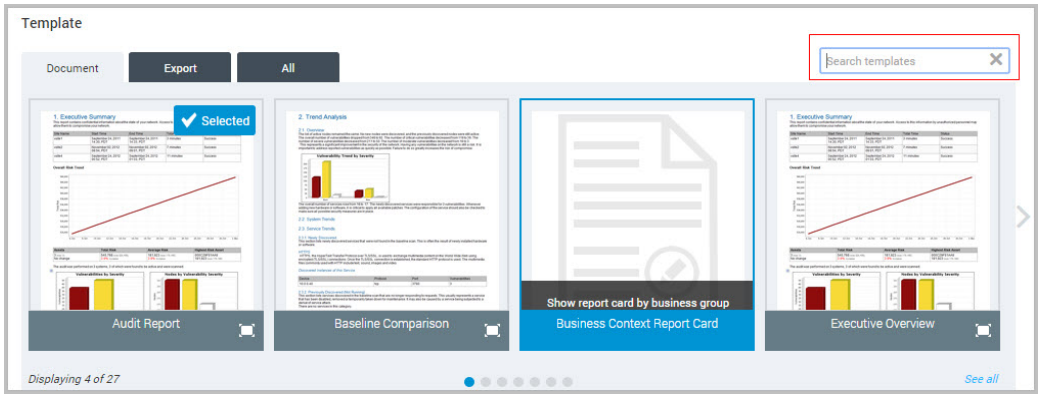
1. Click the **Reports** icon.
   OR
   Click the **Create** tab at the top of the page and then select *Report* from the drop-down list.

   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.



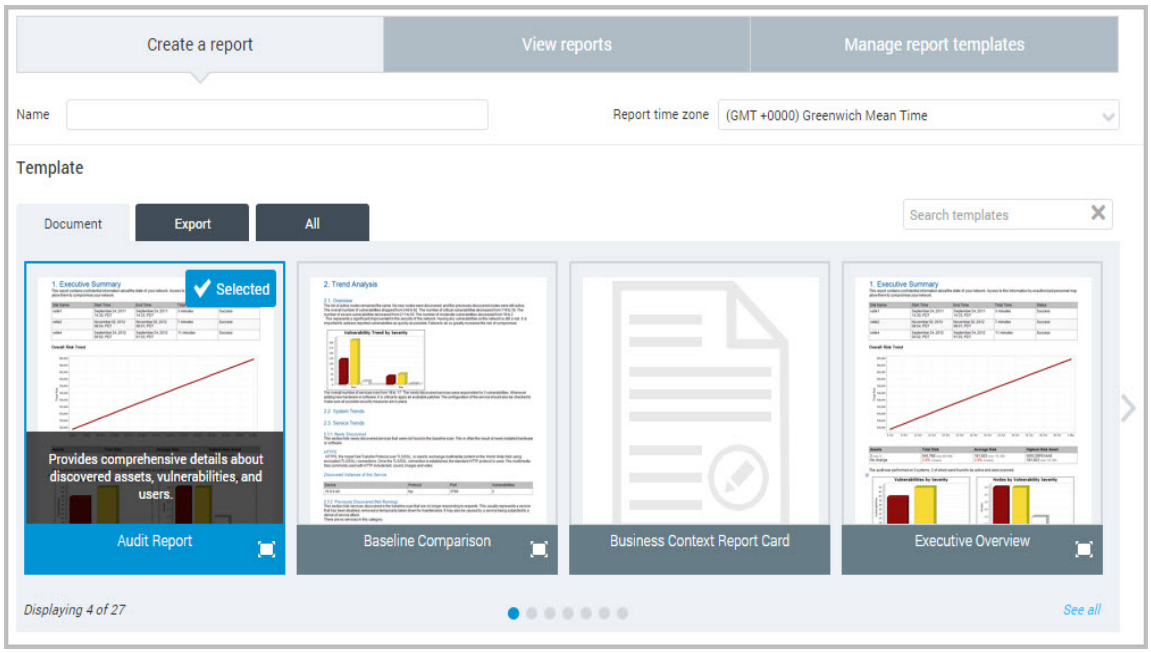
Search report templates

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 1 *Working with report formats*.
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 1 *Working with report formats*.

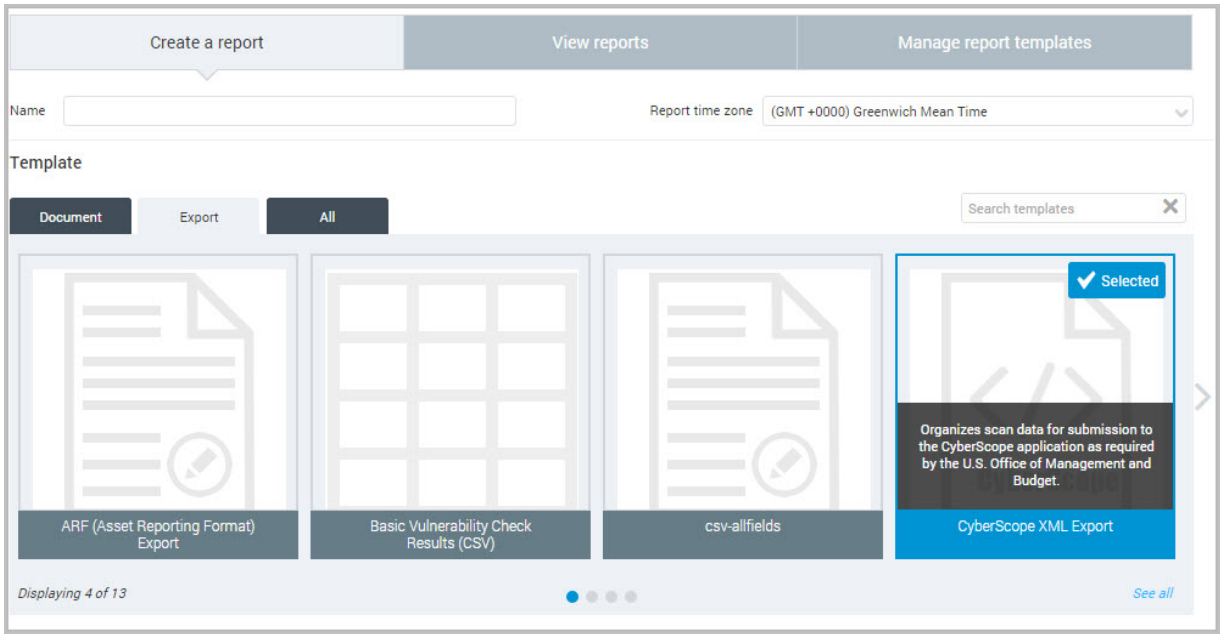
   Tip: See descriptions of all available report templates to help you select the best template for your needs.

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 134 *Entering CyberScope information*. 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.

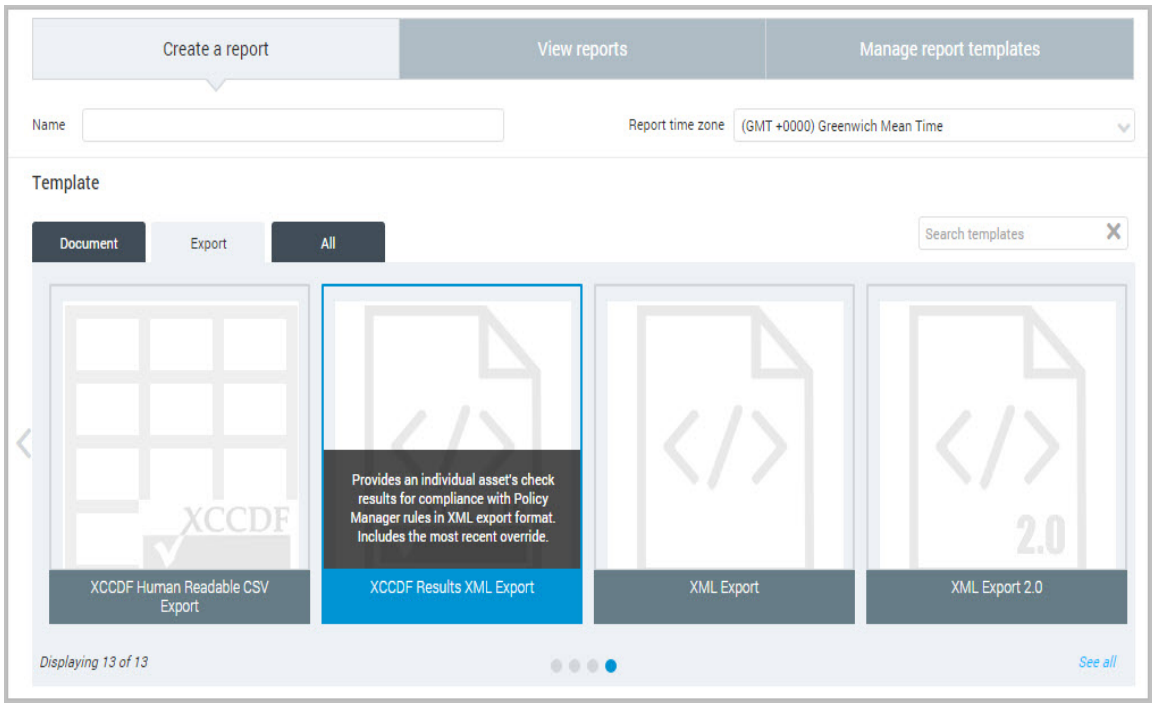
You must enter information in all three fields.

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 1 *Selecting Policy Manager checks* 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.

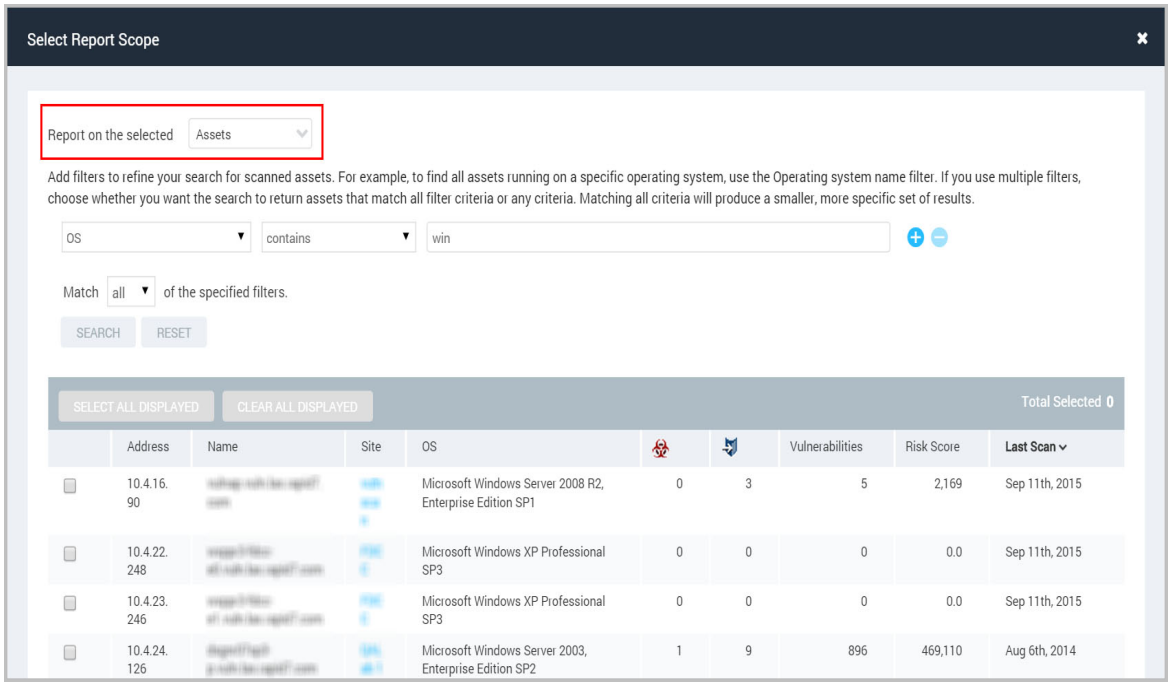
If you selected *Assets*, the Security Console displays search filters. Select a filter, an operator, and then a value.

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 1 *Fine-tuning information with custom report templates*.

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

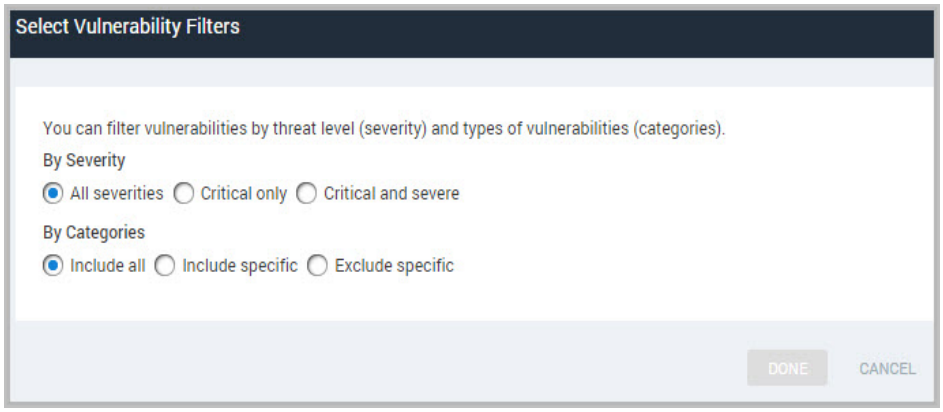
Vulnerability filtering is not supported in the following report templates:

- Cyberscope XML Export
- XCCDF XML
- XCCDF CSV
- Database Export

To filter vulnerability information, take the following steps:

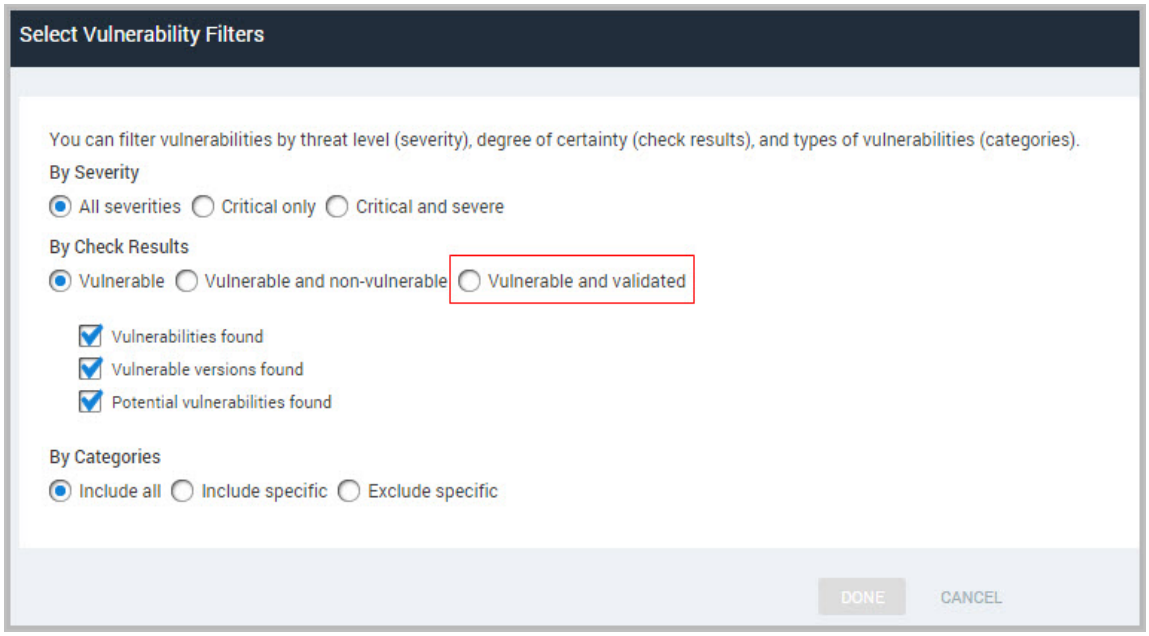
1. Click **Filter report scope based on vulnerabilities** on the *Scope* section of the *Create a report* panel.

   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 1*Working with validated vulnerabilities* .



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:

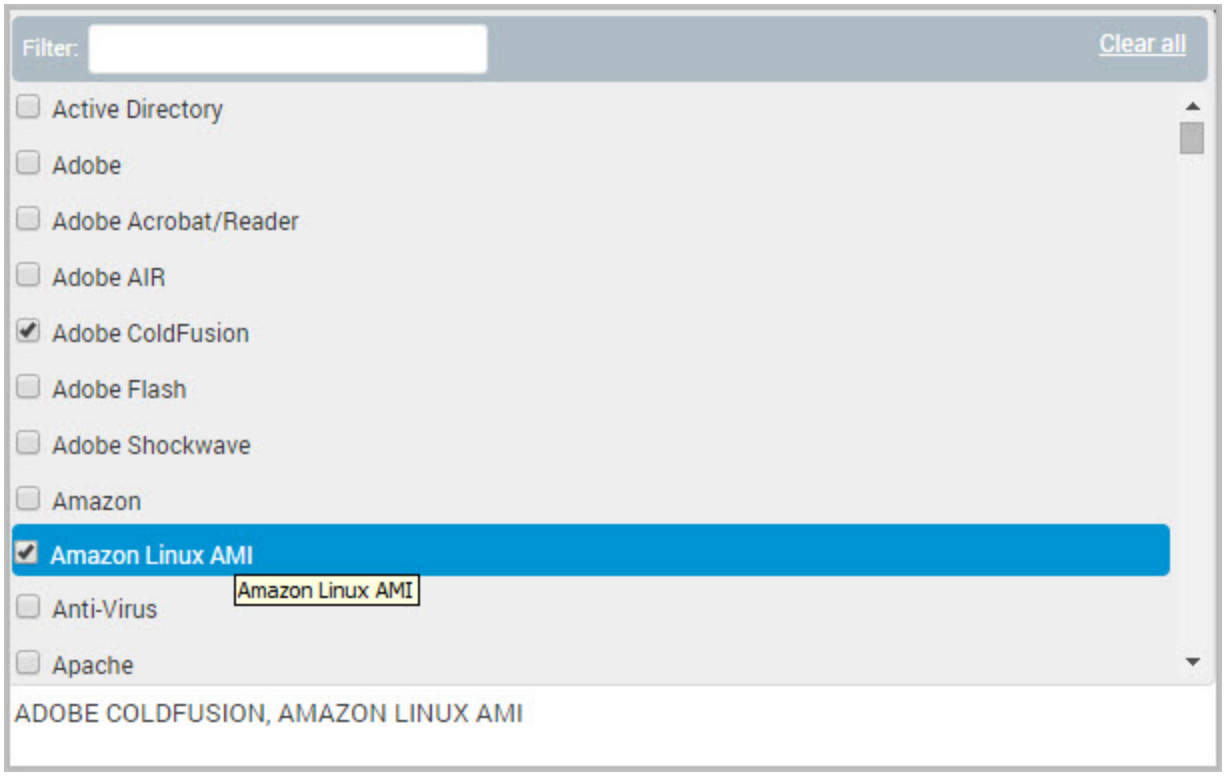
   - **Vulnerabilities found**: Vulnerabilities were flagged because asset-specific vulnerability tests produced positive results. Vulnerabilities with this result type appear with the ve (vulnerable exploited) result code in CSV reports.
   - **Vulnerabilities found**: Vulnerabilities were flagged because 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.

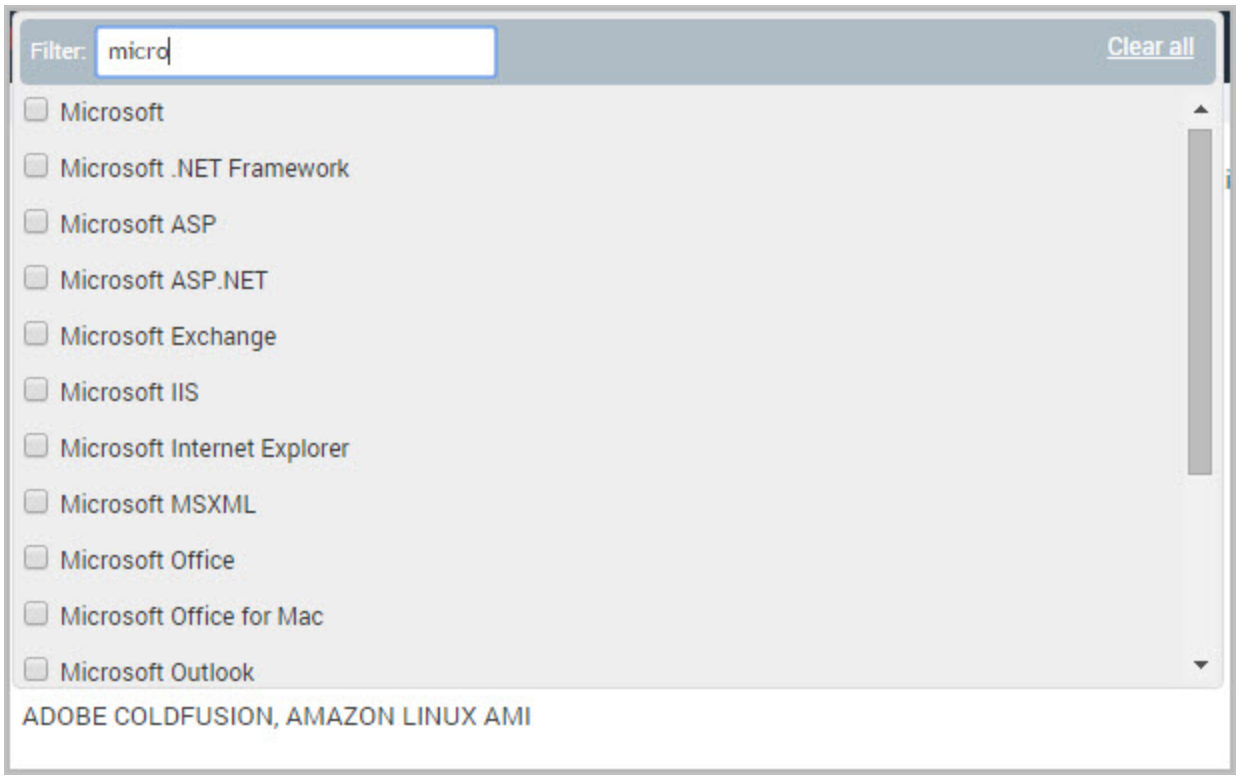
   Tip: Categories that are named for manufacturers, such as Microsoft, can serve as supersets of categories that are named for their products. For example, if you filter by the Microsoft category, you inherently include all Microsoft product categories, such as Microsoft Path and Microsoft Windows. This 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 1 *Configuration steps for vulnerability check settings*.

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.



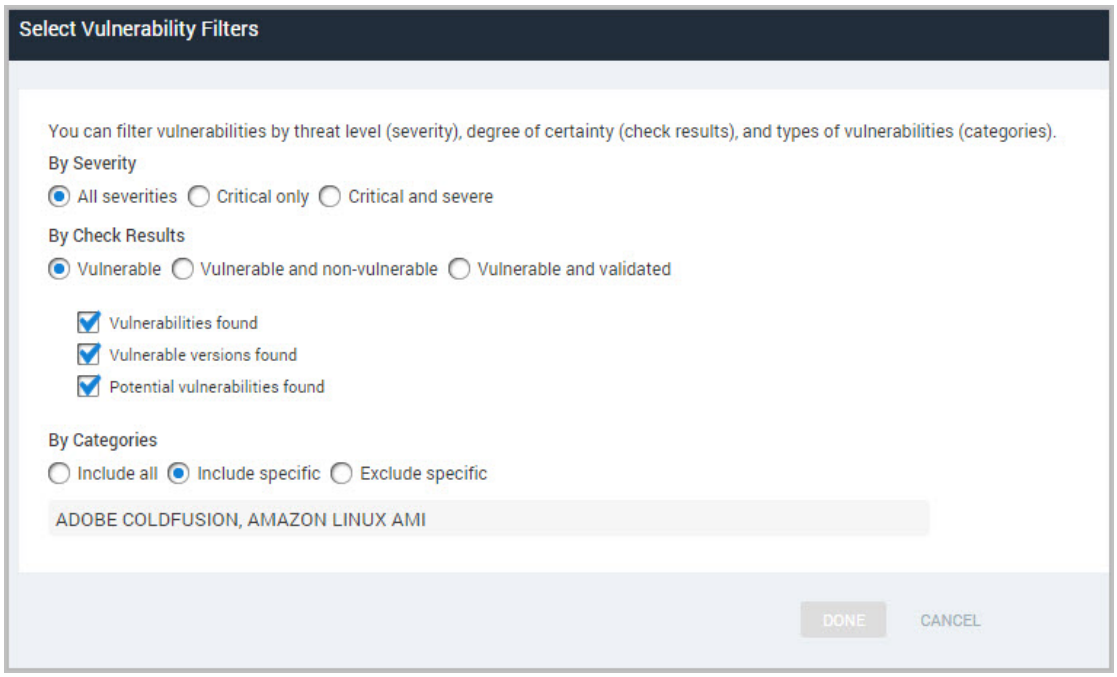
Selecting vulnerability categories by clicking check boxes

- 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 **Do not run a recurring report** 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.

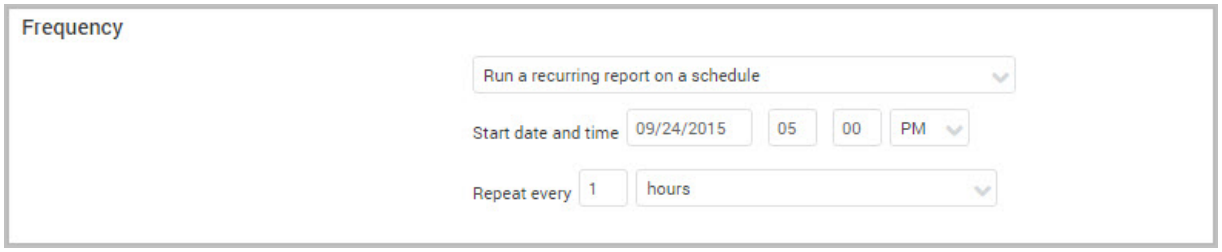
   If you selected the scheduling option, the Security Console displays controls for configuring a schedule.
5. Enter a start date using the mm/dd/yyyy format.

   OR

   Select the date from the calendar widget.
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.



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.

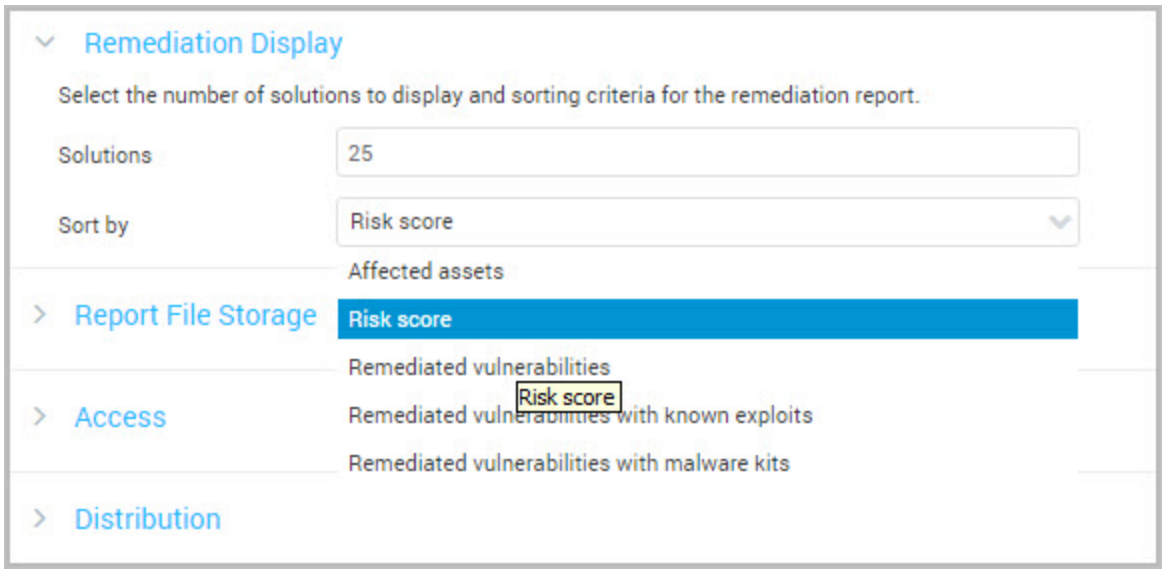
The amount of time required to generate a report depends on the number of included live IP addresses the number of included vulnerabilities—if vulnerabilities are being included—and the level of details in the report template. Generating a PDF report for 100-plus hosts with 2500-plus vulnerabilities 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

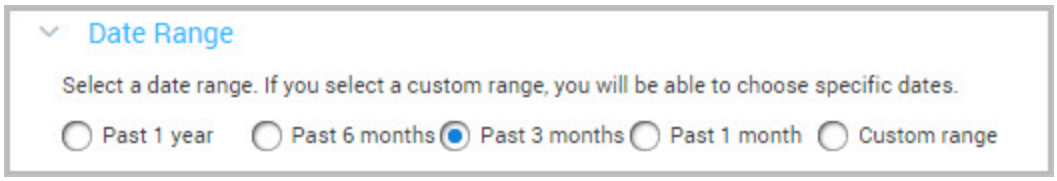
The Vulnerability Trends template provides information about how vulnerabilities in your environment have changed have changed over time. You can configure the time range for the report to see if you are improving your security posture and where you can make improvements. To ensure readability of the 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 date range

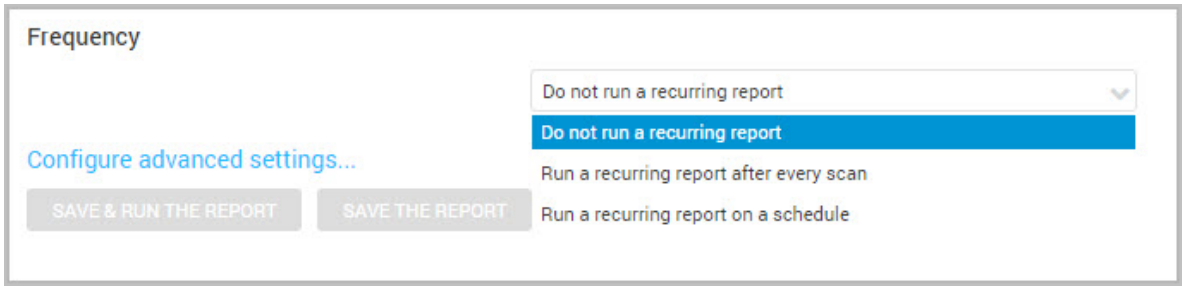
4. Configure other settings that you require for the report.
5. Click **Save & run the report** or **Save the report**, depending on what you want to do.

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 144 *Configuring report frequency*), 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 1 *Viewing, editing, and running reports*.

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 1 *Viewing, editing, and running reports*.



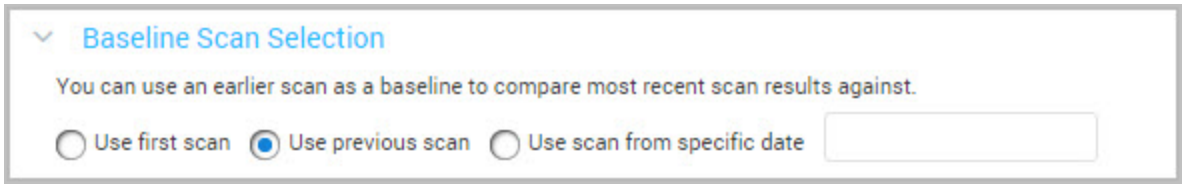
Saving or saving and running a one-time report

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 129*Starting a new report configuration* .

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.

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.

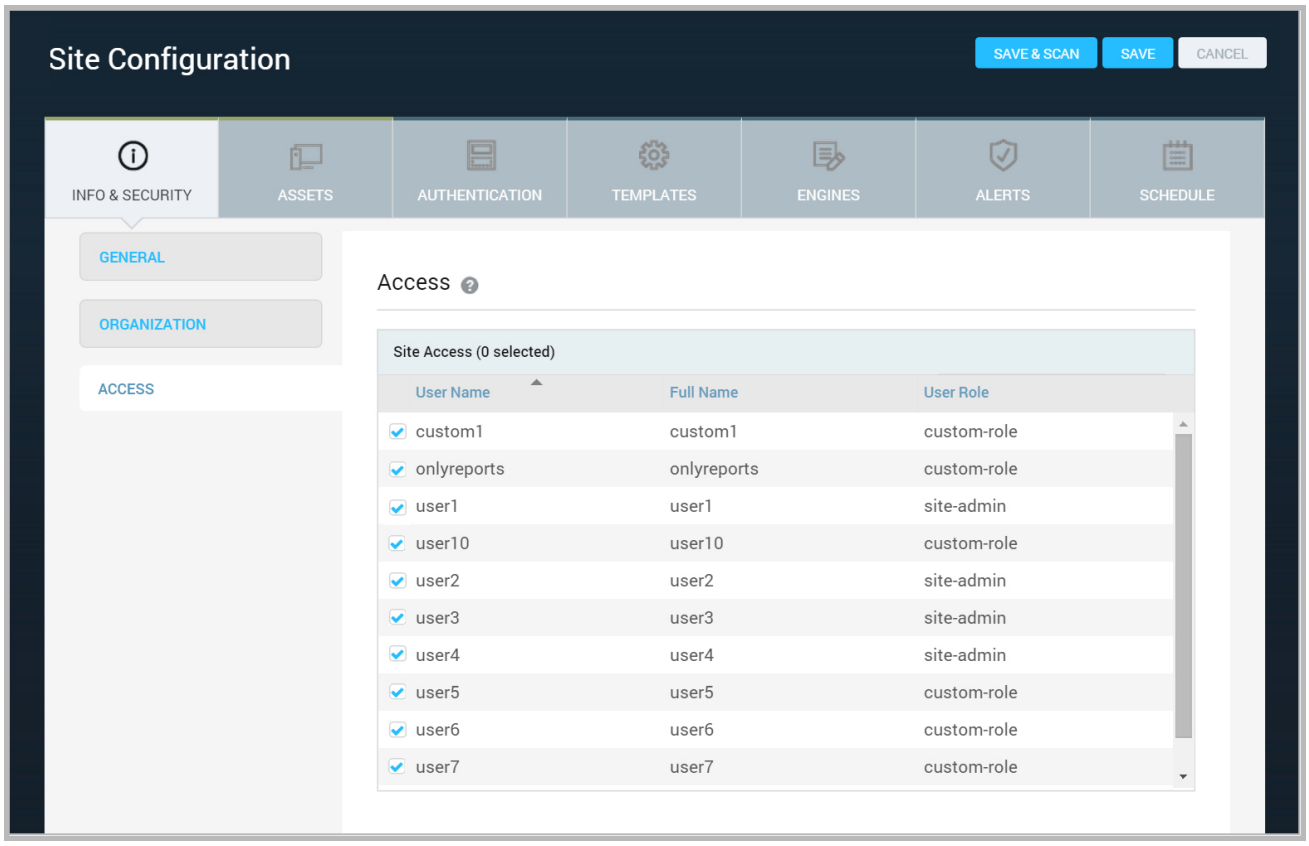
When Global Administrator creates a user account, he or she can grant the user access to all sites, or restrict access by adding the user to access lists for specific sites. See the topic *Configure general user account attributes* in the administrator's guide *Configure general user account attributes*.

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

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 152 *Working with report owners*
- *Managing the sharing of reports* on page 154 *Managing the sharing of reports*
- *Granting users the report-sharing permission* on page 156 *Granting users the report-sharing permission*
- *Restricting report sections* on page 161 *Restricting report sections*
- *Exporting scan data to external databases* on page 163 *Exporting scan data to external databases*
- *Configuring data warehousing settings* on page 164 *Configuring data warehousing settings*

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 152 *Storing reports in report owner directories*.

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 154 *Managing the sharing of reports*.

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

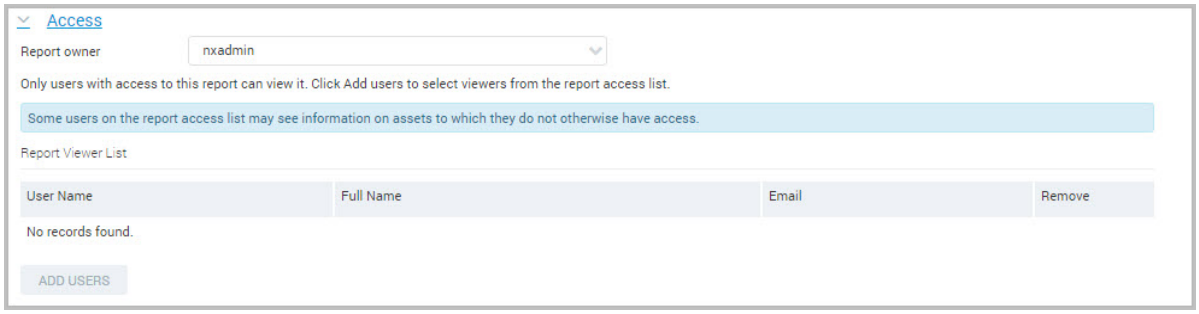
If you are a Global Administrator, or if you have been granted permission to share reports, you can create an access list of users when configuring a report. These users will only be able to view the report. They will not be able to edit or copy it.

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.

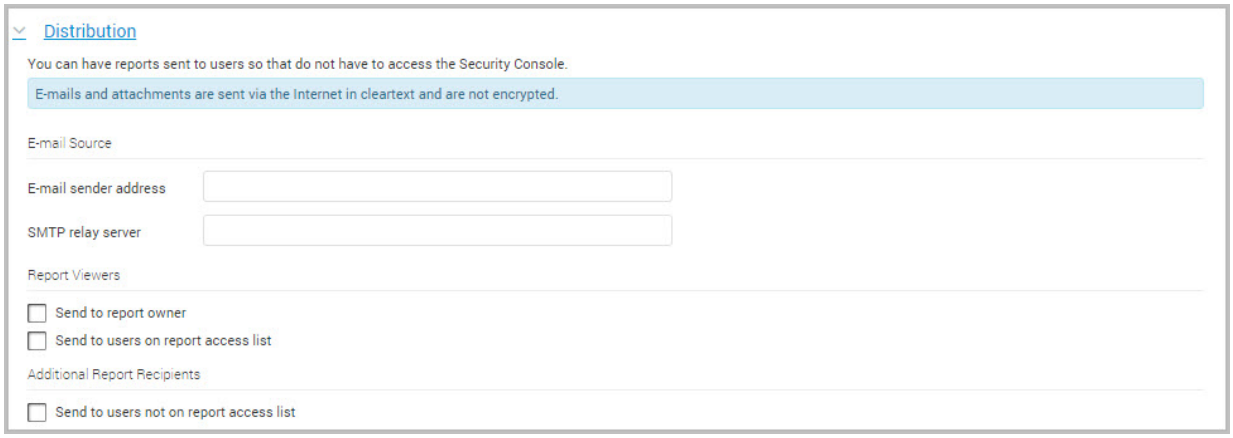
Using the Web-based interface to configure report-sharing settings

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**.

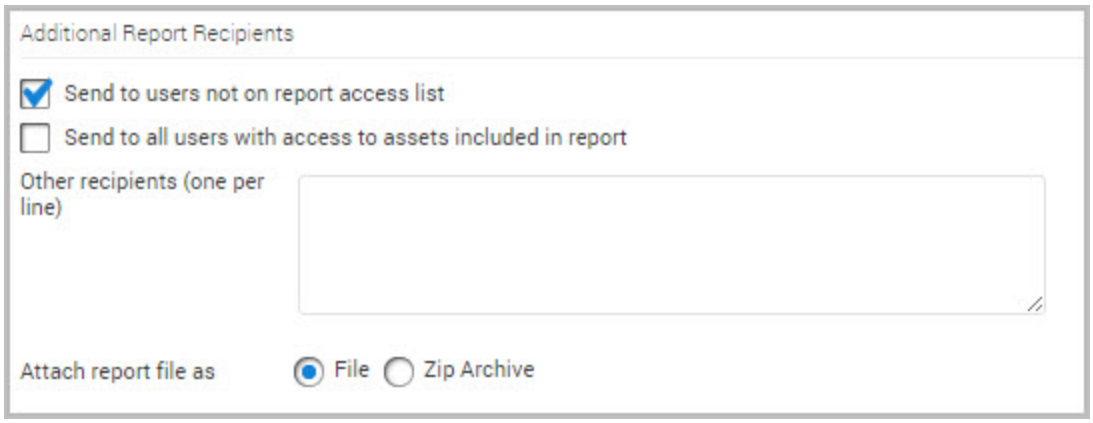


Report Distribution

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 Security Console.

   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.**

Managing users and authentication

Effective use of scan information depends on how your organization analyzes and distributes it, who gets to see it, and for what reason. Managing access to information in the application involves creating asset groups and assigning roles and permissions to users. This chapter provides best practices and instructions for managing users, roles, and permissions.

Mapping roles to your organization

It is helpful to study how roles and permissions map to your organizational structure.

Note: A user authentication system is included. However, if your organization already uses an authentication service that incorporates Microsoft Active Directory or Kerberos, it is a best practice to integrate the application with this service. Using one service prevents having to manage two sets of user information.

In a smaller company, one person may handle all security tasks. He or she will be a Global Administrator, initiating scans, reviewing reports, and performing remediation. Or there may be a small team of people sharing access privileges for the entire system. In either of these cases, it is unnecessary to create multiple roles, because all network assets can be included in one site, requiring a single Scan Engine.

Example, Inc. is a larger company. It has a wider, more complex network, spanning multiple physical locations and IP address segments. Each segment has its own dedicated support team managing security for that segment alone.

One or two global administrators are in charge of creating user accounts, maintaining the system, and generating high-level, executive reports on all company assets. They create sites for different segments of the network. They assign security managers, site administrators, and system administrators to run scans and distribute reports for these sites.

The Global Administrators also create various asset groups. Some will be focused on small subsets of assets. Non-administrative users in these groups will be in charge of remediating vulnerabilities and then generating reports after follow-up scans are run to verify that remediation was successful. Other asset groups will be more global, but less granular, in scope. The non-administrative users in these groups will be senior managers who view the executive reports to track progress in the company's vulnerability management program.

Configuring roles and permissions

Whether you create a custom role or assign a preset role for an account depends on several questions: What tasks do you want that account holder to perform? What data should be visible to the user? What data should not be visible to the user.

For example, a manager of a security team that supports workstations may need to run scans on occasion and then distribute reports to team members to track critical vulnerabilities and prioritizing remediation tasks. This account may be a good candidate for an Asset Owner role with access to a site that only includes workstations and not other assets, such as database servers.

Note: Keep in mind that, except for the Global Administrator role, the assigning of a custom or preset role is interdependent with access to site and asset groups.

If you want to assign roles with very specific sets of permissions you can create custom roles. The following tables list and describe all permissions that are available. Some permissions require other permissions to be granted in order to be useful. For example, in order to be able to create reports, a user must also be able to view asset data in the reported-on site or asset group, to which the user must also be granted access.

The tables also indicate which roles include each permission. You may find that certain roles are granular or inclusive enough for a given account. A list of preset roles and the permissions they include follows the permissions tables. See *Give a user access to asset groups* on page 176 *Give a user access to asset groups*.

Permissions tables

Global permissions

These permissions automatically apply to all sites and asset groups and do not require additional, specified access.

Permission	Description	Role
Manage Sites	Create, delete, and configure all attributes of sites, except for user access. Implicitly have access to all sites. Manage shared scan credentials. **Other affected permissions:** When you select this permission, all site permissions automatically become selected. See Site permissions.	*Global Administrator*
Manage Scan Templates	Create, delete, and configure all attributes of scan templates.	*Global Administrator*
Manage Report Templates	Create, delete, and configure all attributes of report templates.	*Global Administrator*, *Security Manager and Site Owner*, *Asset Owner*, *User*
Manage Scan Engines	Create, delete, and configure all attributes of Scan Engines; pair Scan Engines with the Security Console.	*Global Administrator*
Manage Policies	Copy existing policies; edit and delete custom policies.	*Global Administrator*
Appear on Ticket and Report Lists	Appear on user lists in order to be assigned remediation tickets and view reports. **Prerequisite:** A user with this permission must also have asset viewing permission in any relevant site or asset group: View Site Asset Data; View Group Asset Data	*Global Administrator*, *Security Manager and Site Owner*, *Asset Owner*, *User*
Configure Global Settings	Configure settings that are applied throughout the entire environment, such as risk scoring and exclusion of assets from all scans.	*Global Administrator*
Manage Tags	Create tags and configure their attributes. Delete tags except for built-in criticality tags. Implicitly have access to all sites.	*Global Administrator*

Site permissions

These permissions only apply to sites to which a user has been granted access.

Permission	Description	Role
View Site Asset Data	View discovered information about all assets in accessible sites, including IP addresses, installed software, and vulnerabilities.	*Global Administrator*, *Security Manager and Site Owner*, *Asset Owner*, *User*
Specify Site Metadata	Enter site descriptions, importance ratings, and organization data.	*Global Administrator*, *Security Manager and Site Owner*
Specify Scan Targets	Add or remove IP addresses, address ranges, and host names for site scans.	*Global Administrator*
Assign Scan Engine	Assign a Scan Engine to sites.	*Global Administrator*
Assign Scan Template	Assign a scan template to sites.	*Global Administrator*, *Security Manager and Site Owner*
Manage Scan Alerts	Create, delete, and configure all attributes of alerts to notify users about scan-related events.	*Global Administrator*, *Security Manager and Site Owner*
Manage Site Credentials	Provide logon credentials for deeper scanning capability on password-protected assets.	*Global Administrator*, *Security Manager and Site Owner*
Schedule Automatic Scans	Create and edit site scan schedules.	*Global Administrator*, *Security Manager and Site Owner*
Start Unscheduled Scans	Manually start one-off scans of accessible sites (does not include ability to configure scan settings).	*Global Administrator*, *Security Manager and Site Owner*, *Asset Owner*
Purge Site Asset Data	Manually remove asset data from accessible sites. **Prerequisites:** A user with this permission must also have one of the following permissions: View Site Asset Data; View Group Asset Data	*Global Administrator*
Manage Site Access	Grant and remove user access to sites.	*Global Administrator*

Asset Group permissions

These permissions only apply to asset groups to which a user has been granted access.

Permission	Description	Role
Manage Dynamic Asset Groups	Create dynamic asset groups. Delete and configure all attributes of accessible dynamic asset groups except for user access. **Implicitly have access to all sites**. **Note:** A user with this permission has the ability to view all asset data in your organization.	*Global Administrator*
Manage Static Asset Groups	Create static asset groups. Delete and configure all attributes of accessible static asset groups except for user access. **Prerequisite:** A user with this permission must also have the following permissions and access to at least one site to effectively manage static asset groups: *Manage Group Assets*; *View Group Asset Data*	*Global Administrator*
View Group Asset Data	View discovered information about all assets in accessible asset groups, including IP addresses, installed software, and vulnerabilities.	*Global Administrator*, *Security Manager and Site Owner*, *Asset Owner*, *User*
Manage Group Assets	Add and remove assets in static asset groups. **Note:** This permission does not include ability to delete underlying asset definitions or discovered asset data. **Prerequisite**: A user with this permission must also have of the following permission: View Group Asset Data	*Global Administrator*
Manage Asset Group Access	Grant and remove user access to asset groups.	*Global Administrator*

Report permissions

The Create Reports permission only applies to assets to which a user has been granted access. Other report permissions are not subject to any kind of access.

Permission	Description	Role
Create Reports	Create and own reports for accessible assets; configure all attributes of owned reports, except for user access. **Prerequisites:** A user with this permission must also have one of the following permissions: View Site Asset Data; View Group Asset Data	*Global Administrator*, *Security Manager and Site Owner*, *Asset Owner*, *User*
Use Restricted Report Sections	Create report templates with restricted sections; configure reports to use templates with restricted sections. **Prerequisites:** A user with this permission must also have one of the following permissions: Manage Report Templates	*Global Administrator*
Manage Report Access	Grant and remove user access to owned reports.	*Global Administrator*

Ticket permissions

These permissions only apply to assets to which a user has been granted access.

Permission	Description	Role
Create Tickets	Create tickets for vulnerability remediation tasks. **Prerequisites:** A user with this permission must also have one of the following permissions: View Site Asset Data; View Group Asset Data	*Global Administrator*, *Security Manager and Site Owner*, *Asset Owner*, *User*
Close Tickets	Close or delete tickets for vulnerability remediation tasks. **Prerequisites:** A user with this permission must also have one of the following permissions:View Site Asset Data; View Group Asset Data	*Global Administrator*, *Security Manager and Site Owner*, *Asset Owner*, *User*

Vulnerability exception permissions

These permissions only apply to sites or asset groups to which a user has been granted access.

Permission	Description	Role
Submit Vulnerability Exceptions	Submit requests to exclude vulnerabilities from reports. **Prerequisites:** A user with this permission must also have one of the following permissions: View Site Asset Data; View Group Asset Data	*Global Administrator* , *Security Manager and Site Owner*, *Asset Owner*, *User*
Review Vulnerability Exceptions	Approve or reject requests to exclude vulnerabilities from reports. **Prerequisites:** A user with this permission must also have one of the following permissions: View Site Asset Data; View Group Asset Data	*Global Administrator*
Delete Vulnerability Exceptions	Delete vulnerability exceptions and exception requests. **Prerequisites:** A user with this permission must also have one of the following permissions: View Site Asset Data; View Group Asset Data	*Global Administrator*

List of roles

Global Administrator

The Global Administrator role differs from all other preset roles in several ways. It is not subject to site or asset group access. It includes all permissions available to any other preset or custom role. It also includes permissions that are not available to custom roles:

- Manage all functions related to user accounts, roles, and permissions.
- Manage vConnections and vAsset discovery.
- Manage configuration, maintenance, and diagnostic routines for the Security Console.
- Manage shared scan credentials.

Security Manager and Site Owner

The Security Manager and Site Owner roles include the following permissions:

- *Manage Report Templates*
- *Appear on Ticket and Report Lists*
- *View Site Asset Data*
- *Specify Site Metadata*
- *Assign Scan Template*
- *Manage Scan Alerts*
- *Manage Site Credentials*
- *Schedule Automatic Scans*
- *Start Unscheduled Scans*
- *View Group Asset Data* (Security Manager only)
- *Create Reports*
- *Create Tickets*

The only distinction between these two roles is the Security Manager's ability to work in accessible sites *and* assets groups. The Site Owner role, on the other hand, is confined to sites.

Asset Owner

The Asset Owner role includes the following permissions in accessible sites and asset groups:

- *Manage Report Templates*
- *Appear on Ticket and Report Lists*
- *View Site Asset Data*
- *Start Unscheduled Scans*
- *View Group Asset Data*
- *Create Reports*

User

Although “user” can refer generically to any owner of aNexposeSymantec CCS Vulnerability Manager account, the name *User*, with an upper-case *U,* refers to one of the preset roles. It is the only role that does not include scanning permissions. It includes the following permissions in accessible sites and asset groups:

- *Manage Report Templates*
- *Manage Policies*
- *View Site Asset Data*
- *View Group Asset Data* (Security Manager only)
- *Create Reports*
- *Create Tickets*

ControlsInsight User

This role provides complete access to ControlsInsight with no access to Nexpose.

Managing and creating user accounts

The **Users** links on the *Administration* page provide access to pages for creating and managing user accounts. Click **manage** next to *Users* to view the *Users* page. On this page, you can view a list of all accounts within your organization. The last logon date and time is displayed for each account, giving you the ability to monitor usage and delete accounts that are no longer in use.

To edit a user account:

1. Click **Edit** for any listed account, and change its attributes.

   The application displays the *User Configuration* panel. The process for editing an account is the same as the process for creating a new user account. See *Configure general user account attributes* on page 174 *Configure general user account attributes*.

To delete an account and reassign tickets or reports:

1. Click **Delete** for the account you want to remove.

   A dialog box appears asking you to confirm that you want to delete the account.

2. Click **Yes** to delete the account.

   If that account has been used to create a report, or if that account has been assigned a ticket, the application displays a dialog box prompting you to reassign or delete the report or ticket in question. You can choose delete a report or a ticket that concerns a closed issue or an old report that contains out-of-date information.

3. Select an account from the drop-down list to reassign tickets and reports to.
4. (*Optional*) Click **Delete tickets and reports** to remove these items from the database.
5. Click **OK** to complete the reassignment or deletion.

Configure general user account attributes

You can specify attributes for general user accounts on the *User Configuration* panel.

To configure user account attributes:

1. Click **New User** on the *Users* page.
2. (*Optional*) Click **Create** next to *Users* on the *Administration* page. The Security Console displays the *General* page of the *User Configuration* panel.
3. Enter all requested user information in the text fields.
4. (*Optional*) Select the appropriate source from the drop-down list to authenticate the user with external sources.

   Before you can create externally authenticated user accounts you must define external authentication sources. See *Using external sources for user authentication* on page 176 *Using external sources for user authentication*.

5. Check the **Account enabled** check box.

   You can later disable the account without deleting it by clicking the check box again to remove the check mark.

6. Click **Save** to save the new user information.

Assign a role and permissions to a user

Assigning a role and permissions to a new user allows you to control that user's access to Security Console functions.

To assign a role and permissions to a new user:

1. Go to the *Roles* page.
2. Choose a role from the drop-down list.

   When you select a role, the Security Console displays a brief description of that role.

   If you choose one of the five default roles, the Security Console automatically selects the appropriate check boxes for that role.

   If you choose **Custom Role**, select the check box for each permission that you wish to grant the user.
3. Click **Save** to save the new user information.

Give a user access to specific sites

A Global Administrator automatically has access to all sites. A security manager, site administrator, system administrator, or nonadministrative user has access only to those sites granted by a global administrator.

To grant a user access to specific sites:

1. Go to the *Site Access* page.
2. (*Optional*) Click the appropriate radio button to give the user access to all sites.
3. (*Optional*) Click the radio button for creating a custom list of accessible sites to give the user access to specific sites.
4. Click **Add Sites**.
5. The Security Console displays a box listing all sites within your organization.
6. Click the check box for each site that you want the user to access.
7. Click **Save**.

   The new site appears on the *Site Access* page.
8. Click **Save** to save the new user information.

Give a user access to asset groups

A global administrator automatically has access to all asset groups. A site administrator user has no access to asset groups. A security manager, system administrator, or nonadministrative user has access only to those access groups granted by a global administrator.

To grant a user access to asset group:

1. Go to the *Asset Group Access* page.
2. (*Optional*) Click the appropriate radio button to give the user access to all asset groups.
3. (*Optional*) Click the radio button for creating a custom list of accessible asset groups to give the user access to specific asset groups.
4. Click **Add Groups**.

   The Security Console displays a box listing all asset groups within your organization.
5. Click the check box for each asset group that you want this user to access.
6. Click **Save**.

   The new asset group appears on the *Asset Group Access* page.
7. Click **Save** to save the new user information.

Using external sources for user authentication

You can integrate NexposeSymantec CCS Vulnerability Manager with external authentication sources. If you use one of these sources, leveraging your existing infrastructure will make it easier for you to manage user accounts.

The application provides single-sign-on external authentication with two sources:

- **LDAP (including Microsoft Active Directory):** Active Directory (AD) is an LDAP-supportive Microsoft technology that automates centralized, secure management of an entire network's users, services, and resources.
- **Kerberos:** Kerberos is a secure authentication method that validates user credentials with encrypted keys and provides access to network services through a “ticket” system.

The application also continues to support its two internal user account stores:

- XML file lists default “built-in” accounts. A Global Administrator can use a built-in account to log on to the application in maintenance mode to troubleshoot and restart the system when database failure or other issues prevent access for other users.
- Datastore lists standard user accounts, which are created by a global administrator.

Before you can create externally authenticated user accounts you must define external authentication sources.

To define external authentication sources:

1. Go to the *Authentication* page in the *Security Console Configuration* panel.
2. Click **Add...** in the area labelled *LDAP/AD authentication sources* to add an LDAP/Active Directory authentication source

   The Security Console displays a box labeled *LDAP/AD Configuration*.
3. Click the check box labeled **Enable authentication source**.
4. Enter the name, address or fully qualified domain name, and port of the LDAP server that you wish to use for authentication.

   Note: It is recommended that you enter **a fully qualified domain name in all capital letters** for the LDAP server configuration. Example: SERVER.DOMAIN.EXAMPLE.COM

   Default LDAP port numbers are 389 or 636, the latter being for SSL. Default port numbers for Microsoft AD with Global Catalog are 3268 or 3269, the latter being for SSL.
5. (*Optional*) Select the appropriate check box to require secure connections over SSL.
6. (*Optional*) Specify permitted authentication methods, enter them in the appropriate text field. Separate multiple methods with commas (,), semicolons (;), or spaces.

   Note: It is not recommended that you use PLAIN for non-SSL LDAP connections.

   Simple Authentication and Security Layer (SASL) authentication methods for permitting LDAP user authentication are defined by the Internet Engineering Task Force in document *RFC 2222* (http://www.ietf.org/rfc/rfc2222.txt). The application supports the use of GSSAPI, CRAM-MD5, DIGEST-MD5, SIMPLE, and PLAIN methods.
7. Click the checkbox labeled **Follow LDAP referrals** if desired.

   As the application attempts to authenticate a user, it queries the target LDAP server. The LDAP and AD directories on this server may contain information about other directory servers capable of handling requests for contexts that are not defined in the target directory. If so, the target server will return a referral message to the application, which can then contact these additional LDAP servers. For information on LDAP referrals, see the document *LDAPv3 RFC 2251* (http://www.ietf.org/rfc/rfc2251.txt).
8. Enter the base context for performing an LDAP search if desired. You can initiate LDAP searches at many different levels within the directory.

To force the application to search within a specific part of the tree, specify a search base, such as CN=sales,DC=acme,DC=com.

9. Click one of the three buttons for LDAP attributes mappings, which control how LDAP attribute names equate, or map, to attribute names.

   Your attribute mapping selection will affect which default values appear in the three fields below. For example, the LDAP attribute Login ID maps to the user's login ID. If you select AD mappings, the default value is sAMAccountName. If you select AD Global Catalog mappings, the default value is userPrincipalName. If you select Common LDAP mappings, the default value is uid.

10. Click **Save**.

    The Security Console displays the *Authentication* page with the LDAP/AD authentication source listed.

To add a Kerberos authentication source:

1. Click **Add...** in the area of the Authentication page labeled *Kerberos Authentication sources*.

   The Security Console displays a box labeled *Kerberos Realm Configuration*.

2. Click the checkbox labeled **Enable authentication source**.
3. Click the appropriate checkbox to set the new realm that you are defining as the default Kerberos realm.

   The Security Console displays a warning that the default realm cannot be disabled.

4. Enter the name of the realm in the appropriate text field.
5. Enter the name of the key distribution center in the appropriate field.
6. Select the check box for every encryption type that your authentication source supports. During authentication, the source runs through each type, attempting to decrypt the client's credentials, until it uses a type that is identical to the type used by the client.
7. Click **Save**.

   The Security Console displays the *Authentication* page with the new Kerberos distribution center listed.

   Once you have defined external authentication sources, you can create accounts for users who are authenticated through these sources.

8. Click the **Administration** tab on the *Home* page.
9. Click **Create** next to *Users* on the *Administration* page,

   The Security Console displays the *User Configuration* panel.

On the *General* page, the **Authentication** method drop-down list contains the authentication sources that you defined in the Security Console configuration file.

10. Select an authentication source.

    Note: If you log on to the interface as a user with external authentication, and then click your user name link at the top right corner of any page, the Security Console displays your account information, including your password; however, if you change the password on this page, the application will not implement the change.

    The built-in user store authentication is represented by the NexposeSymantec CCS Vulnerability Manager *user* option.

    The *Active Directory* option indicates the LDAP authentication source that you specified in the Security Console configuration file.

    If you select an external authentication source, the application disables the password fields. It does not support the ability to change the passwords of users authenticated by external sources.

11. Fill in all other fields on the *General* page.
12. Click **Save**.

Manually setting Kerberos encryption types

If you are authenticating users with Kerberos, you can increase security for connections to the Kerberos source, by specifying the types of ticket encryptions that can be used in these connections. To do so, take the following steps:

1. Using a text editor, create a new text file named *kerberos.properties*.
2. Add a line that specifies one or more acceptable encryption types. For multiple types, separate each types with a character space:

```
default_tkt_enctypes=<encryption_type encryption_type>
```

You can specify any of the following ticket encryption types:

- des-cbc-md5
- des-cbc-crc
- des3-cbc-sha1
- rc4-hmac
- arcfour-hmac
- arcfour-hmac-md5
- aes128-cts-hmac-sha1-96
- aes256-cts-hmac-sha1-96

Example:

```
default_tkt_enctypes= aes128-cts-hmac-sha1-96 aes256-cts-hmac-sha1-96
```

3. Save the file in the installation_directory/nsc/conf directory.

   The changes are applied at the next startup.

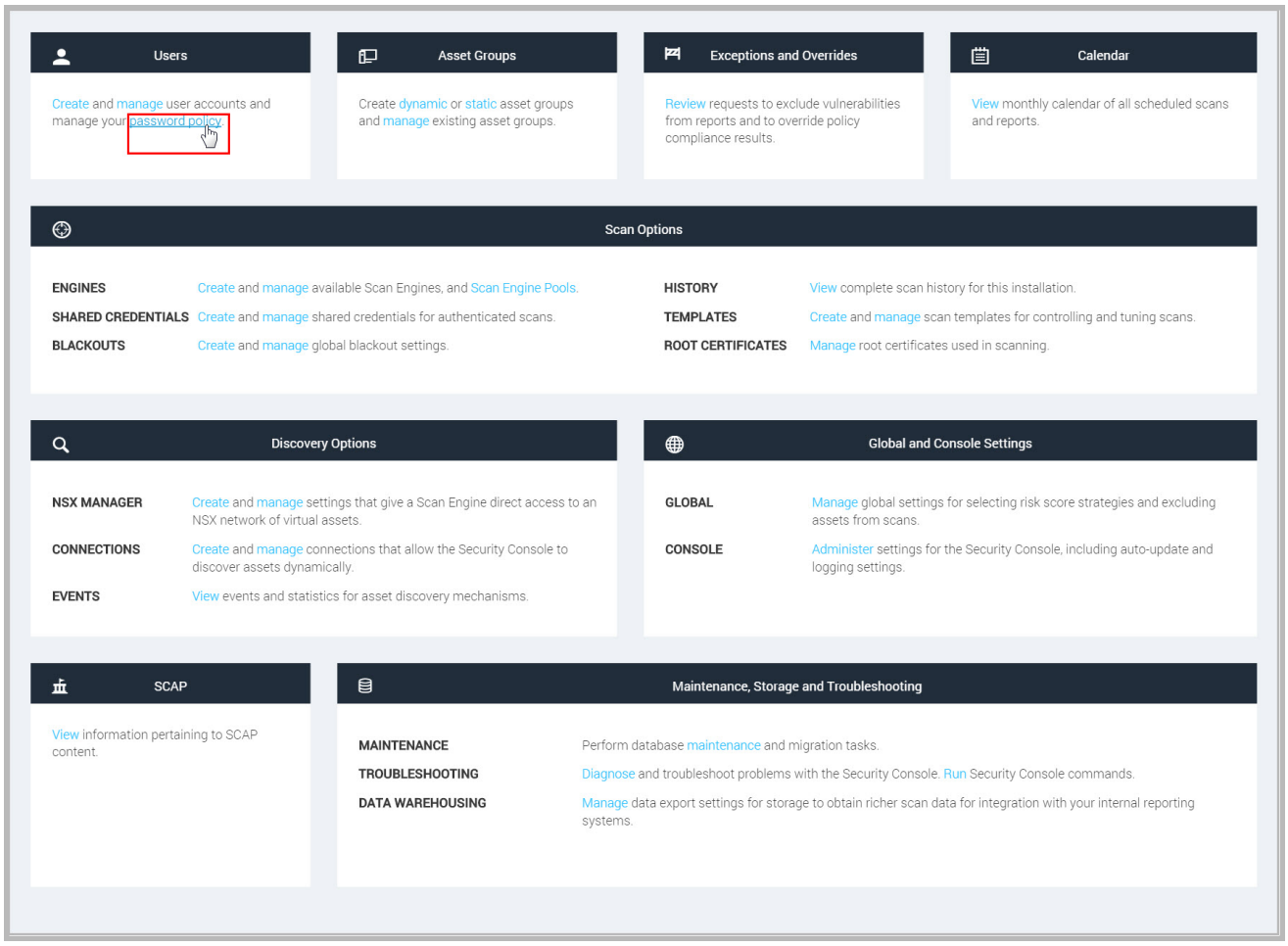
Setting a password policy

Global Administrators can customize the password policy in your NexposeSymantec CCS Vulnerability Manager installation. One reason to do so is to configure it to correspond with your organization's particular password standards.

Note: When you update a password policy, it will take effect for new users and when existing users change their passwords. Existing users will not be forced to change their passwords.

To customize a password policy:

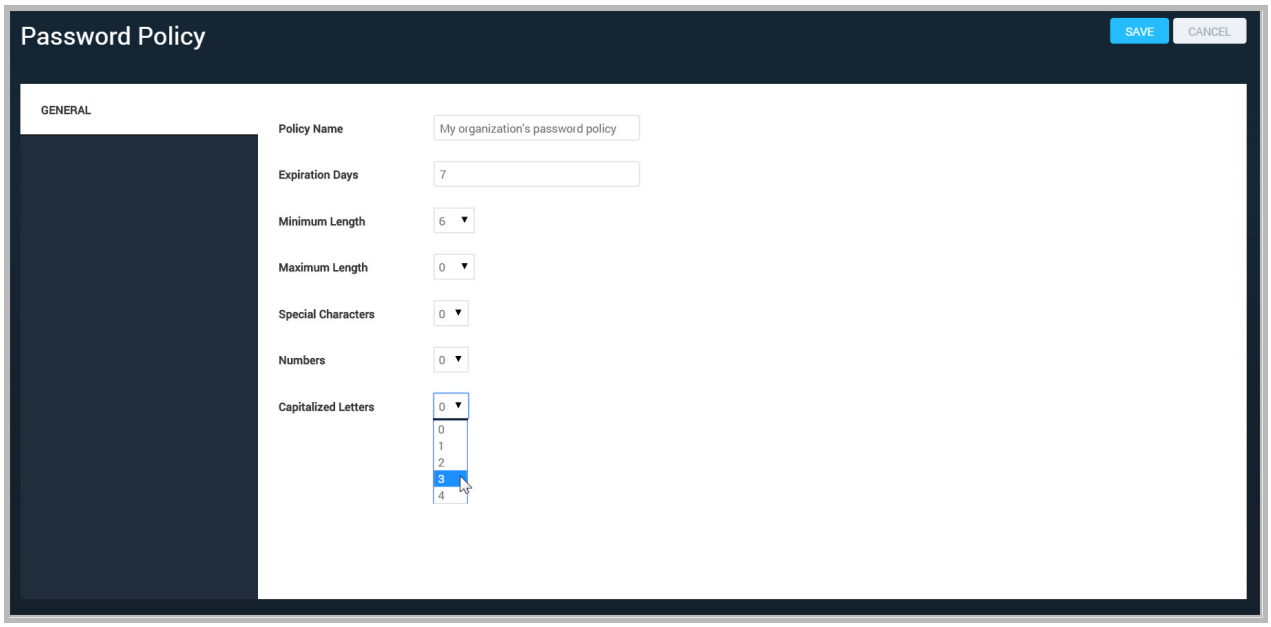
1. In the Security Console, go to the *Administration* page.
2. Select **password policy**.



Navigating to the password policy configuration

3. Change the policy name.
4. Select the desired parameters for the password requirements.

   Note: If you do not want to enforce a maximum length, set the maximum length to 0.

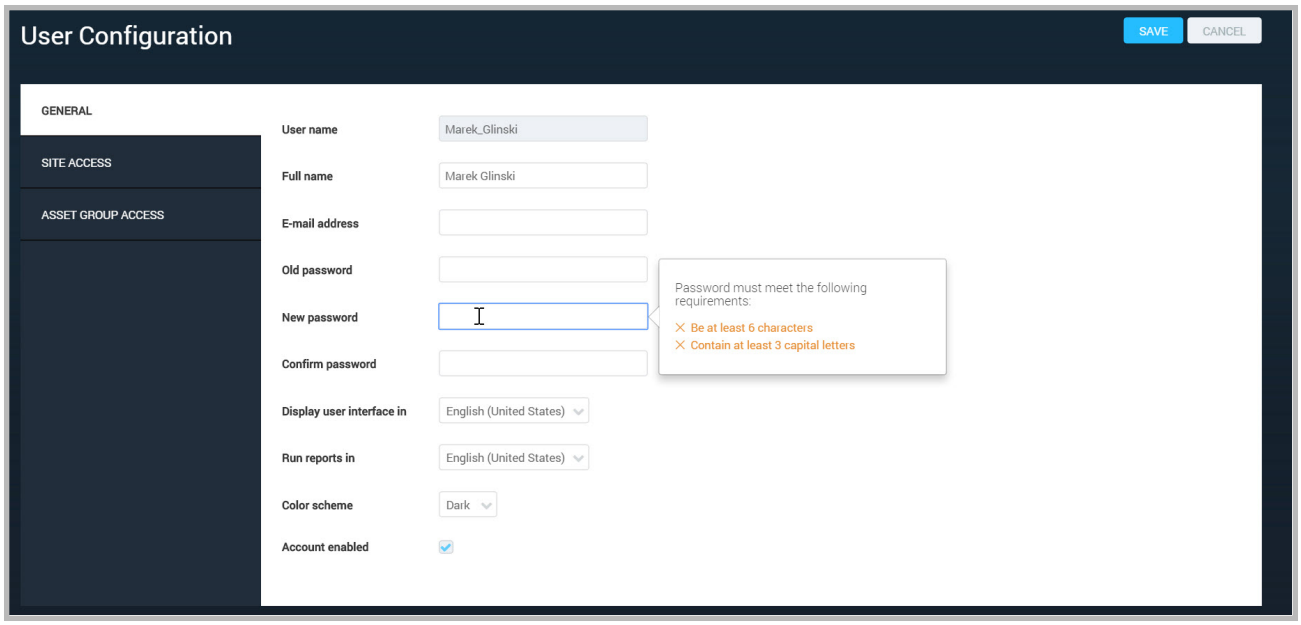


Example: This policy is named Test Policy and enforces a minimum length of 8 characters, maximum length of 24 characters, at least one capital leter, at least one numeric value, and at least one special character.

5. Click **Save**.

Once the password policy is set, it will be enforced on the User Configuration page.

As a new password is typed in, the items on the list of requirements turn from red to green as the password requirements are met.



As a user types a new password, the requirements on the list change from red to green as they are fulfilled.

If a user attempts to save a password that does not meet all the requirements, an error message will appear.

Global settings

Working with risk strategies to analyze threats

One of the biggest challenges to keeping your environment secure is prioritizing remediation of vulnerabilities. If NexposeSymantec CCS Vulnerability Manager 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 190 *Changing your risk strategy and recalculating past scan data*
- *Using custom risk strategies* on page 192 *Using custom risk strategies*
- *Changing the appearance order of risk strategies* on page 194 *Changing the appearance order of risk strategies*

Comparing risk strategies

- *Real Risk strategy* on page 188 *Real Risk strategy*
- *TemporalPlus strategy* on page 188 *TemporalPlus strategy*
- *Temporal strategy* on page 189 *Temporal strategy*
- *Weighted strategy* on page 189 *Weighted strategy*
- *PCI ASV 2.0 Risk strategy* on page 189 *PCI ASV 2.0 Risk strategy*

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 190 *Changing your risk strategy and recalculating past scan data*.

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 1 *Configuring a dynamic site* or *Getting started: Info & Security* on page 1*Getting started: Info & Security*.
- 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** icon 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 NexposeSymantec CCS Vulnerability Manager.

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 NexposeSymantec CCS Vulnerability Manager, 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 192 *Using custom risk strategies* .

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*. NexposeSymantec CCS Vulnerability Manager only calculates risk scores based on data from assets with *completed* scan status.

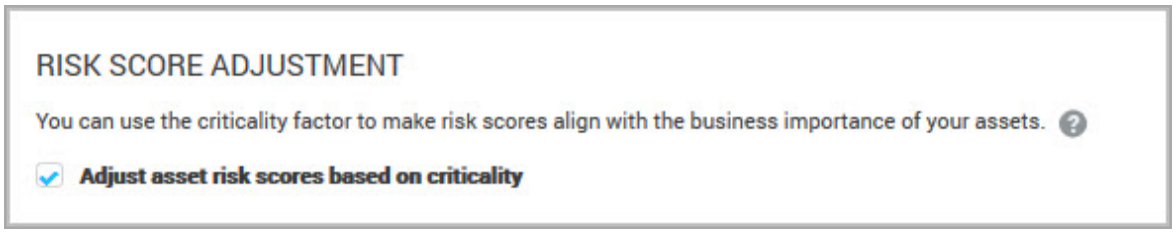
If a scan pauses or stops, The application does not use results from assets that do not have *completed* status for the computation of risk scores. For example: 10 assets are scanned in parallel. Seven have *completed* scan status; three do not. The scan is stopped. Risk is calculated based on the results 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 1*Viewing the scan log* .

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:

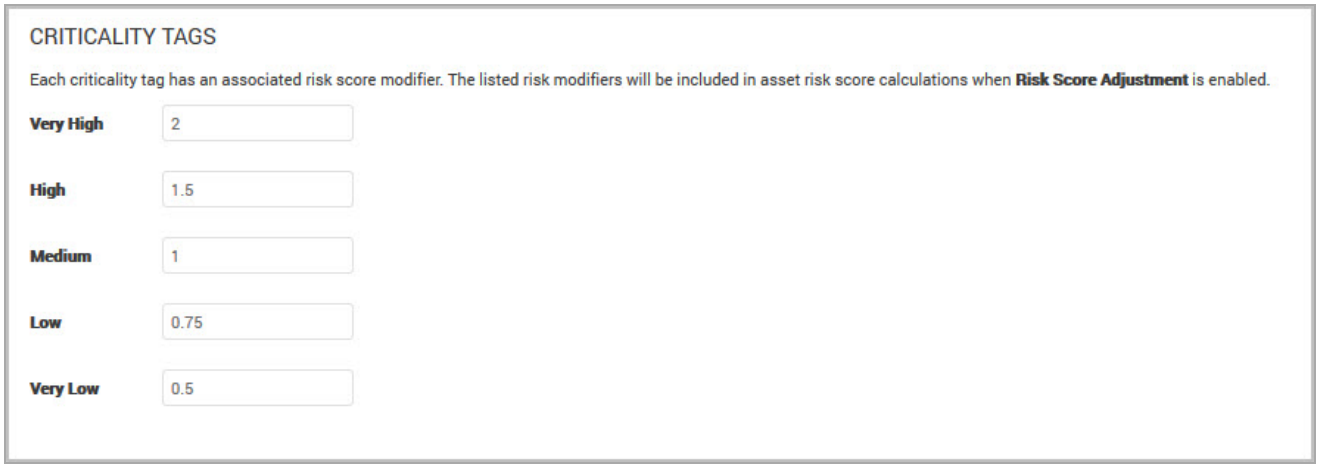
1. On the Administration page, in Global and Console Settings, click the **Manage** link for global settings.
2. In the Global Settings page, select **Risk Score Adjustment**.
3. Select **Adjust asset risk scores based on criticality.**
4. Change any of the modifiers for the listed criticality levels, 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

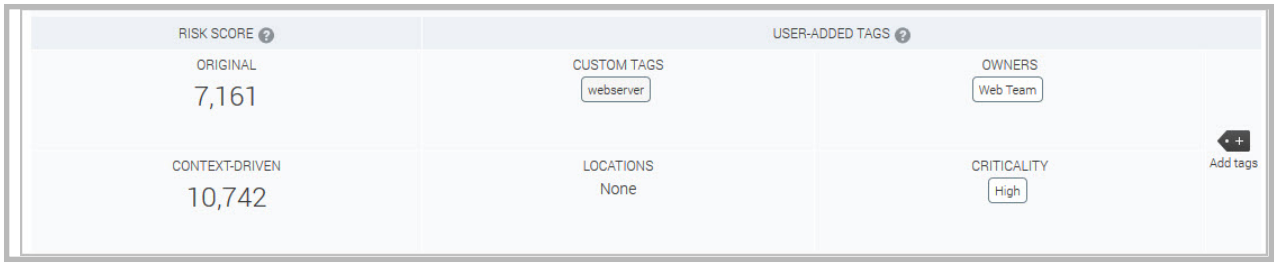


Adjust the multipliers for the criticality levels

Interaction with risk strategy

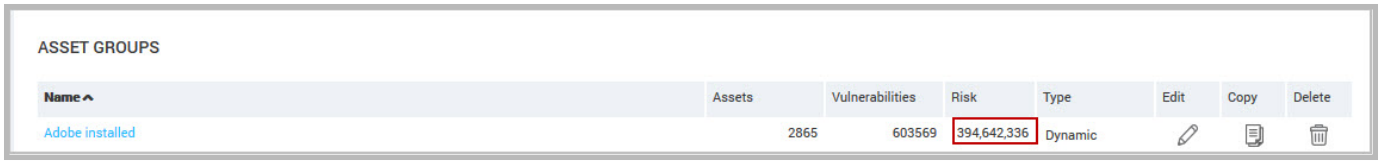
The *Risk Strategy* and Risk Score Adjustment are independent factors that both affect the risk score.

To calculate the risk score for an individual asset, NexposeSymantec CCS Vulnerability Manageruses 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.

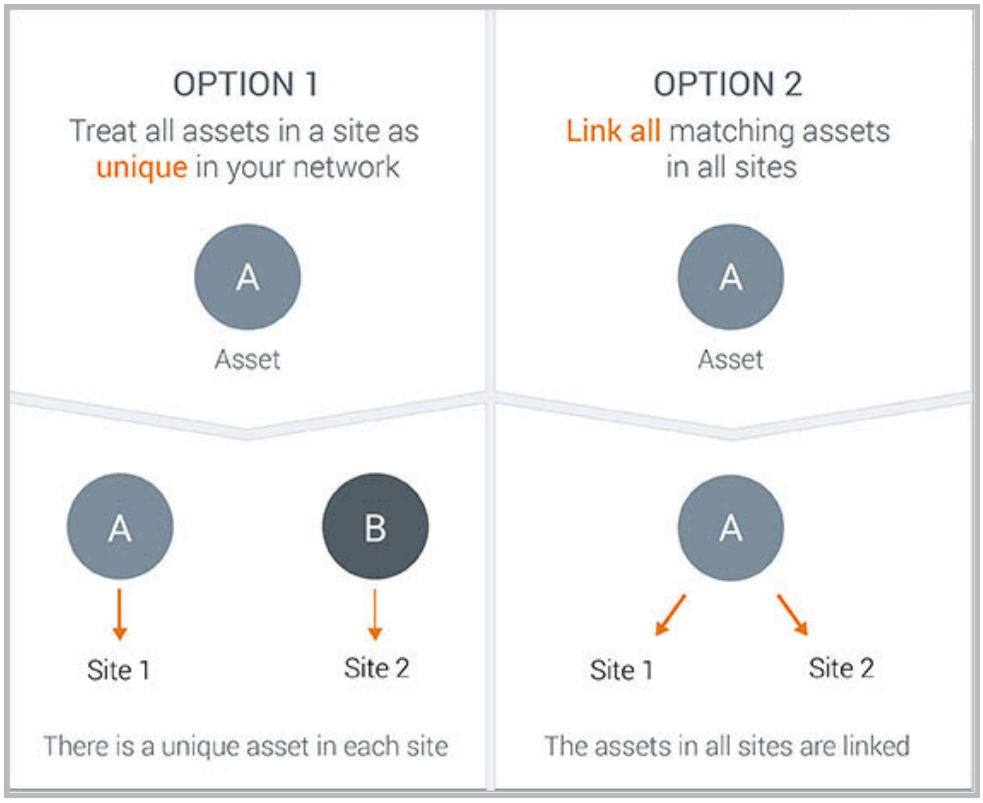
Viewing risk scores

If Risk Score Adjustment is enabled, nearly every risk score you see in your NexposeSymantec CCS Vulnerability Managerinstallation 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.

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 NexposeSymantec CCS Vulnerability Manager, includes the following:

- IP address
- host name
- MAC address
- vulnerabilities
- risk score
- user-applied tags
- site membership
- asset ID (a unique identifier applied by NexposeSymantec CCS Vulnerability Manager when the asset information is integrated into the database)

If the option to link assets across sites is disabled, NexposeSymantec CCS Vulnerability Manager 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, NexposeSymantec CCS Vulnerability Manager 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 NexposeSymantec CCS Vulnerability Manager 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:

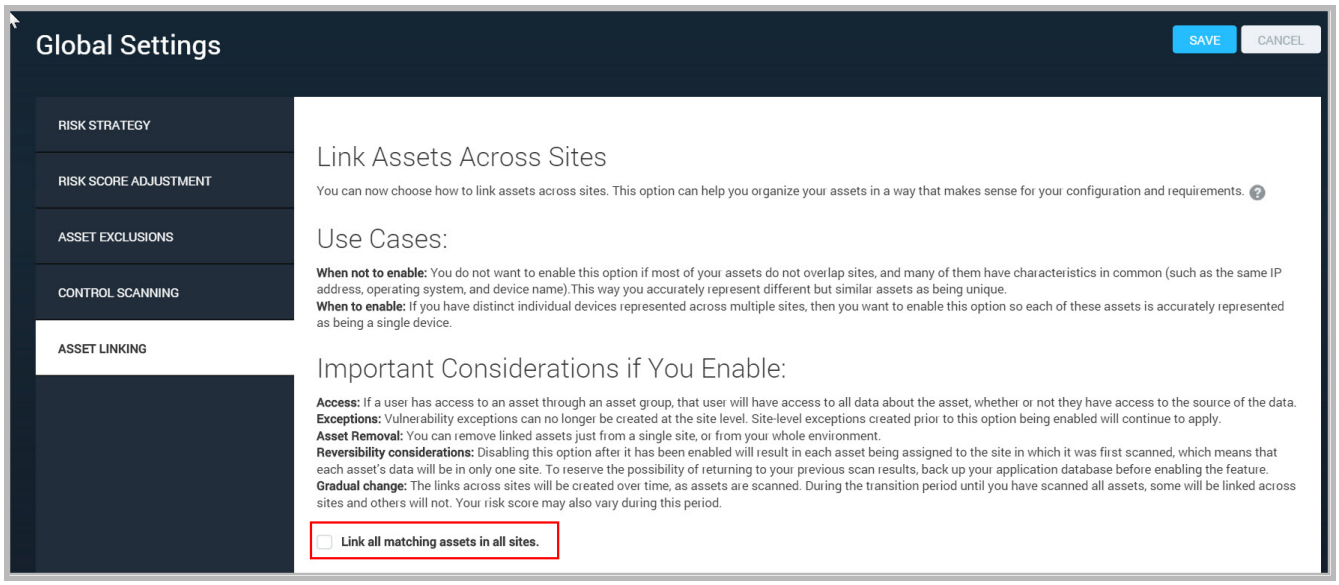
- You will notice that some assets are not updating with scans over time. As you scan, new data for an asset will link with the most recently scanned asset. For example if an asset with IP address 10.0.0.1 is included in both the *Boston* and the *PCI targets* sites, the latest scan data will link with 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*.

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 1 *Shared credentials vs. site-specific credentials*.

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 204 *Naming and describing the new set of shared credentials*
2. *Configuring the account for authentication* on page 205 *Configuring the account for authentication*
3. *Restricting the credentials to a single asset and port* on page 206 *Restricting the credentials to a single asset and port*
4. *Assigning shared credentials to sites* on page 207 *Assigning shared credentials to sites*

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

- *Viewing shared credentials* on page 207 *Viewing shared credentials*
- *Editing shared credentials that were previously created* on page 208 *Editing shared credentials that were previously created*

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 1 *Configuring scan credentials*.

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** icon.

   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** icon.

   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 204 *Naming and describing the new set of shared credentials*
- *Configuring the account for authentication* on page 205 *Configuring the account for authentication*
- *Testing shared scan credentials* on page 205 *Testing shared scan credentials*
- *Restricting the credentials to a single asset and port* on page 206 *Restricting the credentials to a single asset and port*
- *Assigning shared credentials to sites* on page 207 *Assigning shared credentials to sites*

Third Party Integrations

Your deployment includes the following integrations, if you choose to leverage them.

Active Directory Integration

- Allows for pass-through authentication of AD credentials for Nexpose console access.
- Nexpose will require an FQDN for an individual domain controller. Round robin/load balancing is not supported.
- Integration does not facilitate asset discovery.
- Integration does not support AD groups.
- User creation in Nexpose is manual.

vAsset Discovery

- Allows for the passive discovery of assets in a VMware environment.
- Nexpose will require the hostname/IP and read only service credentials to ESXi hosts or vCenter. Credentials must have read-only visibility of asset to be discovered.

DHCP Discovery

- Allows for the identification of new assets when assigned an IP address.
- Support for Microsoft DHCP server and Infoblox Trinzic

AWS Discovery

- Allows for the passive discovery of assets in the AWS Cloud.
- Nexpose will require the creation of an AWS IAM user or role. Please see Identities (Users, Groups, and Roles) and Creating an IAM User in Your AWS Account in the AWS Identity and Access Management User Guide to learn more about IAM users and roles.

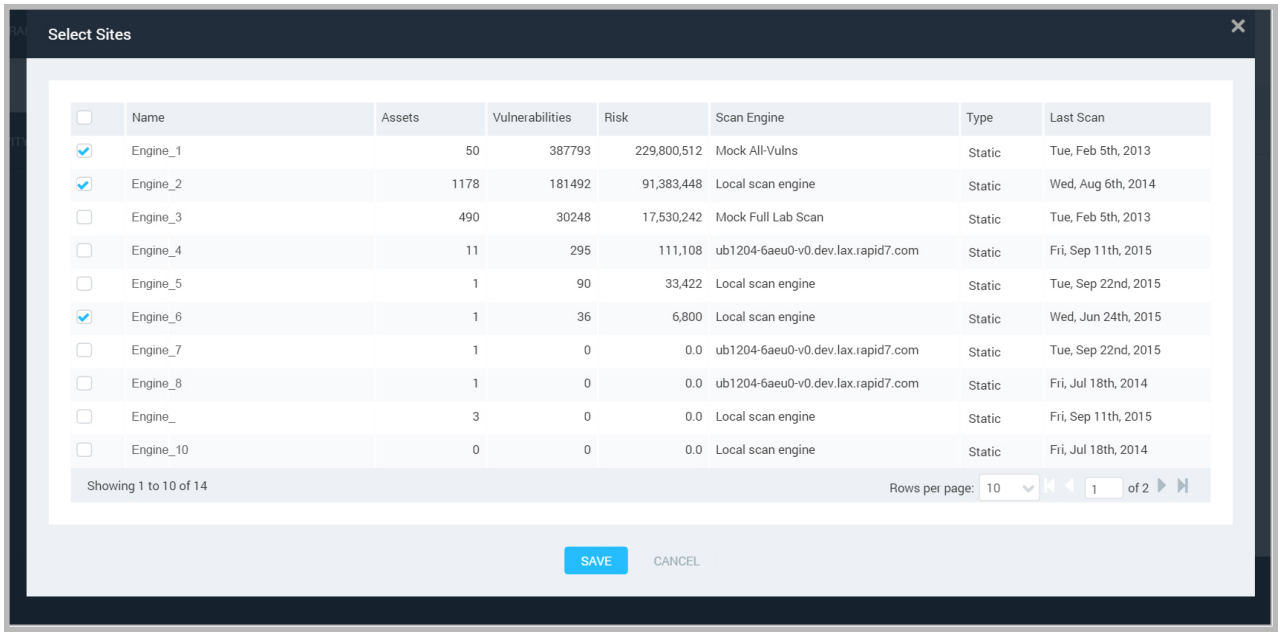
Assigning a site to the new Scan Engine

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.