



Nexpose 5.2 Installation and Quick-start Guide

Revision history

Revision date	Description
November 11, 2009	Verified, tested, and updated installation procedures. Updated document template.
November 25, 2009	Updated lists of required packages for Linux and instructions for using md5sum.
December 3, 2009	Updated system requirements.
March 8, 2010	Added note recommending 64-bit configuration.
June 21, 2010	Added quick-start instructions and appendix on opening the Windows firewall.
October 25, 2010	Updated URL for downloading deprecated libstdc++5 package; added reference to instructions in the administrator's guide for configuring offline activations and updates; removed deprecated references from sections on running the installation program; added instructions for first-time users to activate licenses.
October 25, 2010	Expanded documentation on uninstalling for reinstallation.
January 31, 2011	Removed installation instructions for platform that is not officially supported.
March 18, 2011	Removed references to unsupported platforms.
April 22, 2011	Removed references running on 32-bit and Windows systems; removed platform-specific instructions for opening firewalls on Windows targets.
July 11, 2011	Updated instructions to reflect process with new installer.
July 12, 2011	Corrected minor layout issues.
July 25, 2011	Corrected several instructions for installing and removing Nexpose; updated supported browser information.
August 15, 2011	Added instructions on enabling FIPS mode.
November 15, 2011	Added information about vAsset discovery, dynamic site creation, and using risk trends in reports.
January 18, 2012	Nexpose 5.1. Updated Linux pre-installation instructions.
March 21, 2012	Nexpose 5.2. Updated the information about supported browsers.

Contents

Revision history	2
About this guide	5
Document conventions	5
For technical support	5
Using the Help site and other documents	6
About the product	7
Vulnerability management	7
The main components	7
Installation requirements	8
Hardware requirements	8
Network activities and requirements	8
Supported platforms	9
Making sure you have necessary installation items	10
Installing in Windows environments	11
Uninstalling a previously installed copy	11
Creating the Global Administrator account	11
Installation options	11
Running the Windows uninstaller	16
Installing in Linux environments	17
Uninstalling a previously installed copy	17
Do I need to disable SELinux?	17
Ensuring that the installer file is not corrupted	17
Installing in Ubuntu	18
Installing in Red Hat	18
Running the Linux installer	19
Running the Linux uninstaller	21
Working with FIPS mode	22
Enabling FIPS mode	22
Manually starting and stopping	24
Manually starting or stopping in Windows	24
Changing the configuration for starting automatically as a service	24
Manually starting or stopping in Linux	25
Working with the daemon	25

Getting started	26
Obtaining information on offline activations and updates	26
Logging on	27
Navigating the Security Console Home page	28
Using the search feature	30
Using configuration panels	30
Setting up a site and configuring scans	30
Manually starting, stopping, pausing, and resuming scans	33
Viewing scan data	34
Creating asset groups	35
Configuring reports	35
Glossary	41

About this guide

Use this guide to help you to perform the following tasks:

- install the Windows or Linux version of Nexpose software
- enable FIPS mode (if necessary)
- start Nexpose
- log onto the Security Console Web interface
- get started using Nexpose

Document conventions

Words in **bold** are names of hypertext links and controls.

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

1. Steps of procedures are indented and are numbered.

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

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

Variables in command examples are enclosed in box brackets.

Example: [installer_file_name]

Options in commands are separated by pipes.

Example: \$ /etc/init.d/[daemon_name] start|stop|restart

Keyboard commands are bold and are enclosed in arrow brackets.

Example: Press and hold <Ctrl + Delete>

NOTES, TIPS, and WARNINGS appear in the margin.

NOTES contain information that:

- enhance a description or a procedure.
- provide additional details that only apply in certain cases.

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

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

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

For technical support

For technical support:

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

Using the Help site and other documents

After you start Nexpose and log onto the Security Console Web interface, use the *Help* site by clicking the **Help** link that appears on any page of the interface. The site provides information on:

- important concepts and terms
- setting up sites and scans
- running scans
- creating and running reports
- viewing vulnerabilities and excluding specific vulnerabilities from reports
- creating tickets (only available with the Enterprise version of Nexpose)
- creating and modifying scan templates (only available with the Enterprise version of Nexpose)
- creating user accounts
- creating asset groups
- configuring various settings
- maintaining and troubleshooting
- backing up and restoring the database

You will find these documents useful, as well:

- administrator's guide
- user's guide
- API guides

You can download these documents from the *Support* page in *Help*. Click the **Help** link that appears on any page of the Security Console Web interface. In the left navigation pane of *Help*, click the **Support** link.

About the product

This section will help you to understand the components that you are about to install.

Vulnerability management

Nexpose is a unified vulnerability detection and management solution that scans networks to identify the devices running on them and to probe these devices for vulnerabilities. It analyzes the scan data and processes it for reports. You can use these reports to help you assess your network security at various levels of detail and remediate any vulnerabilities quickly.

The vulnerability checks identify security weaknesses in all layers of a network computing environment, including operating systems, databases, applications, and files. The application can detect malicious programs and worms, identify areas in your infrastructure that may be at risk for an attack, and verify patch updates and security compliance measures.

The main components

Nexpose consists of two main components:

- **Scan Engines**
Perform asset discovery and vulnerability detection operations. You can deploy them outside your firewall, within your secure network perimeter, or inside your DMZ to scan any network asset.
- **Security Console**
Communicates with Scan Engines to start scans and retrieve scan information. All exchanges between it and Scan Engines occur through encrypted SSL sessions over a dedicated TCP port that you can select. For better security and performance, Scan Engines do not communicate with each other; they only communicate with the Security Console.

When an asset is scanned for the first time, the Security Console creates a repository of information about that asset in its database. With each ensuing scan of the asset, the console updates the information in the repository.

The Security Console includes a Web-based interface for configuring and using the application. An authorized user can log on to this interface securely using HTTPS to perform any task that his or her role permits. See the section *Managing users and asset groups* in the *administrator's guide*. The authentication database is stored in an encrypted format on the console server, and passwords are never stored or transmitted in plain text.

Other Security Console functions include generating user-configured reports and regularly downloading patches and other critical updates from the central update system.

You can download software-only Linux or Windows versions for installation on your own in-house servers, depending on your license.

Nexpose components are also available in a dedicated hardware and software combination called an *Appliance*. Another option is to purchase remote scanning services from Rapid7.

This guide is for installing the software-only version of Nexpose.

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.

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
provide Web interface access to Nexpose 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 2008 (R2 SP1), Standard, Enterprise 64-bit
- Windows Server 2003 (R1 and R2, SP2), Standard, Enterprise 64-bit
- Windows Server 2003 (R1 and R2, SP2), Standard, Enterprise 32-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.

Linux

- RHEL Server 5.x 64-bit
- Ubuntu 8.04 LTS 64-bit
- Ubuntu 8.04 LTS 32-bit
- Ubuntu 10.04 LTS 64-bit

Making sure you have necessary installation 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 onto Nexpose.

If you purchased Nexpose or registered for an evaluation, Rapid7 sent you an e-mail that includes links for downloading these items and the product key. We recommend you add Nexpose to your e-mail client white list communication to ensure you receive future e-mails about Nexpose.

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 Nexpose 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 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 *Running the Windows uninstaller* on page 16 to uninstall any previously installed copies.

Creating the Global Administrator account

Regardless of your role, you must create the Global Administrator account and create credentials for the account when you install the application. You 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.

The Global Administrator can modify your account, including changing your credentials after you complete the installation (see *Managing and creating user accounts in Help*).

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.

Installation options

During the installation, you can:

- Select the components you want to install and where to install them.
- Enable the application to initialize during the installation and start automatically after installation.

The installation procedure contains the steps to make these choices.

Selection of components

You have the option of installing the Security Console and Scan Engine, or only the Scan Engine. If you install only the Scan Engine, you must install the Security Console before you can use the Scan Engine. This is because 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 (compared to an installation in which the option is disabled). Although disabling it 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

Make sure that:

- Your system meets the minimum installation requirements. See *Installation requirements* on page 8 for details.
- You have all of the items you need to complete the installation. See *Making sure you have necessary installation items* on page 10 for details.
- You have uninstalled any previously installed copies of the application. See *Running the Windows uninstaller* on page 16 for details.

To install the application, take these steps:

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

1. Double-click the **installer icon**.
A message is displayed that it is preparing the wizard to guide you through the installation, then the *Welcome* page of the wizard is displayed.
Command-line interface screens open once you begin the installation.
Although you do not need them, do not close them.
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.
4. Read the agreement and select the **I accept the agreement** option. If you do not accept it, you cannot continue the installation.
5. Click **Next**.
The installer displays the *User details* page.
6. Type your first name, last name, and company name in the appropriate boxes.
7. Indicate whether you have a product key by doing one of the following:
 - Select the **I already have a product key** option and click **Next**.
The *Type and destination* page is displayed. Go to **step 10** to continue.
 - Leave the **I would like to register for a product key** option selected and click **Next**.
The registration form is displayed. Go to **step 8**.
8. Type 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!.
9. Click **Next**. The registration form is submitted. You should receive an e-mail from Rapid7 within 5 minutes that contains the product key.
Type and destination page is displayed.
10. Select the components you want to install by doing one of the following:
 - Select the **Nexpose Security Console with local Scan Engine** option. If you do not install the Security Console, the application cannot initialize during installation.
 - Select the **Nexpose Scan Engine only** option. If you install only the Scan Engine, you must install the Security Console before you can use the Scan Engine.

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

11. Select where you want to install the components by doing one of the following:
 - Click **Next** to accept the default directory.
 - Change the installation directory by doing one of the following:
 - Type the preferred installation directory path in **Destination directory** box, then click **Next**.
The *Account details* page is displayed.
 - Click **Change** to open the Select Directory dialog and select or create the preferred directory, then click **OK**.
The directory shows in the Destination directory box. Change it if needed by opening the Select Directory dialog again, or click **Next**.
The *Account details* page is displayed.
12. In the *Account details* page, type a user name and password. Type the password again for confirmation, and click **Next**.
The installer displays the *Shortcut location* page.
13. To choose to have the shortcut, do one of the following:
 - To create a shortcut, leave the check box selected for creating a **Start Menu** folder.
 - If you do not want to create a shortcut, clear the check box for creating a **Start Menu** folder. Click **Next** and go to step 15.
14. To choose the location of the shortcut, do one of the following:
 - To accept the default location (a folder named Nexpose, 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.
15. Review your settings and do one of the following:
 - Go to step 16 if you do not need to change any settings.
 - To change any settings, click **Previous** to go to the desired page, make the changes, then return to the *Confirm selections* page.
16. To create a desktop icon you can double-click to start the program after installation, leave the appropriate check box selected. Otherwise, clear it.
17. 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).
If you want to enable FIPS mode, disable this option. FIPS mode must be enabled before the application starts for the first time.

18. 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.

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

19. 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.

The application files are installed. If you only installed the Scan engine, complete step 20 and 21 to finish the installation. If you installed the Security Console, complete steps 22, 23, and 24 to finish the installation.

Scan Engine

20. Click **Finish**.

21. Start the Scan Engine (see *Working with FIPS mode* on page 22).

Security Console

22. Read the instructions for getting started with the product.

23. Do one of the following:

- If you disabled the initialization option, you must start the application manually (see *Working with FIPS mode* on page 22).
- 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.

24. Click **Finish**. See *Getting started* on page 26 for information on getting started using the application.

Running the Windows uninstaller

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

WARNING: To prevent a loss of sites, configurations, reports, and other data, make sure you back up all of your data before you begin the procedure.

Uninstalling completely removes all components. It also deletes sites, configurations, reports, and any scan data on discovered assets, nodes, and vulnerabilities.

To uninstall the application:

1. Start the program to uninstall by doing one of the following:
 - Click the Windows **Start** button and select the **Control Panel**.
 - Select the **uninstall** option or the **remove a program** option (depends on the version of Windows you are running).
 - (If you have a shortcut folder.) Click the Windows **Start** button, go to the Nexpose folder, and select the **Uninstaller**.
2. Double-click Nexpose in the list of programs.
3. Run the uninstaller program.

The uninstaller displays a *Welcome* page. Read the warning about backing up data.
4. Click **Next**.

The uninstaller displays a status bar with a message that uninstallation is in progress followed by a message that the uninstallation is complete.
Do not close the command line window.
5. Click **Finish**.

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 *Running the Linux uninstaller* on page 21 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.

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=`.
3. If the setting is `enforcing`, change it to `disabled`: `SELINUX=disabled`.
4. Save and close the file.
5. 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.

Before you begin

Make sure that you downloaded the installation file and the md5sum file. See *Making sure you have necessary installation items* on page 10 for details.

To check the installer file, take these steps:

1. Go to the directory that contains the installer and the md5sum file.
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.

Before you begin

Make sure that:

- You have downloaded all items necessary for installation. See *Making sure you have necessary installation items* on page 10 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 17.

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.

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 packages must be installed:

- screen
- libstdc++5 (32-bit only)

Next Steps

Run the Linux installer (see *Running the Linux installer* on page 19).

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.

Before you begin

Make sure that:

- You have downloaded all items necessary for installation. See *Making sure you have necessary installation items* on page 10.
- 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 17.

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

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 11)). 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 *Making sure you have necessary installation items* on page 10.
- You have disabled SELinux (if necessary). See *Do I need to disable SELinux?* on page 17.
- (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 17.
- You have installed the required packages for your Linux platform.
- You have uninstalled any previously installed copies. See *Running the Linux uninstaller* on page 21.

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. Type **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:
 - Type **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. Type **y** and press **<ENTER>** to go to the next screen.
7. At the final screen of the agreement, if you agree with the terms, type **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 the company name by doing the following:
 - Type your **first name** and press **<ENTER>**.
 - Type your **last name** and press **<ENTER>**.
 - Type your **company name** and press **<ENTER>**.
A prompt is displayed to select an installation directory.

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

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

9. Select the installation directory by doing one of the following:
 - Press <ENTER> to accept the default installation directory (displayed in square brackets).
 - Type a **different directory path**, then press <ENTER>.A prompt is displayed to select the components you want to install.
10. 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.
11. To create the Global Administrator account, do the following:
 - Type a **user name** and press <ENTER>.
 - Type a **password** and press <ENTER>.
 - Type the **password** again for confirmation and press <ENTER>.Your installation settings are displayed.
12. 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 is created in the **Applications | Internet** menus. Type **y** and press <ENTER> to create the icon or type **n** to decline it.An option is displayed to have the application initialize during installation and start automatically after installation.
13. Type **y** and press <ENTER> to accept the option, or type **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.
14. Read the additional information.
15. Press <ENTER> to exit the installer.

Running the Linux uninstaller

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

Uninstalling completely removes all components. It also deletes sites, configurations, reports, and any scan data on discovered assets, nodes, and vulnerabilities.

To uninstall the application, take these steps:

1. Run: `$ [installation directory]/.install14j`
`install14j` is a hidden directory. To list hidden directories, run: `ls -a`.
2. Run: `$/uninstall`

WARNING: To prevent a loss of sites, configurations, reports, and other data, make sure you back up all of your data before you begin the procedure.

Working with FIPS mode

Enabling FIPS mode

If you are operating Nexpose in an environment where the use of FIPS-enabled products is mandatory, or if you want the security of using a FIPS-certified encryption module, you should enable FIPS mode. The application supports the use of Federal Information Processing Standard (FIPS) 140-2 encryption, which is required by government agencies and companies that have adopted FIPS guidelines.

What is FIPS?

The FIPS publications are a set of standards for best practices in computer security products. FIPS certification is applicable to any part of a product that employs cryptography. A FIPS-certified product has been reviewed by a lab and shown to comply with FIPS 140-2 (Standard for Security Requirements for Cryptographic Modules), and to support at least one FIPS-certified algorithm.

Government agencies in several countries and some private companies are required to use FIPS-certified products.

What is FIPS mode?

FIPS mode is a configuration that uses FIPS-approved algorithms only. When the application is configured to operate in FIPS mode, it implements a FIPS-certified cryptographic library to encrypt communication between the Security Console and the user for both the browser and API interfaces.

FIPS mode considerations

It is important to note that due to encryption key generation considerations, the decision to run in FIPS mode or non-FIPS mode is irrevocable. The application must be configured to run in FIPS mode immediately after installation and before it is started for the first time, or else left to run in the default non-FIPS mode. Once the application has started with the chosen configuration, you will need to reinstall it to change between modes.

Activating FIPS mode

When Nexpose is installed, it is configured to run in non-FIPS mode by default. The application must be configured to run in FIPS mode before being started for the first time. See *Activating FIPS mode in Linux* on page 23.

When FIPS mode is enabled, communication between the application and non-FIPS enabled applications such as Web browsers or API clients cannot be guaranteed to function correctly.

Activating FIPS mode in Linux

You must follow these steps after installation, and BEFORE starting the application for the first time.

To enable FIPS mode:

1. Install `rng-utils`.
The encryption algorithm requires that the system have a large entropy pool in order to generate random numbers. To ensure that the entropy pool remains full, the `rngd` daemon must be running while the application is running. The `rngd` daemon is part of the `rng-utils` Linux package.
2. Download and install the `rng-utils` package using the system's package manager.
3. Run the command `rngd -b -r /dev/urandom`.
4. Create a properties file for activating FIPS mode.
5. Create a new file using a text editor.
6. Enter the following line in this file:
`fipsMode=1`
7. Save the file in the `[install_directory]/nsc` directory with the following name:
`CustomEnvironment.properties`
8. Start the Security Console.

TIP: Add the `rngd` command to the system startup files so that it runs each time the server is restarted.

Activating FIPS mode in Windows

You must follow these steps after installation, and before starting the application for the first time.

To enable FIPS mode:

1. Create a properties file for activating FIPS mode.
2. Create a new file using a text editor.
3. Enter the following line in this file:
`fipsMode=1`
4. Save the file in the `[install_directory]\nsc` directory with the following name:
`CustomEnvironment.properties`
5. Start the Security Console.

NOTE: You can disable database consistency checks on startup using the `CustomEnvironment.properties` file. Do this only if instructed by Technical Support.

Verifying that FIPS mode is enabled

To ensure that FIPS mode has been successfully enabled, check the Security Console log files for the following messages:

```
FIPS 140-2 mode is enabled. Initializing crypto provider
Executing FIPS self tests...
```

Manually starting and stopping

If you disabled the initialize and start option as part of the installation, or if you have configured Nexpose so that it does not start automatically as a service when the host system starts, you need to start it manually.

Manually starting or stopping in Windows

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

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

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

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

To manually stop in Windows

To manually stop the application in Windows:

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 Nexpose 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 Nexpose 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 Nexpose icon in 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
```

Run the script: `./nsc.sh`

Working with the daemon

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

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 `nscsvc`:

```
./[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:

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

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

Getting started

After you have installed Nexpose, you can use it right away to find vulnerabilities in your environment. This section provides instructions for:

- logging on
- becoming familiar with the Security Console Web interface
- setting up a site and configuring a scan
- starting and stopping a scan manually
- viewing scan data
- working with asset groups
- creating a report

For more detailed instructions, go to *Help* by clicking the **Help** link on any page of the Web interface.

Click the **Support** link to view and download all documentation.

Obtaining information on offline activations and updates

If your Security Console is not connected to the Internet, you can find directions for performing offline activations and updates in the *administrator's guide*. Download the guide from the *Support* page in *Help*.

Logging on

The Security Console Web interface supports the following browsers:

- Internet Explorer 7.0.x, 8.0.x, and 9.0
- Mozilla Firefox 3.5.x, 3.6.x, and 10.0.x
- Google Chrome 16 and 17

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 type it with or without hyphens. Whether you choose to include or omit hyphens, do so consistently for all four sets of numerals.

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

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

To log on to the Security Console:

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`
2. 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.
If there is a usage conflict for port 3780, you can specify another available port in the XML file `[installation_directory]\nsc\conf\httpd.xml`. You also can switch the port after you log on. See *Managing Security Console settings* in the *administrator's guide* or *Help*.
Your browser displays the *Logon* box.
If the logon box indicates that the Security Console is in maintenance mode, then either an error has stopped the system from starting properly, or a scheduled task has initiated maintenance mode. See *Running in maintenance mode* in the *administrator's guide* or *Help*.
3. Enter your user name and password that you specified during installation.
User names and passwords are case-sensitive and non-recoverable.
4. Click the **Logon** button.
If you are a first-time user and have not yet activated your license, the console displays an activation dialog box. Follow the instructions to enter your product key.
5. Click **Activate** to complete this step.
If the console displays a warning about authentication services being unavailable, and your network uses an external authentication source such as LDAP or Kerberos, your Global Administrator must check the configuration for that source. See *Using external sources for user authentication* in the *administrator's guide*. The problem may also indicate that the authentication server is down.
6. Click the **Home** link to view the Security Console *Home* page.
7. Click the **Help** link on any page of the Web interface for information on how to use the application.

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

Navigating the Security Console Home page

When you log on 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 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.

- A row of tabs appears at the top of the *Home* page, as well as every page of the Security Console. Use these tabs to navigate to the main pages for each area.
- 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 *Tickets* page lists remediation tickets and their status.
- The *Reports* page lists all generated reports and provides controls for editing and creating report templates.
- The *Administration* page is the starting point for all management activities, such as creating and editing user accounts, asset groups, and scan and report templates. Only global administrators see this tab.














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.

On the *Home* page and throughout the interface, you can use various controls for navigation and administration.

Control	Description
	Minimize any pane so that only its title bar appears.
	Expand a minimized pane.
	Close a pane.
Configure link	Click to display a list of closed panes and open any of the listed panes.
	Reverse the sort order of listed items in a given column. You can also click column headings to produce the same result.
	Export asset data to a comma-separated value (CSV) file.
	Start a manual scan.
	Pause a scan.
	Resume a scan.
	Stop a scan.
	Edit properties for a site, report, or a user account.
	Preview a report template.
	Delete a site, report, or user account.
	Exclude a vulnerability from a report.
Help link	View Help.
News link	View the <i>News</i> page which lists all updates.
Log Out link	Log out of the Security Console interface. The <i>Logon</i> box appears. For security reasons, the Security Console automatically logs out a user who has been inactive for 10 minutes.
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.
Search box	Search the database for assets, asset groups, and vulnerabilities.

Using the search feature

With the powerful full-text search feature, you can search the database using a variety of criteria, including full or partial IP addresses. For example, you can search for “192.168”, and all IP address that start with 192.168.x.x are returned.

Enter your search criteria in the **Search** box on any a page of the security console interface, and click the magnifying glass icon.

The application displays the *Search* page, which lists results in various categories. Within each category pane, the application displays the results in a table that includes all possible features for that category. For example, the table in the *Vulnerability Results* pane includes all the columns that appear on the *Vulnerabilities* page. At the bottom of each category pane, you can view the total number of results and change settings for how results are displayed.

In the *Search Criteria* pane, you can refine and repeat the search. You can change the search phrase and select check boxes 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 configuration panels

Nexpose provides panels for configuration and administration tasks:

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

All panels have the same navigation scheme. You can either use the navigation buttons in the upper-right corner of each panel page to progress through each page of the panel, or you can click a page link listed on the left column of each panel page to go directly to that page.

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

To save configuration changes, click the **Save** button that appears on every page. To discard changes, click the **Cancel** button.

Setting up a site and configuring scans

Before you can set up a site you must have a Scan Engine running and paired with the Security Console. See the topic *Setting up Scan Engines* in *Help*.

Types of sites

The two basic types of sites you can set up are dynamic sites and static sites. The procedure below shows you how to set up a static site. For more information about creating dynamic sites, see *Using discovery to track your assets* and *Setting up sites and scans* in *Help* or the *administrator's guide*.

Selection of site assets

When you set up a site, you determine which assets you want to be scanned by selecting which assets to be included in scans and which assets to be excluded from scans. The information you need to do this are the IP addresses and host names of the assets.

When you selects assets for inclusion or exclusion, you can manually enter the IP addresses and host names, or you can import comma delimited or new-line delimited ASCII text file that contain the IP addresses and host names. IP addresses can be specified by range or as single asset addresses.

User access

You must give users access to a site in order for them to be able view assets or perform asset-related operations, such as scanning or reporting, with assets in that site.

Using templates to configure scans

When you configure scans for a site, you can use pre-defined scan templates that enable you to define the scan properties quickly and easily (this prevents you from having to manually define scan properties). Some examples of scan properties are port scan methods and targeted vulnerabilities. See *Specifying scan settings* in *Help* for a comparison of pre-defined scan templates and *Working with scan templates* in *Help* for information on how to customize scan templates.

Scan configuration options

You have the option of utilizing a number of options when you configure scans for a site. These options include:

- scheduling scans
- adding credentials
- setting up alerts

Scheduling scans

When you configure scans you can choose to have the scans run automatically based on a schedule. You are also able to select the scheduling options.

Adding credentials

When you configure scans you can choose to include credentials in the scan (a scan that contains credentials is referred to as a credentialed scan). Making a scan a credentialed scan enables the application to perform deep checks, inspecting assets for a wider range of vulnerabilities. Additionally, credentialed scans can check for software applications and packages such as hotfixes. For more information, see *Configuring scan credentials* in *Help*.

Setting up alerts

You have the option of setting up alerts so you can be automatically notified when important scan events occur, such as the discovery of certain vulnerabilities. Some alert settings filter alerts according to criteria such as the level of severity or the level of certainty that these vulnerabilities exist. See *Setting up alerts* in *Help*.

Before you begin

Make sure that you have a Scan Engine running and paired with the Security Console.

To create a static site:

1. Click the **New Site** button on the *Home* page.
The *Site Configuration* panel is displayed.
2. Enter a name and description for your site.
3. Select a level of importance, which corresponds to a risk factor used to calculate a risk index for the site.
4. Go to the *Assets* page.
5. Select the assets to be included in scans by:
 - Entering the **IP addresses** (by range or by asset) and the **host names**.
 - Importing a comma delimited or new-line delimited ASCII text file that contains the IP addresses and host names.
6. Select the assets to be excluded from scans by:
 - Entering the **IP addresses** (by range or by asset) and the **host names** in the *Devices to Exclude* box.
 - Importing a comma delimited or new-line delimited ASCII text file that contains the IP addresses and host names.
7. Go to the *Scan Setup* page.
8. Select the **Enable schedule** option to have the scan to run automatically based on a schedule.
9. Select the **schedule** settings.
10. Go to the *Alerting* page.
11. Click the **New Alert** button and edit or select settings according to your preferences.
12. Go to the *Credentials* page.
13. Click **New Login**. The steps for setting up credentials depend on the type of system you want to access. See *Configuring scan credentials* in *Help*.
14. Go to the *Access* page.
15. Click **Add Users**.
The *Add Users* dialog box is displayed.
16. Select the check box for every user account you want to add to the access list.
17. Click **Save**.
18. To save the site configuration, click **Save** on any page of the panel. To discard changes, click the **Cancel** button.

Manually starting, stopping, pausing, and resuming scans

Once you set up a site, you can manually start, stop, pause, and resume scans regardless of whether or not you scheduled scans to run automatically for that site.

Starting and stopping a scan

To manually start and stop a scan, take these steps:

1. Choose to run the scan for one site or multiple sites by doing the following:
 - (Single site) Click the **New Manual Scan** icon for a site in the *Site Listing* pane of the *Home* page.
 - (Single or multiple sites) Click the **New Manual Scan** button on the *Sites* page or on the page for a specific site.
The *Start New Scan* dialog shows all asset scan targets you specified in the site configuration.
2. Select the assets to be scanned by doing one of the following:
 - Select the **option to scan all assets** within the scope of a site.
 - Select **specific** assets.
The IP addresses or host names of the assets are listed in the text box.
3. Click the **Start Now** button to begin the scan immediately.
4. Go to any of these pages to view the status of the scan as it runs:
 - the *Home* page
 - the *Sites* page
 - the page for the site that is being scanned
 - the page for the actual scan
5. To stop the scan, do one of the following:
 - (*Home* page or *Sites* page) Click the **Stop** icon.
 - (Specific *site* page) Click the **Stop** icon.
 - (Specific *scan* page) Click the **Stop Scan** button.
A message is displayed asking you to confirm that you want to stop the scan.
6. Click **OK**. It may take 30 second or more to stop the scan, depending on any in-progress scan activity.

TIP: Use breadcrumb links to go back and forth between the *Home* page, *Sites* page, and specific site and scan pages.

Pausing and resuming a scan

To manually pause and resume a scan that is running, take these steps:

1. To pause the scan, do one of the following:
 - (*Home* page or *Sites* page) Click the **Pause** icon.
 - (Specific *site* page) Click the **Pause** icon.
 - (Specific *scan* page) Click the **Pause Scan** button.
A message is displayed asking you to confirm that you want to pause the scan.
2. Click **OK**.
3. To resume the scan, do one of the following:
 - (*Home* page or *Sites* page) Click the **Resume** icon.
 - (Specific *site* page) Click the **Resume** icon.
 - (Specific *scan* page) Click the **Resume Scan** button.
A message is displayed asking you to confirm that you want to resume the scan.
4. Click **OK**.

Viewing scan data

The Security Console Web interface provides detailed views of scanned assets and discovered vulnerabilities.

To view asset data, click the **Assets** tab. On the *Assets* page, click the **View** link for the category by which you want to see the assets organized.

- sites to which they are assigned
- asset groups to which they are assigned
- operating systems that they are running
- services that they are running
- software that they are running
- policy check results

Viewing vulnerabilities and their risk scores helps you to prioritize remediation projects.

To view vulnerabilities, click the **Vulnerabilities** tab that appears on every page of the Security Console interface. The console displays the *Vulnerabilities* page.

For every vulnerability, a set of metrics that indicate the danger that this vulnerability poses to your network security is displayed. Vulnerabilities that make your environment susceptible to being compromised by exploits or malware kits appear with icons that you can click for more information about these exposures. See *Viewing active vulnerabilities* in *Help* or the *user's guide*.

You can click the icon in the *Exclude* column for any listed vulnerability to exclude that vulnerability from a report. See *Creating vulnerability exceptions* in *Help*.

Creating asset groups

While it is easy to view information about scanned assets, it is a best practice to create asset groups to control which users can see which asset information in your organization. Since an asset group can contain assets from multiple sites, each using a different Scan Engine, you can generate reports incorporating information from multiple Scan Engines.

Asset groups provide different ways for members of your organization to grant access to, view, and report on, asset information. You can use the same grouping principles that you use for sites, create subsets of sites, or create groups that include assets from any number of different sites.

Asset groups also have a useful security function in that they limit what member users can see, and dictate what non-member users cannot see. The asset groups that you create will influence the types of roles and permissions you assign to users, and vice-versa.

You can create two types of asset groups:

- A *dynamic asset group* contains scanned assets that meet a specific set of search criteria. The list of assets in a dynamic group is subject to change with every scan.
- A *static asset group* contains assets that meet a set of criteria that you define according to your organization's needs. Unlike with a dynamic asset group, the list of assets in a static group does not change unless you alter it manually.

For information on how to create and use asset groups, see *Using asset groups to your advantage* in *Help*.

Configuring reports

Nexpose provides pre-defined templates that enable you to configure reports that focus on vulnerabilities, specific risk levels of vulnerabilities, remediation plans, policy evaluation, PCI compliance, and other criteria.

The pre-defined templates contain attributes that you can use to ensure that reports can easily be made available to others in your organization that use the reports. For example, reports can be exported to external databases or formatted Web-based viewing. To export reports to an external database, you must have one or more external, JDBC-compliant databases available to you. See *Specifying general report attributes* in *Help* for more information about report templates and formats.

In addition to using pre-defined templates, you can configure custom report templates for your specific needs (see *Creating a custom report template* in *Help*).

As with setting up sites and scans, the Security Console Web interface provides a wizard for configuring reports.

Ownership of reports

Roles affect ownership of reports. If you are not a Global Administrator, you are automatically designated as the report owner when you create a report. You can also become a report owner if a Global Administrator designates you as the owner of a report they generate.

After a report is generated, only a Global Administrator and the report owner can see the report on the Reports page. If you are not a Global Administrator and you create a report, you are automatically designated as the report owner.

If you are a Global Administrator, you can choose to retain ownership of any report you create or you can assign a user to be the owner of the report. If you create a report and assign a user as the report owner, you can choose to have a copy of the report stored in the report owner's directory.

Report configuration options

You have a number of options available to you during the report configuration process that enable you to tailor reports to fit the needs of your organization.

Selection of scan data (historical or most recent only)

You have the option of including only the most recent scan data in the report, instead of all historical scan data. The default is to include all historical scan data.

Inclusion of risk trend graphs

You can choose to include risk trend graphs in your Executive Overview or custom report templates. The graphs represent how risk has changed over time for a particular asset or group of assets. When selecting assets, you can select individual assets, groups of assets, the five highest risk sites, the five highest risk asset groups, or the five highest risk assets.

In addition to selecting assets, you can choose to include the Total risk score and Average risk score in the graphs. Setting the date range for your report establishes the report period for risk trends in your reports. For more information about using risk trends, see the *administrator's guide*.

Report generation (automatic or manual)

You can configure reports to be generated automatically or manually. This is a good idea if you have an asset group that contains assets that are assigned to many different sites, and each site has a different scan template. Since these assets are scanned frequently, it makes sense to generate reports automatically.

Automatic

You can configure the application to generate reports automatically based on a schedule or immediately after a scan.

Manual

You can configure a report so that it is run once only, as soon as you complete the configuration. Use this option to run reports on an as-needed basis.

Report availability

If you are a Global Administrator, you can choose to make reports available to users that either do not have a Security Console or users that cannot view a report because they are not the report owner. This can be done by:

- exporting reports to external databases
- storing reports in user directories
- distributing reports by e-mail

Exporting to external databases

You can export reports to an external database to make the reports available to users that have access to those databases. Only reports that have the Database Export report format can be exported to external databases.

Storing reports in user directories

You can store copies of reports in specific user directories of the file system. This enables users with access to those directories to view the reports immediately after they are created. To use of this feature, you need to create custom user directories (user directory paths must follow a canonical naming convention). For more information, see *Storing reports in user directories* in *Help*. See the *user's guide* for detailed instructions on the naming conventions for user directory paths.

Distributing reports by e-mail

You also can configure reports to be distributed by e-mail. The reports are sent as a URL link or as an attachment. This is a convenient way to distribute reports automatically to users who are responsible for remediation of vulnerabilities.

You may require an SMTP relay server to use this feature. This is because a firewall may prevent the application from accessing your network's mail server.

If you are using an SMTP relay server, type its address in the appropriate field. If you leave SMTP relay server field blank, the application searches for a suitable mail server for sending reports. Also, the application regards the mail sender address as the “originator” of e-mailed reports.

Configuring a report

This procedure shows you how to configure a report. It includes the steps to enable each of the report configuration options.

To configure a report, take these steps:

1. Click the **New Report** button on the *Reports* page.
The console displays the *General* page of the *Report Configuration* panel.
2. Enter a unique name for the new report.
3. Select a report format. If you want to export the report to an external database, you must select **Database Export**.
If you select **Database Export**, the *Report Configuration—Output* page has fields for transferring scan data to a database.
4. Select a template from the drop-down list.
5. Click the **Browse Templates** button to view information about templates.
6. Click the **Preview** icon in the *Browse Templates* dialog box to view a sample of a template.
7. Select a time zone for the report.
8. (Global Administrator only) Go to the *Scope* page and select a report owner.
9. Select the assets to be included in the report by doing one or more of the following:
 - Click the **Select devices...** button to view a list of all assets in your organization as defined when the sites were created.
 - Click the appropriate buttons to **select entire sites** or **asset groups**.
 - Click the **Select devices...** button to select **individual assets**.
 - Type or select the search criteria and click the **Apply Filter** button to select **sites, asset groups, and individual assets**.
All the filter settings are applied and the console displays a list of search results. Click the check boxes for each asset that you wish to add to the group. Click the **Save** button.
10. Select the type of scan data you want in the report. You can:
 - Accept the default to include **all historical data**.
 - Select the option to include **only the most recent scan data**.
11. Go to the *Report Configuration—Schedule* page.
12. To configure the report to be generated this time only, click the **This time only** radio button.
13. To configure the report to be generated automatically based on a schedule, do the following:
 - Click the **On the following schedule** button.
 - Click the **calendar** icon to select a start date.
 - Type a **start time** in the hour and minute fields to the right of the calendar icon.
 - Type a value in the **Repeat every** field to select the time interval and select a time unit.

TIP: You can page through the list or search for specific assets by IP address range, device name, site, or operating system.

-
14. To configure the report to be generated automatically immediately after a scan, click the **After each scan** radio button.

The next steps are for including risk trend graphs in the report. (They are optional.)

15. Go to the *Scope* page of the *Report Configuration* panel.
16. Select the assets to include in the graphs go to *Advanced Properties* page and do one of the following:
 - Select **All assets in report scope** to graph all assets in your organization
 - Choose the **five highest risk sites**.
 - Choose the **five highest risk asset groups**.
 - Choose the **five highest risk assets**.
17. Specify **Total risk score** and **Scope trend** to include the **Average risk score** or **Number of assets** in your graphs.

The next steps are for making the report more widely available to users. They are optional and can only be completed by a Global Administrator.

18. Create custom directories within the Nexpose directory structure.
19. Go to the *Report Configuration—Output* page.
20. To configure the report to be stored in a user directory, type the **path of the user directory** using a canonical naming convention, in which variables replace certain absolute values.
See the *user's guide* for detailed instructions.
21. To configure database export setting, do the following:
 - Select the **database type** from the drop-down list of the *Output* page.
 - Enter the **IP address** and **port** of the database server.
 - Enter a **name** for the database.
 - Enter the **administrative user ID and password** for logging on to that database.
22. (Optional) Check the tables in the target database to confirm that the scan results were exported.
23. If you are using an SMTP relay server, type its **address** in the appropriate field.
If you leave it blank, the application searches for a suitable mail server for sending reports. Also, the application regards the mail sender address as the “originator” of e-mailed reports.
24. Go to the *Report Configuration—Distribution* page.
25. Select the **Send E-mail** check box.
26. Choose the attachment option you want by doing one of the following:
 - Click the **URL** option.
 - Click the **uncompressed file** option (**File**).
 - Click the **zipped file** option.
27. Select the appropriate checkbox to send the report to users that have access to the assets included in the report.
28. Type the **e-mail addresses** of any other people you want to automatically receive the report by e-mail.
29. Type the **e-mail address** of the sender.

To save the report configuration.

30. Click the **Save** button to save the report configuration.

WARNING: If you do not use the uncompressed file option for reports that consist of multiple files, such as HTML pages with graphs, only the HTML pages are sent: the files for the graphs are not sent.

Glossary

For more detailed information on any term in this glossary, search for the term in *Help*.

Advanced Policy Engine

Advanced Policy Engine is a license-enabled scanning feature that performs checks for compliance with Federal Desktop Core Configuration (FDCC), United States Government Configuration Baseline (USGCB), and other configuration policies. For information about other tools related to compliance with FDCC configuration policies, see *What are your compliance goals?* in the *administrator's guide*.

API (application programming interface)

An API is a function that a developer can integrate with another software application by using program calls. The term *API* also refers to one of two sets of XML APIs, each with its own included operations: API v1.1 and Extended API v1.2. To learn about each API, see the API documentation, which you can download from the *Support* page of Help.

Appliance

An Appliance is a set of Nexpose components shipped as a dedicated hardware/software unit. Appliance configurations include a Security Console/Scan Engine combination and an Scan Engine-only version.

Asset

An asset is a single device on a network that the application discovers during a scan. In the Web interface and API, an asset may also be referred to as a *device*. See *Managed asset* on page 45 and *Unmanaged asset* on page 50. An asset's data has been integrated into the scan database, so it can be listed in sites and asset groups. In this regard, it differs from a *node*. See *Node* on page 45.

Asset group

An asset group is a logical collection of managed assets to which specific members have access for creating or viewing reports or tracking remediation tickets. An asset group may contain assets that belong to multiple sites or other asset groups. An asset group is either static or dynamic. An asset group is not a site. See *Site* on page 48. See *Dynamic asset group* on page 43 and *Static asset group* on page 49.

Asset Owner

Asset Owner is one of the preset roles. A user with this role can view data about discovered assets, run manual scans, and create and run reports in accessible sites and asset groups.

Asset search filter

An asset search filter is a set of criteria with which a user can refine a search for assets to include in a dynamic asset group. An asset search filter is different from a *vAsset discovery filter* on page 50.

Authentication

Authentication is the process of a security application verifying the logon credentials of a client or user that is attempting to gain access. By default the application authenticates users with an internal process, but you can configure it to authenticate users with an external LDAP or Kerberos source.

Average risk

Average risk is a setting in risk trend report configuration. It is based on a calculation of your risk scores on assets over a report date range. For example, average risk gives you an overview of how vulnerable your assets might be to exploits whether it's high or low or unchanged. Some assets have higher risk scores than others. Calculating the average score provides a high-level view of how vulnerable your assets might be to exploits.

Benchmark

In the context of scanning for FDCC policy compliance, a benchmark is a combination of policies that share the same source data. Each policy in the Advanced Policy Engine contains some or all of the rules that are contained within its respective benchmark. See *Federal Desktop Core Configuration (FDCC)* on page 44 and *United States Government Configuration Baseline (USGCB)* on page 49.

Breadth

Breadth refers to the total number of assets within the scope of a scan.

Category

In the context of scanning for FDCC policy compliance, a category is a grouping of policies in the Advanced Policy Engine configuration for a scan template. A policy's category is based on its source, purpose, and other criteria. See *Advanced Policy Engine* on page 41, *Federal Desktop Core Configuration (FDCC)* on page 44, and *United States Government Configuration Baseline (USGCB)* on page 49.

Command console

The command console is a page in the Security Console Web interface for entering commands to run certain operations. When you use this tool, you can see real-time diagnostics and a behind-the-scenes view of Security Console activity. To access the command console page, click the **Run console commands** link next to the *Troubleshooting* item on the *Administration* page.

Common Configuration Enumeration (CCE)

Common Configuration Enumeration (CCE) is a standard for assigning unique identifiers known as CCEs to configuration controls to allow consistent identification of these controls in different environments. CCE is implemented as part of its compliance with SCAP criteria for an Unauthenticated Scanner product.

Common Platform Enumeration (CPE)

Common Platform Enumeration (CPE) is a method for identifying operating systems and software applications. Its naming scheme is based on the generic syntax for Uniform Resource Identifiers (URI). CCE is implemented as part of its compliance with SCAP criteria for an Unauthenticated Scanner product.

Common Vulnerabilities and Exposures (CVE)

The Common Vulnerabilities and Exposures (CVE) standard prescribes how the application should identify vulnerabilities, making it easier for security products to exchange vulnerability data. CVE is implemented as part of its compliance with SCAP criteria for an Unauthenticated Scanner product.

Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System (CVSS) is an open framework for calculating vulnerability risk scores. CVSS is implemented as part of its compliance with SCAP criteria for an Unauthenticated Scanner product.

Compliance

Compliance is the condition of meeting standards specified by a government or respected industry entity. The application tests assets for compliance with a number of different security standards, such as those mandated by the Payment Card Industry (PCI) and those defined by the National Institute of Standards and Technology (NIST) for Federal Desktop Core Configuration (FDCC).

Continuous scan

A continuous scan starts over from the beginning if it completes its coverage of site assets within its scheduled window. This is a site configuration setting.

Depth

Depth indicates how thorough or comprehensive a scan will be. Depth refers to level to which the application will probe an individual asset for system information and vulnerabilities.

Discovery (scan phase)

Discovery is the first phase of a scan, in which the application finds potential scan targets on a network. Discovery as a scan phase is different from *vAsset discovery* on page 50.

Dynamic asset group

A dynamic asset group contains scanned assets that meet a specific set of search criteria. You define these criteria with asset search filters, such as IP address range or operating systems. The list of assets in a dynamic group is subject to change with every scan or when vulnerability exceptions are created. In this regard, a dynamic asset group differs from a static asset group. See *Asset group* on page 41 and *Static asset group* on page 49.

Dynamic Scan Pool

The Dynamic Scan Pool feature allows you to use Scan Engine pools to enhance the consistency of your scan coverage. A Scan Engine pool is a group of shared Scan Engines that can be bound to a site so that the load is distributed evenly across the shared Scan Engines. You can configure scan pools using the Extended API v1.2.

Dynamic site

A dynamic site is a collection of assets that are targeted for scanning and that have been discovered through vAsset discovery. Asset membership in a dynamic site is subject to change if the discovery connection changes or if filter criteria for asset discovery change. See *Static site* on page 49, *Site* on page 48, and *vAsset discovery* on page 50.

Exploit

An exploit is an attempt to penetrate a network or gain access to a computer through a security flaw, or vulnerability. Malicious exploits can result in system disruptions or theft of data. Penetration testers use benign exploits only to verify that vulnerabilities exist. The Metasploit product is a tool for performing benign exploits. See *Metasploit* on page 45. See *Published exploit* on page 46.

Exposure

An exposure is a vulnerability, especially one that makes an asset susceptible to attack via malware or a known exploit.

Extensible Configuration Checklist Description Format (XCCDF)

As defined by the National Institute of Standards and Technology (NIST), Extensible Configuration Checklist Description Format (XCCDF) “is a specification language for writing security checklists, benchmarks, and related documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring.” Advanced Policy Engine checks for FDCC policy compliance are written in this format.

False positive

A false positive is an instance in which the application flags a vulnerability that doesn't exist. A false negative is an instance in which the application fails to flag a vulnerability that does exist.

Federal Desktop Core Configuration (FDCC)

The Federal Desktop Core Configuration (FDCC) is a grouping of configuration security settings recommended by the National Institute of Standards and Technology (NIST) for computers that are connected directly to the network of a United States government agency. The Advanced Policy Engine provides checks for compliance with these policies in scan templates. Performing these checks requires a license that enables the Advanced Policy Engine feature and FDCC scanning.

Global Administrator

Global Administrator is one of the preset roles. A user with this role can perform all operations that are available in the application and they have access to all sites and asset groups.

Host

A host is a physical or virtual server that provides computing resources to a guest virtual machine. In a high-availability virtual environment, a host may also be referred to as a node. The term *node* has a different context in the application. See *Node* on page 45.

Latency

Latency is the delay interval between the time when a computer sends data over a network and another computer receives it. Low latency means short delays.

Malware

Malware is software designed to disrupt or deny a target systems's operation, steal or compromise data, gain unauthorized access to resources, or perform other similar types of abuse. The application can determine if a vulnerability renders an asset susceptible to malware attacks.

Malware kit

Also known as an exploit kit, a malware kit is a software bundle that makes it easy for malicious parties to write and deploy code for attacking target systems through vulnerabilities.

Managed asset

A managed asset is a network device that has been discovered during a scan and added to a site's target list, either automatically or manually. Only managed assets can be checked for vulnerabilities and tracked over time. Once an asset becomes a managed asset, it counts against the maximum number of assets that can be scanned, according to your license.

Manual scan

A manual scan is one that you start at any time, even if it is scheduled to run automatically at other times. Synonyms include *ad-hoc scan* and *unscheduled scan*.

Metasploit

Metasploit is a product that performs benign exploits to verify vulnerabilities. See *Exploit* on page 44.

MITRE

The MITRE Corporation is a body that defines standards for enumerating security-related concepts and languages for security development initiatives. Examples of MITRE-defined enumerations include Common Configuration Enumeration (CCE) and Common Vulnerability Enumeration (CVE). Examples of MITRE-defined languages include Open Vulnerability and Assessment Language (OVAL). A number of MITRE standards are implemented, especially in verification of FDCC compliance.

National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce. The agency mandates and manages a number of security initiatives, including Security Content Automation Protocol (SCAP). See *Security Content Automation Protocol (SCAP)* on page 48.

Node

A node is a device on a network that the application discovers during a scan. After the application integrates its data into the scan database, the device is regarded as an *asset* that can be listed in sites and asset groups. See *Asset* on page 41.

Open Vulnerability and Assessment Language (OVAL)

Open Vulnerability and Assessment Language (OVAL) is a development standard for gathering and sharing security-related data, such as FDCC policy checks. In compliance with an FDCC requirement, each OVAL file that the application imports during configuration policy checks is available for download from the *SCAP* page in the Security Console Web interface.

Override

An override is a change made by a user to the result of a check for compliance with a configuration policy rule. For example, a user may override a Fail result with a Pass result.

Payment Card Industry (PCI)

The Payment Card Industry (PCI) is a council that manages and enforces the PCI Data Security Standard for all merchants who perform credit card transactions. The application includes a scan template and report templates that are used by Approved Scanning Vendors (ASVs) in official merchant audits for PCI compliance.

Permission

A permission is the ability to perform one or more specific operations. Some permissions only apply to sites or asset groups to which an assigned user has access. Others are not subject to this kind of access.

Policy

A policy is a set of primarily security-related configuration guidelines for a computer, operating system, software application, or database. Compliance is verified with a number of different policies, including those encompassed in the United States Government Configuration Baseline (USGCB) and the Federal Desktop Core Configuration (FDCC). See *Advanced Policy Engine* on page 41, *Federal Desktop Core Configuration (FDCC)* on page 44, *United States Government Configuration Baseline (USGCB)* on page 49, *United States Government Configuration Baseline (USGCB)* on page 49, and *Scan* on page 47.

Policy Result

In the context of FDCC policy scanning, a result is a state of compliance or non-compliance with a rule or policy. Possible results include *Pass*, *Fail*, or *Not Applicable*.

Policy Rule

A rule is one of a set of specific guidelines that make up an FDCC configuration policy. See *Federal Desktop Core Configuration (FDCC)* on page 44, *United States Government Configuration Baseline (USGCB)* on page 49, and *Policy* on page 46.

Published exploit

In the context of the application, a published exploit is one that has been developed in Metasploit or listed in the Exploit Database. See *Exploit* on page 44.

Real Risk strategy

Real Risk is one of the built-in strategies for assessing and analyzing risk. It is also the recommended strategy because it applies unique exploit and malware exposure metrics for each vulnerability to Common Vulnerability Scoring System (CVSS) base metrics for likelihood (access vector, access complexity, and authentication requirements) and impact to affected assets (confidentiality, integrity, and availability). See *Risk strategy* on page 47.

Risk

In the context of vulnerability assessment, risk reflects the likelihood that a network or computer environment will be compromised, and it characterizes the anticipated consequences of the compromise, including theft or corruption of data and disruption to service. Implicitly, risk also reflects the potential damage to a compromised entity's financial well-being and reputation.

Risk score

A risk score is a rating that the application calculates for every asset and vulnerability. The score indicates the potential danger posed to network and business security in the event of a malicious exploit. You can configure the application to rate risk according to one of several built-in risk strategies, or you can create custom risk strategies.

Risk strategy

A risk strategy is a method for calculating vulnerability risk scores. Each strategy emphasizes certain risk factors and perspectives. Four built-in strategies are available: *Real Risk strategy* on page 47, *TemporalPlus risk strategy* on page 49, *Temporal risk strategy* on page 49, and *Weighted risk strategy* on page 51. You can also create custom risk strategies.

Risk trend

A risk trend graph illustrates a long-term view of your assets' probability and potential impact of compromise that may change over time. Risk trends can be based on average or total risk scores. The highest-risk graphs in your report demonstrate the biggest contributors to your risk on the site, group, or asset level. Tracking risk trends helps you assess threats to your organization's standings in these areas and determine if your vulnerability management efforts are satisfactorily maintaining risk at acceptable levels or reducing risk over time. See *Average risk* on page 42 and *Total risk* on page 49.

Role

A role is a set of permissions. Five preset roles are available. You also can create custom roles by manually selecting permissions. See *Asset Owner* on page 41, *Security Manager* on page 48, *Global Administrator* on page 44, *Site Owner* on page 49, and *User* on page 50.

Scan

A scan is a process by which the application discovers network assets and checks them for vulnerabilities. See *Exploit* on page 44 and See *Vulnerability check* on page 51.

Scan credentials

Scan credentials are the user name and password that the application submits to target assets for authentication to gain access and perform deep checks. Many different authentication mechanisms are supported for a wide variety of platforms.

Scan Engine

The Scan Engine is one of two major application components. It performs asset discovery and vulnerability detection operations. Scan engines can be *distributed* within or outside a firewall for varied coverage. Each installation of the Security Console also includes a local engine, which can be used for scans within the console's network perimeter.

Scan template

A scan template is a set of parameters for defining how assets are scanned. Various preset scan templates are available for different scanning scenarios. You also can create custom scan templates. Parameters of scan templates include the following:

- methods for discovering assets and services
- types of vulnerability checks, including safe and unsafe
- Web application scanning properties
- verification of compliance with policies and standards for various platforms

Scheduled scan

A scheduled scan starts automatically at predetermined points in time. The scheduling of a scan is an optional setting in site configuration. It is also possible to start any scan manually at any time.

Security Console

The Security Console is one of two major application components. It controls Scan Engines and retrieves scan data from them. It also controls all operations and provides a Web-based user interface.

Security Content Automation Protocol (SCAP)

Security Content Automation Protocol (SCAP) is a collection of standards for expressing and manipulating security data. It is mandated by the U.S. government and maintained by the National Institute of Standards and Technology (NIST). The application complies with SCAP criteria for an Unauthenticated Scanner product.

Security Manager

Security Manager is one of the preset roles. A user with this role can configure and run scans, create reports, and view asset data in accessible sites and asset groups.

Site

A site is a collection of assets that are targeted for a scan. Each site is associated with a list of target assets, a scan template, one or more Scan Engines, and other scan-related settings. See *Dynamic site* on page 44 and *Static site* on page 49. A site is not an asset group. See *Asset group* on page 41.

Site Owner

Site Owner is one of the preset roles. A user with this role can configure and run scans, create reports, and view asset data in accessible sites.

Static asset group

A static asset group contains assets that meet a set of criteria that you define according to your organization's needs. Unlike with a dynamic asset group, the list of assets in a static group does not change unless you alter it manually. See *Dynamic asset group* on page 43.

Static site

A static site is a collection of assets that are targeted for scanning and that have been manually selected. Asset membership in a static site does not change unless a user changes the asset list in the site configuration. For more information, see *Dynamic site* on page 44 and *Site* on page 48.

Temporal risk strategy

One of the built-in risk strategies, Temporal indicates how time continuously increases likelihood of compromise. The calculation applies the age of each vulnerability, based on its date of public disclosure, as a multiplier of CVSS base metrics for likelihood (access vector, access complexity, and authentication requirements) and asset impact (confidentiality, integrity, and availability). Temporal risk scores will be lower than TemporalPlus scores because Temporal limits the risk contribution of partial impact vectors. See *Risk strategy* on page 47.

TemporalPlus risk strategy

One of the built-in risk strategies, TemporalPlus provides a more granular analysis of vulnerability impact, while indicating how time continuously increases likelihood of compromise. It applies a vulnerability's age as a multiplier of CVSS base metrics for likelihood (access vector, access complexity, and authentication requirements) and asset impact (confidentiality, integrity, and availability). TemporalPlus risk scores will be higher than Temporal scores because TemporalPlus expands the risk contribution of partial impact vectors. See *Risk strategy* on page 47.

Total risk

Total risk is a setting in risk trend report configuration. It is an aggregated score of vulnerabilities on assets over a specified period.

United States Government Configuration Baseline (USGCB)

The United States Government Configuration Baseline (USGCB) is an initiative to create security configuration baselines for information technology products deployed across U.S. government agencies. USGCB evolved from FDCC, which it replaces as the configuration security mandate in the U.S. government. The Advanced Policy Engine provides checks for Microsoft Windows 7, Windows 7 Firewall, and Internet Explorer for compliance with USGCB baselines. Performing these checks requires a license that enables the Advanced Policy Engine feature and USGCB scanning. See *Advanced Policy Engine* on page 41 and *Federal Desktop Core Configuration (FDCC)* on page 44.

Unmanaged asset

An unmanaged asset is a device that has been discovered during a scan but not correlated against a managed asset or added to a site's target list. The application is designed to provide sufficient information about unmanaged assets so that you can decide whether to manage them. An unmanaged assets does not count against the maximum number of assets that can be scanned according to your license.

Unsafe check

An unsafe check is a test for a vulnerability that can cause a denial of service on a target system. Be aware that the check itself can cause a denial of service, as well. It is recommended that you only perform unsafe checks on test systems that are not in production.

Update

An update is a released set of changes to the application. By default, two types of updates are automatically downloaded and applied:

- *Content* updates include new checks for vulnerabilities, patch verification, and security policy compliance. Content updates always occur automatically when they are available.
- *Product* updates include performance improvements, bug fixes, and new product features. Unlike content updates, it is possible to disable automatic product updates and update the product manually.

User

User is one of the preset roles. An individual with this role can view asset data and run reports in accessible sites and asset groups.

vAsset discovery

vAsset discovery is a process by which the application automatically discovers virtual assets through a connection with a vSphere server or virtual machine host. You can refine or limit asset discovery with criteria filters. See *vAsset discovery filter* on page 50 and *vConnection* on page 50. vAsset discovery is different from *Discovery (scan phase)* on page 43.

vAsset discovery filter

A vAsset discovery filter is a set of criteria refining or limiting vAsset discovery results. This type of filter is different from an *Asset search filter* on page 41.

vConnection

A vConnection is a connection that is initiated with a server that manages virtual machines in order to discover those assets. A Global Administrator can configure a vConnection. See *vAsset discovery filter* on page 50.

Vulnerability

A vulnerability is a security flaw in a network or computer.

Vulnerability check

A vulnerability check is a series of operations that are performed to determine whether a security flaw exists on a target asset.

Vulnerability exception

A vulnerability exception is the removal of a vulnerability from a report and from any asset listing table. Excluded vulnerabilities also are not considered in the computation of risk scores.

Weighted risk strategy

One of the built-in risk strategies, *Weighted* is based primarily on asset data and vulnerability types, and it takes into account the level of importance, or weight, that you assign to a site when you configure it. See *Risk strategy* on page 47.