



NeXpose Software Installation and Quick-start Guide

Document version 2.4

Copyright © 2010 Rapid7 LLC. Boston, Massachusetts, USA. All rights reserved. Rapid7 and NeXpose are trademarks of Rapid7, LLC. Other names appearing in this content may be trademarks of their respective owners.

Contents

- Revision history..... 3**
- About this guide..... 4**
 - Document conventions 4
 - Using the Help site and other documents..... 4
 - Contacting Technical Support..... 5
- About NeXpose 6**
 - Understanding what NeXpose does 6
 - Understanding NeXpose components..... 6
- NeXpose requirements..... 8**
 - Hardware requirements..... 8
 - Network activities and requirements 9
 - Officially supported platforms..... 9
 - Windows..... 9
 - Linux 9
 - Unofficially supported platforms..... 10
 - Windows..... 10
 - Linux 10
- Downloading installation items 11**
- Installing NeXpose in Windows environments 12**
 - Starting NeXpose in Windows..... 13
 - Making NeXpose start automatically when Windows starts..... 13
 - Removing NeXpose from Windows..... 13
- Installing NeXpose in Linux environments..... 14**
 - Ensuring that the installer file is not corrupted 14
 - Installing NeXpose in an Ubuntu environment..... 14
 - Manually installing necessary packages in Ubuntu..... 14
 - Running the NeXpose installer in Ubuntu 15
 - Starting NeXpose in Ubuntu..... 16
 - Installing NeXpose as a daemon in Ubuntu 16
 - Removing NeXpose in Ubuntu 17
 - Installing NeXpose in a Red Hat environment 17
 - Manually installing necessary packages in Red Hat..... 17
 - Ensuring that SELinux is disabled 18
 - Running the NeXpose installer in Red Hat..... 18
 - Starting NeXpose in Red Hat 19
 - Installing NeXpose as a daemon in Red Hat..... 19
 - Removing NeXpose in Red Hat..... 20
 - Installing NeXpose in a SUSE environment..... 20

Manually installing necessary packages in SUSE	20
Ensuring that AppArmor is disabled	21
Running the NeXpose installer in SUSE	21
Starting NeXpose in SUSE.....	22
Installing NeXpose as a daemon in SUSE	22
Removing NeXpose in SUSE	23
Getting started with NeXpose	24
Logging on to NeXpose.....	24
Navigating the NeXpose Security Console Home page	25
Using the search function in NeXpose	28
Using wizards in NeXpose.....	28
Setting a site and configuring a scan	29
Manually starting and stopping a scan	29
Viewing scan data.....	30
Creating asset groups.....	31
Creating reports from preset templates	31
Appendix: Opening the Windows firewall for NeXpose scans	34
Opening the firewall in a domain-joined environment.....	34
Opening the firewall in a stand-alone environment.....	35
Enabling settings in the Standard Profile of Windows Policy Editor.....	35
Starting Remote Registry	35
Additional steps in Windows Vista	36

Revision history

The current document version is 2.4

Revision Date	Version	Description
November 11, 2009	2.0	Verified, tested, and updated installation procedures. Updated document template.
November 25, 2009	2.1	Updated lists of required packages for Linux and instructions for using md5sum.
December 3, 2009	2.2	Updated system requirements.
March 8, 2009	2.3	Added note recommending 64-bit configuration.
June 21, 2010	2.4	Added quick-start instructions for using NeXpose and appendix on opening the Windows firewall. Also added note on where to download deprecated libstdc++5 package.

About this guide

Use this guide to help you to perform three tasks:

- installing the Windows or Linux version of NeXpose software
- starting NeXpose
- logging on to the NeXpose Security Console Web interface, with which you can perform all NeXpose functions

Document conventions

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

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

Procedural steps appear in a blue sans serif typeface.

Command examples appear in the Courier typeface in shaded boxes.

Generalized file names in command examples appear between box brackets. Example:

```
[installer_file_name]
```

Multiple options in commands appear between arrow brackets: Example: \$ /etc/init.d/[daemon_name] <start|stop|restart>

NOTES appear in shaded boxes.

Using the Help site and other documents

After you start NeXpose and log on to the NeXpose 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 how to perform all NeXpose functions:

- learning important NeXpose 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 NeXpose settings

- maintaining and troubleshooting NeXpose
- backing up and restoring the NeXpose database

You will find these documents useful, as well:

- *NeXpose Administrator's Guide*
- *NeXpose User's Guide*
- *NeXpose Reporting Guide*
- NeXpose API guides

You can download these documents from the *Support* page in NeXpose Help.

Contacting Technical Support

To contact Technical Support, send an e-mail to support@rapid7.com.

For additional contact information and resources, click the **Support** link on the NeXpose Security Console Web interface.

About NeXpose

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

Understanding what NeXpose does

NeXpose is a unified vulnerability 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 in NeXpose identify security weaknesses in all layers of a network computing environment, including operating systems, databases, applications, and files. NeXpose 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.

Understanding NeXpose components

NeXpose consists of two main components:

- **NeXpose Scan Engines** perform asset discovery and vulnerability detection operations. You can deploy scan engines outside your firewall, within your secure network perimeter, or inside your DMZ to scan any network *asset*.

DEFINITION: An asset is a device on your network that is identified by an IP address, such as a computer, router, or printer. Assets are what NeXpose scans. In the NeXpose Security Console Web interface, the words "asset" and "device" are used interchangeably. In some of NeXpose's report templates, assets are referred to as "nodes".

- The **NeXpose Security Console** communicates with NeXpose Scan Engines to start scans and retrieve scan information. All exchanges between the console and scan engines occur via 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 NeXpose scans an asset for the first time, the console creates a repository of information about that asset in its database. With each ensuing scan that includes that asset, the console updates the repository.

The console includes a Web-based interface for configuring and operating NeXpose. An authorized user can log on to this interface securely, using HTTPS, to perform any NeXpose-related task that his or her role permits. See the section titled *Understanding user roles and permissions in NeXpose* in the *NeXpose 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 console functions include generating user-configured reports and regularly downloading patches and other critical updates from the Rapid7 central update system.

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

NeXpose components are also available in a dedicated hardware/software combination called an *appliance*. Another option is to purchase remote scanning services from Rapid 7.

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

NeXpose requirements

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

Hardware requirements

A computer hosting NeXpose components should have the following configuration:

NeXpose Enterprise Edition	
server	dedicated server with no IPS, IDS, or virus protection
processor	2 GHz
RAM	4 GB (32-bit), 8 GB (64-bit)
disk space	80 GB + for a console/scan engine combination; 10 GB + for a scan engine only
network interface card (NIC)	100 Mbps

NOTE: The 64-bit configuration is recommended for enterprise-scale deployments. For smaller deployments, the 32-bit configuration may be sufficient.

NeXpose Community Edition	
server	dedicated server with no IPS, IDS, or virus protection
processor	2 GHz or greater
RAM	2 GB (32-bit), 4 GB RAM (64-bit)
disk space	10 GB +
network interface card (NIC)	100 Mbps

Network activities and requirements

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

Activity	Type of communication
manage scan activity on NeXpose 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; console accepts HTTPS requests over port 3780

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

Ideally there should be no firewalls or similar devices between a scan engine and its target assets. These devices interfere with the scanning process and can limit the accuracy of results. See *Appendix: Opening the Windows firewall for NeXpose scans* (on page 34).

Scanning may also require some flexibility in security policies. For more information, see the *NeXpose Administrator's Guide*.

Officially supported platforms

NeXpose can run in many operating environments. Rapid7 performs quality assurance testing on the following platforms:

Windows

- MS Windows Server 2003 SP2 / Server 2003 R2

NOTE: Rapid7 does not support installation on Windows XP because of an issue related to this operating system sending packets over raw sockets.

Linux

- Red Hat Enterprise Linux 5
- Ubuntu 8.04 LTS
- SUSE Linux Enterprise Server 10

Unofficially supported platforms

The Rapid7 Technical Support team will provide support for customers running unofficially supported platforms, but cannot provide quality assurance testing of those platforms prior to releasing updates.

Windows

- MS Windows Server 2003 SP1

Linux

- SUSE Enterprise Linux 9
- Red Hat Enterprise Linux 4
- Fedora 9 or later
- Debian 4.0 or later
- CentOS 4 or later
- Ubuntu 7.10 or later

NOTE: For HTML reporting on Linux, you must have an X Windows server installed or the X Virtual Frame Buffer (Xvfb) must be running.

Downloading installation items

If you purchased NeXpose or registered for an evaluation, Rapid7 sent you an e-mail that includes links for downloading items necessary for installation:

- NeXpose installers for all supported environments in 32-bit and 64-bit versions (.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

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

The e-mail also includes a product key, which you will use to activate your NeXpose license during installation.

Installing NeXpose in Windows environments

You must have local administrator rights in order to install NeXpose on a Windows host. The computer cannot be part of a domain and cannot have a local firewall running. Installation on a Windows domain controller is not supported.

1. Double-click the icon for the NeXpose installer.
2. The installer displays the NeXpose InstallShield Wizard. Click **Next** on the *Welcome* page.
3. The installer displays the end-user license agreement. Read it, and select the option for accepting the terms.
4. The installer displays the default installation directory, which is C:\Program Files\rapid7\nexpose. Click **Next** to accept the default.

OR

If you want to use a different directory, delete the default directory, and type the preferred path in the text box. Then, click **Next**.

OR

Click **Browse** to open an explorer and locate a preferred directory. When you find that directory, click **Open** in the explorer. The path appears in the **Directory Name** text box of the installer wizard. Note the directory you selected. Click **Next**.

5. The installer displays two options for an installation type. If you want to install a NeXpose Security Console that includes a NeXpose Scan Engine, select the **Typical** option. If you want to install the NeXpose Scan Engine only, select the second option. For information about these options, see *Understanding NeXpose components* (on page 6).
6. The installer displays a request for a product key, which you received in the Rapid7 e-mail that included links for installation items. See *Downloading installation items* (on page 11). Enter the product key. You will not be able to complete the installation without a product key. If you do not have one, send an e-mail to support@rapid7.com. After you enter the product key, click **NEXT**.
7. The installer displays a request for your name and company name. NeXpose includes this information when sending logs to Rapid7 Technical Support for troubleshooting. Enter the names, and click **NEXT**.
8. The installer displays a summary of installation details. If you want to change any details, click **Back** to go to the desired wizard page, make the change, and then return to the summary. When you approve of the installation details, click **Install**.

The installer displays a status bar and names of files that it is installing.

9. The installer displays a request for a user name and password. These will be the credentials for the NeXpose global administrator account. If you wish to change the user name from the default "nxadmin", type a new name.
10. Type a password, and retype it for confirmation.
NeXpose does not support recovery of credentials. If you forget your user name or password, you will have to reinstall NeXpose. Credentials are case-sensitive.

NOTE: You can change these credentials later in NeXpose. See *Navigating the NeXpose Security Console Home page* (on page 25).

11. Click **Finish**.
12. The installer displays a success message. Click **Finish**.

Starting NeXpose in Windows

1. To start the console in Windows, double-click the NeXpose Security Console server icon on the desktop:



If the icon isn't available, you can double-click the `nsc.bat` file to start the console. The file is located in the installation directory.

The startup process may take a few minutes the first time you start the console because NeXpose is initializing its database of vulnerabilities. You may log on to the NeXpose Security Console Web interface immediately after NeXpose has completed the startup process.

Making NeXpose start automatically when Windows starts

You can make NeXpose start automatically as a service when Windows starts. This eliminates the need for you start it manually.

1. Click the Windows **Start** button, and select **Run...**
2. In the *Run* dialog box, type `services.msc`, and click **OK**.
3. In the *Services* pane, double-click the icon for the NeXpose Security Console service.
4. From the drop-down list for **Startup type**: select "Automatic", and click **OK**.
5. Close *Services*.
6. Restart your computer. NeXpose starts automatically as a service.

Removing NeXpose from Windows

Each instance of NeXpose must be installed from scratch. If you need to reinstall NeXpose, you must first remove it. Multiple copies of the same instance of NeXpose on the same server will not function correctly and are not supported.

1. Stop the NeXpose server: Go to the NeXpose command prompt, type `quit`, and press **ENTER**.
2. Make sure that the NeXpose PostgreSQL service is no longer running: Open the Windows Command Prompt, and type `net stop nxpgsql`. If the service is still running, this command will stop it. Otherwise, the system will display a message that the service is no longer running.
3. Click the Windows **Start** button, and select **Run...**
4. In the *Run* dialog box, type `regedit`, and click **OK**.
5. In the Registry Editor, open the `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\` folder.
6. Delete the `NeXposeConsole` and `nxpgsql` folders.
7. Restart the computer.
8. Delete the NeXpose installation folder.

Installing NeXpose in Linux environments

While installation steps are generally similar on all supported Linux distributions, there are some variations. See the instructions for your specific Linux distribution.

For all distributions, you must have root privileges to install NeXpose. You can log on as root, begin each command with `sudo`, or run `sudo -i`.

Ensuring that the installer file is not corrupted

After you download the installation file and the md5sum file as described in *Downloading installation items* (on page 11), use the following procedure to ensure that the installer was not corrupted during the download. Rapid7 recommends this step to prevent installation problems.

1. Go to the directory that contains the NeXpose 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
```

3. 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 NeXpose in an Ubuntu environment

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

Make sure you have downloaded all items necessary for installation. See *Downloading installation items* (on page 11).

Manually installing necessary packages in Ubuntu

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

To verify that you have `apt-get`, run:

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

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

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

Following is a list of packages that must be installed on Ubuntu. While it is possible to specify all required packages in a single command, it is recommended that you run one `apt-get` for each package and use the following order.

Certain packages may be installed as dependencies of other packages.

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

- xvfb
- xfonts-base (usually installed as a dependency of xvfb)
- xfonts-75dpi
- xserver-xorg
- libxtst6
- libxp6
- libxt6 (usually installed as a dependency of xserver-xorg)
- ia32-libs (64-bit only)

NOTE: The libstdc++5 package has been deprecated and is no longer available in Ubuntu repositories. You can download it from the Debian packages Web site at <http://packages.debian.org/etch/libstdc++5>.

Running the NeXpose installer in Ubuntu

NOTE: Make sure that you install all necessary packages before running the NeXpose installer. Otherwise, the installation will fail.

After making sure that the required Linux packages are installed, take the following steps.

1. Go to the directory to which you downloaded NeXpose installer.
2. Change the permissions for the installation file to make it executable:

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

3. Start the NeXpose installer:

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

NOTE: If you are using a desktop interface such as KDE or Gnome, omit the `-console` flag. For the rest of the installation, follow the directions that appear in the interface display.

4. The installer displays a message that it will install NeXpose. Press **1** and then **ENTER** to continue.
5. The installer displays the end-user license agreement. Read each displayed section and press **ENTER** to continue.
6. At the end of the agreement, press **1** to accept the terms. Then press **0** to continue.
7. Press **1**, and then press **ENTER** to proceed to the next step.
8. The installer displays the default installation directory, which is `/opt/rapid7/nexpose`. Press **ENTER** to accept the default, or type a different directory, and then press **ENTER**.

NOTE: Make sure to note the installation directory.

9. Press **1**, and then press **ENTER** to proceed to the next step.
10. The installer displays two options for an installation type. If you want to install a NeXpose Security Console that includes a NeXpose Scan Engine, press **1** for the "Typical" option. If you want to install the NeXpose Scan Engine only, press **2**. For information about these options, see *Understanding NeXpose components* (on page 6).
11. Press **1**, and then press **ENTER** to proceed to the next step.
12. The installer displays a request for a product key, which you received in the Rapid7 e-mail that included links for installation items. See *Downloading installation items* (on page 11). Type the product key. You will not be able to complete the installation without a product key. If you do not have one, send an e-mail to support@rapid7.com. After you type the product key, press **ENTER**.

NOTE: You must enter the key with hyphens. The key is not case-sensitive.

13. Press **1**, and then press **ENTER** to proceed to the next step.
 14. The installer displays a request for your name. Type it, and press **ENTER**.
 15. The installer displays a request for your company name. Type it, and press **ENTER**.
 16. Press **1**, and then press **ENTER** to proceed to the next step..
 17. The installer displays details about the installation. Review them, and press **1** to continue. The installer displays the percent of the installation that has been completed.
 18. After the installation is complete, the installer displays a request for a user name for the NeXpose global administrator account. Press **ENTER** to accept the default name "nxadmin", or type a different name, and then press **ENTER**.
 19. The installer displays a request for a password. Type a password, and then press **ENTER**. Type the password again to confirm it, and press **ENTER**.

NeXpose does not support recovery of credentials. If you forget your user name or password, you will have to reinstall NeXpose. Credentials are case-sensitive.
- NOTE:** You can change these credentials later in NeXpose. See *Navigating the NeXpose Security Console Home page* (on page 25).
20. The installer displays a message that the installation is complete. Press **3**.
 21. The installer displays a message that it is executing the DBInitializer. After this process finishes, press **3** to complete the installation and exit the installer.

Starting NeXpose in Ubuntu

1. Make sure that you are in the NeXpose installation directory, which you selected during installation. See *Running the NeXpose installer in Ubuntu* (on page 15).
2. Go to the directory that contains the script that starts NeXpose:

```
$ cd [installation_directory]/nsc
```

3. Type the command to run the script:

```
$ ./nsc.sh
```

The startup process may take a few minutes the first time you start the console because NeXpose is initializing its database of vulnerabilities. You may log on to the NeXpose Security Console interface immediately after NeXpose has completed the startup process.

Installing NeXpose as a daemon in Ubuntu

Installing NeXpose as a daemon has two benefits: NeXpose can automatically start when the server starts, and will continue running even if the current user logs off.

1. Go to the directory that contains the nexposeconsole.rc file:

```
$ cd [installation_directory]/nsc
```

2. Open the nexposeconsole.rc file in your preferred text editing program.
3. Look for two consecutive lines that read:

```
#defines  
NXP_ROOT=/opt/rapid7/nexpose
```

The directory in the second line is the default installation directory.

4. If you did not use the default directory for installation, change the directory path to the one you chose:

```
#defines  
NXP_ROOT=[installation_directory]
```

5. Save and close the nexposeconsole.rc file.

6. Copy the nexposeconsole.rc file to the /etc/init.d directory, and give it the desired daemon name:

```
$ cp [installation_directory]/nexposeconsole.rc /etc/init.d/[daemon_name]
```

7. Ensure that the daemon can run:

```
$ chmod +x /etc/init.d/[daemon-name]
```

8. Make the daemon start when the operating systems starts:

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

Manually starting, stopping, or restarting NeXpose as a daemon

To manually start, stop, or restart NeXpose as a daemon:

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

Preventing the daemon from automatically starting with the host system

To prevent the NeXpose daemon from automatically starting when the host system starts:

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

Removing NeXpose in Ubuntu

Each instance of NeXpose must be installed from scratch. If you need to reinstall NeXpose, you must first remove it. Multiple copies of the same instance of NeXpose on the same server will not function correctly and are not supported.

To remove NeXpose:

```
$ rm -fr [installation_directory]
```

NOTE: Be careful to enter this command exactly as it appears.

Installing NeXpose in a Red Hat environment

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

Make sure you have downloaded all items necessary for installation. See *Downloading installation items* (on page 11).

You need a Red Hat Enterprise Linux license in order to install NeXpose.

Manually installing necessary packages in Red Hat

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

To verify that you have yum, run:

```
$ yum --version
```

To verify that you have RPM, run:

```
$ rpm -v
```

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

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

The following packages must be installed:

- compat-libstdc++-33.i386 (32-bit only)
- screen

Ensuring that SELinux is disabled

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

1. Open the SELinux configuration file in your preferred text editor, for example:

```
$ vi /etc/selinux/config
```

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

3. If the setting is `enabled`, 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
```

Running the NeXpose installer in Red Hat

NOTE: Make sure that you install all necessary packages before running the NeXpose installer. Otherwise, the installation will fail.

After making sure that the required Linux packages are installed, take the following steps.

1. Go to the directory to which you downloaded NeXpose installer.
2. Change the permissions for the installation file to make it executable:

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

3. Start the NeXpose installer:

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

NOTE: If you are using a desktop interface such as KDE or Gnome, omit the `-console` flag. For the rest of the installation, follow the directions that appear in the interface display.

4. The installer displays a message that it will install NeXpose. Press **1** and then **ENTER** to continue.
5. The installer displays the end-user license agreement. Read each displayed section and press **ENTER** to continue.
6. At the end of the agreement, press **1** to accept the terms. Then press **0** to continue.
7. Press **1**, and then press **ENTER** to proceed to the next step.
8. The installer displays the default installation directory, which is `/opt/rapid7/nexpose`. Press **ENTER** to accept the default, or type a different directory, and then press **ENTER**.

NOTE: Make sure to note the installation directory.

9. Press **1**, and then press **ENTER** to proceed to the next step.
10. The installer displays two options for an installation type. If you want to install a NeXpose Security Console that includes a NeXpose Scan Engine, press **1** for the "Typical" option. If you want to install the NeXpose Scan Engine only, press **2**. For information about these options, see *Understanding NeXpose components* (on page 6).

11. Press **1**, and then press **ENTER** to proceed to the next step.
12. The installer displays a request for a product key, which you received in the Rapid7 e-mail that included links for installation items. See *Downloading installation items* (on page 11). Type the product key. You will not be able to complete the installation without a product key. If you do not have one, send an e-mail to support@rapid7.com. After you type the product key, press **ENTER**.

NOTE: You must enter the key with hyphens. The key is not case-sensitive.

13. Press **1**, and then press **ENTER** to proceed to the next step.
14. The installer displays a request for your name. Type it, and press **ENTER**.
15. The installer displays a request for your company name. Type it, and press **ENTER**.
16. Press **1**, and then press **ENTER** to proceed to the next step..
17. The installer displays details about the installation. Review them, and press **1** to continue. The installer displays the percent of the installation that has been completed.
18. After the installation is complete, the installer displays a request for a user name for the NeXpose global administrator account. Press **ENTER** to accept the default name "nxadmin", or type a different name, and then press **ENTER**.
19. The installer displays a request for a password. Type a password, and then press **ENTER**. Type the password again to confirm it, and press **ENTER**.

NeXpose does not support recovery of credentials. If you forget your user name or password, you will have to reinstall NeXpose. Credentials are case-sensitive.

NOTE: You can change these credentials later in NeXpose. See *Navigating the NeXpose Security Console Home page* (on page 25).

20. The installer displays a message that the installation is complete. Press **3**.
21. The installer displays a message that it is executing the DBInitializer. After this process finishes, press **3** to complete the installation and exit the installer.

Starting NeXpose in Red Hat

1. Make sure that you are in the NeXpose installation directory, which you selected during installation. See *Running the NeXpose installer in Red Hat* (on page 18).
2. Go to the directory containing the script that starts NeXpose:

```
$ cd [installation_directory]/nsc
```

3. Type the command to run the script:

```
$ ./nsc.sh
```

The startup process may take a few minutes, especially the first time you start the console, since NeXpose is initializing its database of vulnerabilities. You may log on to the NeXpose Security Console interface immediately after NeXpose has completed the startup process.

Installing NeXpose as a daemon in Red Hat

Installing NeXpose as a daemon has two benefits: NeXpose can automatically start when the server starts, and it will continue running even if the current user logs off.

1. Go to the directory that contains the nexposeconsole.rc file:

```
$ cd [installation_directory]/nsc
```

2. Open the nexposeconsole.rc file in your preferred text editing program.

3. Look for two consecutive lines that read:

```
#defines
NXP_ROOT=/opt/rapid7/nexpose
```

The directory in the second line is the default installation directory.

4. If you did not use the default directory for installation, change the directory path to the one you chose:

```
#defines
NXP_ROOT=[installation_directory]
```

5. Save and close the nexposeconsole.rc file.

6. Copy the nexposeconsole.rc file to the /etc/init.d directory, and give it the desired daemon name:

```
$ cp [installation_directory]/nexposeconsole.rc /etc/init.d/[daemon_name]
```

7. Ensure that the daemon can run:

```
$ chmod +x /etc/init.d/[daemon_name]
```

8. Make the daemon start when the operating systems starts:

```
$ chkconfig --add [daemon_name]
```

Manually starting, stopping, or restarting NeXpose as a daemon

To manually start, stop, or restart NeXpose as a daemon:

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

Preventing the daemon from automatically starting with the host system

To prevent the NeXpose daemon from automatically starting when the host system starts:

```
$ chkconfig --del [daemon_name]
```

Removing NeXpose in Red Hat

Each instance of NeXpose must be installed from scratch. If you need to reinstall NeXpose, you must first remove it. Multiple copies of the same instance of NeXpose on the same server will not function correctly and are not supported.

To remove NeXpose:

```
$ rm -fr [installation_directory]
```

NOTE: Be careful to enter this command exactly as it appears.

Installing NeXpose in a SUSE environment

These steps apply to SUSE 10.0. There may be some variation on other versions of SUSE.

Make sure you have downloaded all items necessary for installation. See *Downloading installation items* (on page 11).

Manually installing necessary packages in SUSE

You need yast2 to install packages on SUSE.

To verify that you have yast2, run:

```
$ /sbin/yast2 -h
```

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

```
$ /sbin/yast2 --install [package_name]
```

The following packages must be installed:

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

Ensuring that AppArmor is disabled

AppArmor is a security-related feature that must be disabled before you can install NeXpose. The SUSE environment provides an easy removal method through its graphical user interface (GUI).

1. Start the GUI.
2. In the GUI, click **Computer**, then **Control Center** under *System* in the right pane.
3. Click **Open Administrator Settings** under *Common Tasks* in the left pane.
4. Enter the root password, and click **OK**.
5. The YaST Control Center opens. Click **Novell AppArmor** under *Groups* in the left pane.
6. Click **AppArmor Control Panel** under *Novell AppArmor* in the right pane.
7. Clear the check box labeled **Enable App Armor**, and then click **Done**.
8. From the command prompt, restart the operating system:

```
$ shutdown -r now
```

Running the NeXpose installer in SUSE

NOTE: Make sure that you install all necessary packages before running the NeXpose installer. Otherwise, the installation will fail.

After making sure that the required Linux packages are installed, take the following steps.

1. Go to the directory to which you downloaded NeXpose installer.
2. Change the permissions for the installation file to make it executable:

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

3. Start the NeXpose installer:

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

NOTE: If you are using a desktop interface such as KDE or Gnome, omit the `-console` flag. For the rest of the installation, follow the directions that appear in the interface display.

4. The installer displays a message that it will install NeXpose. Press **1** and then **ENTER** to continue.
5. The installer displays the end-user license agreement. Read each displayed section and press **ENTER** to continue.
6. At the end of the agreement, press **1** to accept the terms. Then press **0** to continue.
7. Press **1**, and then press **ENTER** to proceed to the next step.
8. The installer displays the default installation directory, which is `/opt/rapid7/nexpose`. Press **ENTER** to accept the default, or type a different directory, and then press **ENTER**.

NOTE: Make sure to note the installation directory.

9. Press **1**, and then press **ENTER** to proceed to the next step.

10. The installer displays two options for an installation type. If you want to install a NeXpose Security Console that includes a NeXpose Scan Engine, press **1** for the "Typical" option. If you want to install the NeXpose Scan Engine only, press **2**. For information about these options, see *Understanding NeXpose components* (on page 6).
11. Press **1**, and then press **ENTER** to proceed to the next step.
12. The installer displays a request for a product key, which you received in the Rapid7 e-mail that included links for installation items. See *Downloading installation items* (on page 11). Type the product key. You will not be able to complete the installation without a product key. If you do not have one, send an e-mail to support@rapid7.com. After you type the product key, press **ENTER**.

NOTE: You must enter the key with hyphens. The key is not case-sensitive.

13. Press **1**, and then press **ENTER** to proceed to the next step.
14. The installer displays a request for your name. Type it, and press **ENTER**.
15. The installer displays a request for your company name. Type it, and press **ENTER**.
16. Press **1**, and then press **ENTER** to proceed to the next step..
17. The installer displays details about the installation. Review them, and press **1** to continue. The installer displays the percent of the installation that has been completed.
18. After the installation is complete, the installer displays a request for a user name for the NeXpose global administrator account. Press **ENTER** to accept the default name "nxadmin", or type a different name, and then press **ENTER**.
19. The installer displays a request for a password. Type a password, and then press **ENTER**. Type the password again to confirm it, and press **ENTER**.
NeXpose does not support recovery of credentials. If you forget your user name or password, you will have to reinstall NeXpose. Credentials are case-sensitive.

NOTE: You can change these credentials later in NeXpose. See *Navigating the NeXpose Security Console Home page* (on page 25).

20. The installer displays a message that the installation is complete. Press **3**.
21. The installer displays a message that it is executing the DBInitializer. After this process finishes, press **3** to complete the installation and exit the installer.

Starting NeXpose in SUSE

1. Make sure that you are in the NeXpose installation directory, which you selected during installation. See *Running the NeXpose installer in SUSE* (on page 21).
2. Go to the directory that contains the script that starts NeXpose:

```
$ cd [installation_directory]/nsc
```

3. Type the command to run the script:

```
$ ./nsc.sh
```

The startup process may take a few minutes, especially the first time you start the console, since NeXpose is initializing its database of vulnerabilities. You may log on to the NeXpose Security Console interface immediately after NeXpose has completed the startup process.

Installing NeXpose as a daemon in SUSE

Installing NeXpose as a daemon has two benefits: NeXpose can automatically start when the server starts, and will continue running even if the current user logs off.

1. Go to the directory that contains the nexposeconsole.rc file:

```
$ cd [installation_directory]/nsc
```

2. Open the nexposeconsole.rc file in your preferred text editing program.
3. Look for two consecutive lines that read:

```
#defines  
NXP_ROOT=/opt/rapid7/nexpose
```

The directory in the second line is the default installation directory.

4. If you did not use the default directory for installation, change the directory path to the one you chose:

```
#defines  
NXP_ROOT=[installation_directory]
```

5. Save and close the nexposeconsole.rc file.
6. Copy the nexposeconsole.rc file to the /etc/init.d directory, and give it the desired daemon name:

```
$ cp [installation_directory]/nexposeconsole.rc /etc/init.d/[daemon_name]
```

7. Ensure that the daemon can run:

```
$ chmod +x /etc/init.d/[daemon-name]
```

8. Make the daemon start when the operating systems starts:

```
$ insserv [daemon_name]
```

Manually starting, stopping, or restarting NeXpose as a daemon in SUSE

To manually start, stop, or restart NeXpose as a daemon:

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

Preventing the daemon from automatically starting with the host system in SUSE

To prevent the NeXpose daemon from automatically starting when the host system starts:

```
$ innserv -r [daemon_name]
```

Removing NeXpose in SUSE

Each instance of NeXpose must be installed from scratch. If you need to reinstall NeXpose, you must first remove it. Multiple copies of the same instance of NeXpose on the same server will not function correctly and are not supported.

To remove NeXpose:

```
$ rm -fr [installation_directory]
```

NOTE: Be careful to enter this command exactly as it appears.

Getting started with NeXpose

After you have installed NeXpose, you can use it to find and report vulnerabilities in your environment. This section provides quick instructions for getting started:

- logging on to NeXpose
- becoming familiar with the Web interface
- setting up a site and configuring a scan
- starting and stopping a scan manually
- viewing scan data
- creating an asset group
- creating a report

For more detailed instructions, go to NeXpose Help, by clicking the **Help** link on any page of the Web interface. Click the **Support** link to view and download all NeXpose documentation.

Logging on to NeXpose

1. Start a Web browser. The NeXpose Security Console Web interface supports Microsoft Internet Explorer 7.x and Firefox 3.5 browsers. Other browsers may operate successfully with the interface.
2. If you are running the browser on the same computer as the console, go to the IP address 127.0.0.1, and specify port 3780. Make sure to indicate HTTPS protocol when entering the URL.

Example: `https://127.0.0.1:3780`

NOTE: If there is a usage conflict for port 3780, you may 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 NeXpose Security Console settings* in the *NeXpose Administrator's Guide*.

If you are running the browser on a separate computer, substitute `127.0.0.1` with the correct host name IP address.

NOTE: Browsers do not include non-English, UTF-8 character sets, such as those for Chinese languages, in their default installations. To use your browser with one of these languages, you must install the appropriate language pack. In the Windows version of Internet Explorer 7.0, you can add a language by selecting Internet Options from the Tools menu, and then clicking the Languages button in the Internet Options dialog box. In the Windows version of Firefox 2.0, select Options from the Tools menu and then clicked the Advanced icon in the Options dialog box. In the Languages pane, click **Choose...** to select a language to add.

3. When your browser displays the *Log in* box, enter your user name and password that you specified during installation. Click the **Login** button. User names and passwords are case-sensitive and non-recoverable.

NOTE: If the logon box indicates that the NeXpose 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 NeXpose in maintenance mode* in the *NeXpose Administrator's Guide*.

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 NeXpose global administrator must check the configuration for that source. See *Using external sources for user authentication* in the *NeXpose Administrator's Guide*. The problem may also indicate that the authentication server is down.

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

4. Click the **Home** link to view the NeXpose Security Console *Home* page.

5. Click the **Help** link on any page of the Web interface for information on how to use NeXpose.

Navigating the NeXpose Security Console Home page

When you log on to the NeXpose *Home* page for the first time, you see place holders for information, but no information contained in them. After installation, the only information in the NeXpose 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, based on NeXpose 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 console interface. Use these tabs to navigate to the main pages for each area of the interface.

NOTE: If the logged-on account is a security manager, site administrator, or system administrator, only the information for accessible sites and asset groups will be visible. If the logged in account is a nonadministrative user, only tickets and asset groups will be visible on the Home page. Nonadministrative users do not have access to sites.

- 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 *Tickets* page lists remediation tickets and their status.
- The *Reports* page lists all reports generated by NeXpose and provides controls for editing and creating report templates.
- The *Vulnerabilities* page lists all vulnerabilities discovered by NeXpose.
- The *Administration* page is the starting point for all management activities in NeXpose, 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 site, 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. See instructions following this table.
	Reverse the sort order of listed items in a given column. You also can click column headings to produce the same affect.
	Generate a Microsoft Excel spreadsheet of any listed site, asset group, or ticket.
	Start a manual scan.
	Pause a scan.
	Resume a scan.
	Stop a scan.
	Edit properties for a site, report, or user account.
	Preview a report template.
	Delete a site, report, or user account.
	Exclude a vulnerability from a report.
Help link	View NeXpose Help.
News link	View the <i>News</i> page, which lists all updates to the installed NeXpose system.
Log Out link	Log out of the NeXpose Security Console interface. The console then displays the <i>Log In</i> box. For security reasons, NeXpose 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 <i>User Configuration</i> wizard, in which 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 NeXpose database for assets, asset groups, and vulnerabilities.

For the *Home* page and any other page on the site that displays data, you can make closed panes visible by clicking the **Customize dashboard** link on the left side of the tab bar. A list of closed panes appears. Click the plus icon for any panes that you wish to make visible, and then click **Close**.

Keep this feature in mind when you go to a page of the interface that does not seem to be displaying any data.

Wherever you go on the console interface, you can check and change your location by using the breadcrumbs that appear in the upper-left corner of every page.

Using the search function in NeXpose

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

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

NeXpose displays the *Search* page, which lists results in various categories. Within each category pane, NeXpose 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 wizards in NeXpose

NeXpose provides wizards 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 NeXpose Security Console settings
- troubleshooting and maintaining NeXpose

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

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

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

Setting a site and configuring a scan

You must set up at least one *site* containing at least one *asset* in order to run scans in NeXpose. Make sure that you have a NeXpose Scan Engine running and paired with the NeXpose Security Console beforehand. See the topic *Setting up NeXpose Scan Engines* in NeXpose Help.

DEFINITION: A site is a physical group of assets assembled for a scan by a specific, dedicated scan engine. The grouping principle may be something meaningful to you, such as a common geographic location or a range of IP addresses. Or, you may organize a site for a specific type of scan.

The Web interface provides wizards for all key NeXpose activities, including site creation. You can either use the navigation buttons in the upper-right corner of each wizard page to progress through each page, or you can click a page link listed on the left column to go directly to that page. To save configuration changes, click the **Save** button that appears on every page. To discard changes, click the **Cancel** button. Parameters labeled in red denote required parameters on all wizard pages.

1. Click the **New Site** button on the *Home* page. This opens the Site Configuration wizard.
2. On the *Site Configuration – General* page, enter a name and description for your site. Select a level of importance, which corresponds to a risk factor that NeXpose uses to calculate a risk index for each site.
3. Go to the *Devices* page. You can manually enter addresses and host names. You also can import a comma- or new-line-delimited ASCII-text file that lists IP address and host names of assets you want to scan. To prevent assets within an IP address range from being scanned, manually enter addresses and host names in the text box labeled *Devices to Exclude* from scanning; or import a comma- or new-line-delimited ASCII-text file that lists addresses and host names that you don't want to scan.
4. Go to the *Scan Setup* page to select a scan template and/or scan engine other than the default settings. A scan template is a predefined set of scan attributes that you can select quickly rather than manually define properties, such as port scan methods and targeted vulnerabilities. See the following topics in NeXpose Help for more information:
 - *Specifying scan settings* for a comparison of preset scan templates that are offered with NeXpose
 - *Working with scan templates* for information on how to customize templates.
5. If you want to schedule scans to run automatically, select the check box labeled **Enable schedule**. Then select schedule settings.
6. Alerts make you aware of important scan events, such as the discovery of certain vulnerabilities. If you want NeXpose to send alerts, go to the *Alerting* page and click the **New Alert** button, and edit and select settings according to your preferences. 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 NeXpose Help.
7. Credentials enable NeXpose 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. If you want to set up credentials for your scan, go to the *Credentials* page and click **New Login**. The steps for setting up credentials depend on the type of system you want to access. See *Establishing scan credentials* in NeXpose Help.
8. To save configuration changes, click the **Save** button that appears on every page. To discard changes, click the **Cancel** button.

Manually starting and stopping a scan

Once you set up a site, you can run a manual scan regardless of whether or not you scheduled scans to run automatically for that site.

1. Click the **New Manual Scan** icon for a given site in the *Site Listing* pane of the *Home* page.
OR
Click the **New Manual Scan** button on the *Sites* page or on the page for a specific site.
2. The console displays the *Start New Scan* dialog box, which lists all the assets that you specified in the site configuration for NeXpose to scan, or to exclude from the scan. Select either the option to scan all assets within the scope of a site, or to specify certain target assets.
3. If you select the latter, enter their IP addresses or host names in the text box.
4. Click the **Start Now** button to begin the scan immediately.

You can view the status of any currently running scan in several areas:

- the *Home* page
- the *Sites* page
- the page for the site that is being scanned
- the page for the actual scan

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

To pause a scan, click the **Pause** icon for the scan on the *Home*, *Sites*, or specific site page; or click the **Pause Scan** button on the specific scan page. NeXpose displays a message, asking you to confirm that you want to pause the scan. Click **OK**.

To resume a paused scan, click the **Resume** icon for the scan on the *Home*, *Sites*, or specific site page; or click the **Resume Scan** button on the specific scan page. NeXpose displays a message, asking you to confirm that you want to resume the scan. Click **OK**.

To stop a scan, click the **Stop** icon for the scan on the *Home*, *Sites*, or specific site page; or click the **Stop Scan** button on the specific scan page. NeXpose displays a message, asking you to confirm that you want to stop the scan. Click **OK**.

The stop operation may take 30 seconds or more to complete pending any in-progress scan activity.

Viewing scan data

The NeXpose 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 would like 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

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 console interface. The console displays the *Vulnerabilities* page.

For every displayed vulnerability, NeXpose displays a set of metrics that indicate the danger that this vulnerability poses to your network security. For information about these metrics, see [Viewing active vulnerabilities in NeXpose Help](#).

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 NeXpose 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 NeXpose 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.

NOTE: You can only create an asset group after running an initial scan of assets that you wish to include in that group.

1. Click the **New Asset Group** button on the *Home* page.
2. On the *Group Configuration—General* page, type a name and description for the new asset group.
3. Go to the *Group Members* page, and click the **Select Users...** button. Click the check box for each user that you wish to add to the group. Then, click the **Save** button.
4. Go to the *Assets* page and click the **Select Devices...** button. The console displays a list of all your organization's assets, as defined when sites were created. You can page through the list, or you can search for specific assets by IP address range, device name, site, or operating system. To do the latter, type and or select the desired search criteria and click the **Apply Filter** button. NeXpose applies all filter settings. The console displays a list of search results.
5. Click the check boxes for each asset that you wish to add to the group. Then, click the **Save** button. The selected assets appear on the *General* page.
6. After you finish configuring your new asset group, click the **Save** button that appears on every page of wizard.

Creating reports from preset templates

You can create a variety of reports based on scan data. NeXpose templates enable you to initiate reports that focus on vulnerabilities, specific risk levels of vulnerabilities, remediation plans, policy evaluation, PCI compliance, or other criteria. Template attributes include options for exporting reports to external databases or formatting them for Web-based viewing. In addition to using pre-made templates, you can create custom report templates (see [Creating a custom report template](#) in NeXpose Help).

As with setting up sites and scans, the Web interface provides a wizards setting up reports.

1. Click the **New Report** button on the *Reports* page. The console displays the *General* page of the *Report Configuration* wizard.
2. Enter a name for the new report, which will be unique in NeXpose. Select a format.
3. Select a report format. To learn about formats, see [Specifying general report attributes](#) in NeXpose Help.

NOTE: If you select *Database Export* as your report format, the *Report Configuration—Output* page of the wizard contains fields specifically for transferring scan data to a database. You have an external, JDBC-compliant database available in order to use the Database Export format.

4. Select a template from the dropdown list. Click the **Browse Templates** button to view information about each template. In the *Browse Templates* dialog box, you can click the **Preview** icon for any template to view a sample. For more information about scan templates, see [Specifying general report attributes](#) in NeXpose Help.

5. Select a time zone for reports.
6. Go to the *Content* page. Select a NeXpose account user name from the **Asset owner** dropdown to assign that user or administrator ownership of the new report. Only global administrators can assign report ownership to other administrators or users. If a nonadministrative user is creating the report, that user will be the owner.
7. Select assets to be included in the report. You can select entire sites or asset groups by clicking those respective buttons, or you can select individual assets by clicking the **Select devices...** button. These choices are not mutually exclusive; you can combine selections of sites, asset groups, and individual assets. If you click the **Select devices...** button, the console displays a list of all your organization's assets, as defined when sites were created. You can page through the list...

...or you can search for specific assets by IP address range, device name, site, or operating system. To do the latter, type and/or select the desired search criteria and click the **Apply Filter** button. NeXpose applies all filter settings. 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.

If you want to use only the most recent scan data in your report, click the check box for that option. Otherwise, NeXpose will include all historical scan data in the report.

8. You can configure NeXpose to generate reports automatically on a schedule. Doing this is a good idea if you have an asset group containing assets that are assigned to many different sites, each with a different scan template. Since these assets will be scanned frequently, it makes sense to generate reports automatically. Go to the *Report Configuration—Schedule* page. If you wish to produce a report manually, on the spot, click the radio button labeled **This time only**. If you want NeXpose to generate a report every time it successfully completes a scan of any one asset, click the radio button labeled **After each scan**.

If you want to schedule reports for regular time intervals, click the option button labeled **On the following schedule**. 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. To set a time interval for repeating the report, type a value in the field labeled **Repeat every** and select a time unit. If you wish to run a report only once, type "0" in the field labeled **Repeat every**.

9. If you want users to view reports without going to the NeXpose Security Console, do one of the following actions:

Store reports in user directories

You can store copies of reports in specific user directories of the file system. Users with access to those directories can view the reports immediately after they are created. Go to the *Report Configuration—Output* page. Click the check box labeled **Store reports in NeXpose**. Type the path of the desired user directory using a canonical naming convention, in which variables replace certain absolute values. See the example displayed on the *Output* page for reference.

NOTE: In order to store copies of reports in specific user directories, you must create custom directories within the NeXpose directory structure beforehand. See *Storing reports in user directories* in NeXpose Help.

Configure database export settings

You can export report data to an external database. To do so, you have to select Database Export as your report format in step 3.

Select the database type from the dropdown list of the *Output* page. Enter the IP address and port of the database server. Enter a name for the database. Then, enter the administrative user ID and password for logging on to that database. After NeXpose completes a scan, check the database to make sure that the scan data has populated the tables.

Have NeXpose send reports via e-mail

You also can configure NeXpose to distribute reports via e-mail as a URL link or an attachment. Go to the *Report Configuration—Distribution* page. Select the check box labeled **Send E-mail**. Click an option button for attaching the report as a URL, an uncompressed file (*File*), or a zipped file.

NOTE: Selecting the uncompressed file option is not recommended for reports that consist of multiple files, such as HTML pages with graphs. If such a report is attached without being zipped, NeXpose will send only the HTML page and not the graph files.

If you want to e-mail reports to NeXpose users with access to the assets included into the report, click the appropriate check box. This is a convenient way to distribute reports automatically to users who are responsible for remediation of vulnerabilities. Type all other desired recipient e-mail addresses. Then, type the e-mail address of the sender.

NOTE: You may require an SMTP relay server for one of several reasons. For example, a firewall may prevent NeXpose 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, NeXpose searches for a suitable mail server for sending reports. Also NeXpose regards the mail sender address as the "originator" of e-mailed reports.

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

Appendix: Opening the Windows firewall for NeXpose scans

You can open your Windows firewall to make it possible for NeXpose to perform deep scans within your network.

By default, Microsoft Windows XP SP2, Vista, Server 2003, and Server 2008 enable the firewall to block incoming TCP/IP packets. Maintaining this setting is generally a smart security practice. However, an enabled firewall restricts NeXpose to do nothing more than discover network assets during a scan.

Opening a firewall gives NeXpose access to critical, security-related data, such as what you would require for patch or compliance checks. Read the following procedure to learn how to open the firewall for NeXpose scans, *without disabling it completely*. Typically, a domain administrator would perform these steps.

Opening the firewall in a domain-joined environment

The steps in this section are for an Active Directory environment, in which Windows workstations are members of a domain. During a network logon, a workstation obtains policy settings that create firewall exceptions from the domain controller.

Two settings must be enabled in the group policy settings for the domain in question:

Windows Firewall: Allow remote administration exception

and

Windows Firewall: Allow file and print sharing exception

1. In Windows, click the **Start** button and select **Administrative Tools | Active Directory Users and Computers**.
2. In the *Active Directory Users and Computers* window, right-click the name of the domain in which you wish to open the firewall. From the pop-menu select **Properties**.
3. In the *Properties* window for the selected domain, click the domain policy that you wish to edit, and click **Edit**.
4. In the left navigation pane of the *Group Policy Settings* window, click the *Domain Profile* folder, which is located in the directory path *Computer Configuration | Administrative Templates | Network | Network Connections | Windows Firewall*.
5. After you open the *Domain Profile* folder, find **Windows Firewall: Allow file and printer sharing exception** in the right pane, and double-click it to open the setting dialogue box.
6. In the *Setting* tab of the dialogue box, click the **Enabled** radio button, and then click **OK**.
7. In the right pane of the group policy window, find **Windows Firewall: Allow remote administration exception**. Double-click it to open the setting dialogue box.
8. In the *Setting* tab of the dialogue box, click the **Enabled** radio button.

9. In the text field labeled *Allow unsolicited incoming messages from*;, type the IP address of the NeXpose Scan Engine or network from which scans will originate. Click **OK**.

NOTE: While some parties recommend an additional step of opening port 135, doing so may not produce any significantly different results. Rapid7 recommends keeping port 135 closed and protecting it with the firewall unless there is a specific reason to open it.

You can find useful general information about managing the Windows firewall through group policy settings at www.bookpool.com/ct/165.

Opening the firewall in a stand-alone environment

The steps in this section are for stand-alone configurations of Windows Vista and Windows XP, in which a Windows workstation is not a member of a domain and is not controlled by policy settings.

Enabling settings in the Standard Profile of Windows Policy Editor

Click **Start**, open the *Run* dialog box, and type `gpedit.msc` to start Windows Group Policy Editor.

In Vista, you can alternatively start Windows Group Policy Editor by typing the command from the *Start Search* box. This displays an icon that you can click to start the editor.

In the left pane of Group Policy Editor, go to Local Computer Policy | Administrative Templates | Network | Network Connections | Windows Firewall.

Two settings in *Standard Profile* must have an "Enabled" state for NeXpose to communicate with the firewall:

Allow inbound file and printer sharing exception

and

Allow inbound remote remote administration exception

Double-click the *Allow inbound file and printer sharing exception* in *Standard Profile*.

In the dialog box for that setting, click the **Enabled** option button.

In the box labeled *Allow unsolicited incoming messages from these IP addresses*;, type either an asterisk (*) or the IP address of the host where the scan engine is located.

Click **OK**.

Double-click the *Allow inbound remote administration exception* in *Standard Profile*.

In the dialog box for that setting, click the **Enabled** option button.

In the box labeled *Allow unsolicited incoming messages from these IP addresses*;, type either an asterisk (*) or the IP address of the host where the scan engine is located.

Click **OK**.

All other settings in *Domain Profile* and *Standard Profile* must have a "Not Configured" state.

Starting Remote Registry

Starting Remote Registry makes it possible for NeXpose to fingerprint remote scan targets accurately.

1. Click **Start**, open the *Run* dialog box, and type `services.msc` to start the Services manager.
In Vista, you can alternatively start the Services manager by typing the command from the *Start Search* box. This displays an icon that you can click to start the manager.
2. In the right pane of the Services manager, look at the Remote Registry status. If it is "Started," you do not have to do anything.
If it is not "Started," double-click the setting name.
3. In the dialog box, click **Start**, and then click **OK**.

Additional steps in Windows Vista

If you are using Windows Vista, you must perform additional steps so that NeXpose can communicate with the firewall:

- making sure the setting *Prohibit use of Internet connection firewall on your DNS domain network* has a "Disabled" or "Not configured" state
- turning off User Account Control

To make sure that the firewall is not enabled...

1. Click **Start**, open the *Run* dialog box, and type `gpedit.msc` to start Windows Group Policy Editor.
OR
Type the `gpedit.msc` command in the *Start Search* box and then click the icon to start Windows Group Policy Editor. See *Opening the firewall in a stand-alone environment* (on page 35).
2. In the left pane of Group Policy Editor, go to Local Computer Policy | Administrative Templates | Network | Network Connections.
3. Look at the state of the setting *Prohibit use of Internet connection firewall on your DNS domain network* to verify that the state is "Not configured" or "Disabled." If it is, you do not have to do anything else.
If the state is "Enabled," double-click the setting. In the dialog box for that setting, click the **Disabled** or **Not configured** option button, and then click **OK**.

To turn off User Account Control...

1. Click **Start**, and then select **Control Panel**.
2. Click the link **User Accounts and Family Safety**.
3. Click the link **Turn User Account Control on or off**.
4. Click **User Accounts**
If the check box for turning on User Account Control is selected, clear the check box, and click **OK**. If it is not selected, you do not have to do anything and can click **Cancel**.
If you change this setting, you will have to restart Windows.