NeXpose Software Installation Guide

Document version 2.2

Copyright © 2009 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

Installation guide revision history

The current document version is 2.2

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.

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 are indented and appear in blue type.

```
Command examples appear in the Courier typeface in blue 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 blue 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:

- *Best Practices for Planning and Executing a NeXpose Deployment*
- *Best Practices for Tuning NeXpose Scan Performance*
- *Using the NeXpose API 1.0*
- *Opening the Windows Firewall for NeXpose Scans*

You can download these documents from the *Support* page in NeXpose Help. They are also available in the Rapid7 customer knowledge base.

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 Help site or NeXpose Manual. 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 or greater
RAM	2 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

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 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. Scanning may also require some flexibility in security policies. For more information, see the guide *Best Practices for Planning and Executing a NeXpose Deployment*.

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.

Double-click the icon for the NeXpose installer.

The installer displays the NeXpose InstallShield Wizard. Click **Next** on the *Welcome* page.

The installer displays the end-user license agreement. Read it, and select the option for accepting the terms.

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**.

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).

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 customercare@rapid7.com. After you enter the product key, click **NEXT**.

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**.

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.

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.

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 NeXpose Help or the *NeXpose Manual* for more information.

Click **Finish**.

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

Starting NeXpose in Windows

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 when Windows starts.

Click the Windows **Start** button, and select **Run...**

In the *Run* dialog box, type `services.msc`, and click **OK**.

In the *Services* pane, double-click the icon for the NeXpose Security Console service.

From the drop-down list for **Startup type:** select "Automatic", and click **OK**.

Close *Services*.

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.

Stop the NeXpose server: Go to the NeXpose command prompt, type `quit`, and press **ENTER.**

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.

Click the Windows **Start** button, and select **Run...**

In the *Run* dialog box, type `regedit`, and click **OK**.

In the Registry Editor, open the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ folder.

Delete the NeXposeConsole and nxpgsql folders.

Restart the computer.

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.

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

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 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)

Running the NeXpose installer in Ubuntu

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

Go to the directory to which you downloaded NeXpose installer.

Change the permissions for the installation file to make it executable:

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

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.

The installer displays a message that it will install NeXpose. Press **1** and then **ENTER** to continue.

The installer displays the end-user license agreement. Read each displayed section and press **ENTER** to continue.

At the end of the agreement, press **1** to accept the terms. Then press **0** to continue.

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

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.

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

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).

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

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 customercare@rapid7.com. After you type the product key, press **ENTER**.

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

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

The installer displays a request for your name. Type it, and press **ENTER**.

The installer displays a request for your company name. Type it, and press **ENTER**.

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

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.

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**.

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 NeXpose Help or the *NeXpose Manual* for more information.

The installer displays a message that the installation is complete. Press **3**.

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

Make sure that you are in the NeXpose installation directory, which you selected during installation. See *Running the NeXpose installer in Ubuntu (on page 16)*.

Go to the directory that contains the script that starts NeXpose:

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

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.

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

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

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

Look for two consecutive lines that read:

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

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

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

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

Save and close the nexposeconsole.rc file.

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]
```

Ensure that the daemon can run:

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

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.

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

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

Go the line that begins with `SELINUX=`

If the setting is `enabled`, change it to `disabled`:

```
SELINUX=disabled
```

Save and close the file.

Restart the server for the change to take effect:

```
$ shutdown -r now
```

Running the NeXpose installer in Red Hat

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

Go to the directory to which you downloaded NeXpose installer.

Change the permissions for the installation file to make it executable:

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

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.

The installer displays a message that it will install NeXpose. Press **1** and then **ENTER** to continue.

The installer displays the end-user license agreement. Read each displayed section and press **ENTER** to continue.

At the end of the agreement, press **1** to accept the terms. Then press **0** to continue.

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

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.

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

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).

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

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 customercare@rapid7.com. After you type the product key, press **ENTER**.

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

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

The installer displays a request for your name. Type it, and press **ENTER**.

The installer displays a request for your company name. Type it, and press **ENTER**.

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

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.

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**.

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 NeXpose Help or the *NeXpose Manual* for more information.

The installer displays a message that the installation is complete. Press **3**.

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

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 19).

Go to the directory that contains the script that starts NeXpose:

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

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 will continue running even if the current user logs off.

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

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

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

Look for two consecutive lines that read:

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

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

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

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

Save and close the nexposeconsole.rc file.

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]
```

Ensure that the daemon can run:

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

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).

Start the GUI.

In the GUI, click **Computer**, then **Control Center** under *System* in the right pane**.**

Click **Open Administrator Settings** under *Common Tasks* in the left pane.

Enter the root password, and click **OK**.

The YaST Control Center opens. Click **Novell AppArmor** under *Groups* in the left pane.

Click **AppArmor Control Panel** under *Novell AppArmor* in the right pane.

Clear the check box labeled **Enable App Armor**, and then click **Done**.

From the command prompt, restart the operating system:

```
$ shutdown -r now
```

Running the NeXpose installer in SUSE

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

Go to the directory to which you downloaded NeXpose installer.

Change the permissions for the installation file to make it executable:

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

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.

The installer displays a message that it will install NeXpose. Press **1** and then **ENTER** to continue.

The installer displays the end-user license agreement. Read each displayed section and press **ENTER** to continue.

At the end of the agreement, press **1** to accept the terms. Then press **0** to continue.

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

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.

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

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).

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

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 customercare@rapid7.com. After you type the product key, press **ENTER**.

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

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

The installer displays a request for your name. Type it, and press **ENTER**.

The installer displays a request for your company name. Type it, and press **ENTER**.

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

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.

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**.

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 NeXpose Help or the *NeXpose Manual* for more information.

The installer displays a message that the installation is complete. Press **3**.

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

Make sure that you are in the NeXpose installation directory, which you selected during installation. See *Running the NeXpose installer in SUSE (on page 22)*.

Go to the directory that contains the script that starts NeXpose:

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

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.

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

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

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

Look for two consecutive lines that read:

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

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

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

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

Save and close the nexposeconsole.rc file.

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]
```

Ensure that the daemon can run:

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

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.

Logging on to NeXpose

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.

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 Manual or NeXpose Help.

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.

When your browser displays the *Log in* box, enter your user name and 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 the NeXpose Help topic *Running NeXpose in maintenance mode* in the NeXpose Manual or NeXpose Help.

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 NeXpose Help. 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.

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

Click the **Help** link on any page of the Web interface for information on how to get started using NeXpose.