Extreme Networks Security Juniper NSM Plug-In User Guide

Release 7.7.2.5

Published July 2015

9034858

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys Networks, Inc., reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information about Extreme Networks trademarks, go to: www.extremenetworks.com/company/legal/trademarks/

Support

For product support, including documentation, visit: www.extremenetworks.com/support/

Contact

Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 95134
Tel: +1 408-579-2800
Toll-free: +1 888-257-3000

Table of Contents

1 About This Guide

The *Juniper Networks NSM Plug-In Users Guide* provides you with information on installing and configuring the Juniper Networks NSM Plug-In.

Intended Audience

The guide is intended for system administrators responsible for installing, configuring, or using plug-in components on your Extreme SIEM Console.

Conventions

The following conventions are used throughout this guide:

NOTE

Indicates that the information provided is supplemental to the associated feature or instruction.

CAUTION

Indicates that the information is critical. A caution alerts you to potential loss of data or potential damage to an application, system, device, or network.

WARNING

Indicates that the information is critical. A warning alerts you to potential dangers, threats, or potential personal injury. Read any and all warnings carefully before proceeding.

Technical Documentation

You can access technical documentation, technical notes, and release notes directly from the Extreme Networks documentation page website at www.extremenetworks.com/support. When you access the Extreme Networks documentation page website, locate the product and software release for which you require documentation.

Your comments are important to us. Send your email comments about this guide or any of the Extreme Networks documentation to:

internalinfodev@extremenetworks.com

Include the following information with your comments:

- Document title
- Page number

Contacting Customer Support

To help resolve any issues that you may encounter when installing or maintaining Extreme SIEM, you can contact Customer Support as follows:

- Log a support request 24/7: www.extremenetworks.com/support
- Telephone assistance: www.extremenetworks.com/support/contact

2 Installing the NSM Plug-In

Juniper Networks Network and Security Manager (NSM) is a software application that centralizes control and management of your Juniper Networks devices. Juniper Networks NSM delivers integrated, policy-based security and network management for all devices.

NOTE

Ensure you have the latest Extreme Security patch installed on your Extreme Security Console (Patch 7.0.0.182810 or later).

You can use the Juniper Networks NSM Plug-In to view policy details from the Juniper Networks NSM server for an event.

NOTE

Installing the Juniper Networks NSM Plug-In results in the httpd and Tomcat processes automatically restarting. This causes a service disruption while the processes restart.

Installing the NSM Plug-In

To install the Juniper Networks NSM Plug-In:

1 Using SSH, log in to Extreme Security as the root user.

Username: root

Password: <password>

2 To verify that you have the **nsm_plugin-7.0.0-<build>.i386.rpm** file, type the following command:

```
ls /opt/qradar/rpms
```

Where **<build>** is the related Extreme Security build number.

If the file is not listed, go to step 3. If the file is listed, go to step 4.

3 Mount the Extreme Security installation ISO file and install the NSM Plug-in rpm:

a To mount the Extreme Security installation ISO file, type the following command:

```
mount -o loop <path to the QRadar ISO> /media/cdrom
```

Where <**path to the Extreme Security ISO**> is the directory path to where the installation ISO is stored.

b Type the following command to unpack and install the NSM Plug-in rpm:

```
rpm -Uvh /media/cdrom/post/qradar/nsm_plugin-7.0.0-
<build>.i386.rpm
```

Where **<build>** is the related Extreme Security build number.

The package manager automatically unpacks and installs the NSM Plug-in rpm.

The NSM Plug-in installation is complete when the following text is displayed:

```
Starting Tomcat: [ok]
Starting httpd: [ok]
```

c Go to step 5.

4 Type the following command:

```
rpm -Uvh /opt/qradar/rpms/nsm_plugin-7.0.0-<build>.i386.rpm
```

Where **<build>** is the related Extreme Security build number.

The package manager automatically unpacks and installs the NSM Plug-in rpm.

The NSM Plug-in installation is complete when the following text is displayed:

```
Starting Tomcat: [ok]
Starting httpd: [ok]
```

5 Log in to the Extreme Security user interface:

```
https://<IP Address>
```

Where <**IP Address**> is the IP address of the Extreme Security system.

Username: admin

Password: <password>

The target directory /opt/qradar/conf/webplugins/117/ must exist on your Extreme Security system and is automatically created when you log in to the Extreme Security user interface.

6 Choose one of the following options:

- To connect to a Juniper NSM 2010 device, go to step 7.
- To connect to another Juniper NSM version, go to step 10.

7 Using SSH, log in to Extreme Security as the root user.

Username: root

Password: <password>

Type the following command to copy the server certificate from your Juniper NSM appliance to Extreme Security:

```
scp root@<NSM IP address>:/usr/netscreen/GuiSvr/lib/webproxy/
conf/server.crt /opt/qradar/conf/webplugins/117/nsmPlugin.cert
```

Where **<NSM IP address> is the** IP address of the Juniper Networks NSM server.

The server.crt file is copied from the Juniper Networks NSM appliance and renamed to nsmPlugin.cert on your Extreme Security Console. If an error occurs and the target directory does not exist, go back to step 5 and log in to Extreme Security again.

8 Type the following command to set the file permission for the directory and the nsmPlugin.cert file:

```
chown nobody:nobody /opt/qradar/conf/webplugins/117/
nsmPlugin.cert
```

9 Type the following command to restart Tomcat:

```
service tomcat restart
```

10 Log in to the Extreme Security user interface:

```
https://<IP Address>
```

Where <**IP Address**> is the IP address of the Extreme Security system.

Username: admin

Password: <password>

11 Click the Admin tab.

12 On the navigation menu, click Plug-ins.
The NSM Plug-in Settings icon is displayed.

NOTE

If multiple users or remote users are viewing the Admin tab, you may need to refresh your browser for the NSM Plug-in Settings icon to be displayed.

You are now ready to set up your plug-in. For more information, see Chapter 3, “Setting Up the Plug-In”.

3 Setting Up the Plug-In

The Juniper Networks NSM Plug-in allows QRadar to integrate with your Juniper Networks NSM appliance to view policy-based security and network management information from NSM appliances. Before you can view policy information, you must configure QRadar permissions and user roles.

This section includes the following topics:

Configuring the Server Settings

After you have successfully installed the Juniper Networks NSM Plug-in, you must configure your QRadar Console with the IP address and port number of your Juniper Networks NSM appliance.

To configure the Juniper Networks NSM Plug-In settings:

1 Click the Admin tab.

2 In the navigation menu, click Plug-ins.
The Plug-ins window is displayed.

3 In the Plug-In Configuration pane, click the NSM Plug-in Settings icon.
The NSM Server Settings window is displayed.

4 In the NSM Server URL field, type the IP address or hostname of the Juniper Networks NSM server to which you want to connect.
For example, https://192.168.2.1:8443.

5 Click Save Changes.

Setting User Permissions

You must ensure that each QRadar user who requires access to the Juniper NSM Plug-in has been assigned the appropriate user permissions. You must have administrative privileges to configure user roles in QRadar.

To set the appropriate user permissions for the Juniper Networks NSM Plug-in:

1 Click the Admin tab.

2 On the navigation menu, click System Configuration.
The System Configuration pane is displayed.

3 In the User Management pane, click the User Roles icon.
The Manage User Roles window is displayed.

4 Choose one of the following options:
   a If you want to create a new role, click Create Role.
   b If you want to edit an existing role to include NSM Plug-in Settings, click the Edit icon for the role which requires the assigned permissions.

   The Manage Role Permissions window is displayed.

5 Select the user permissions for the NSM Plug-in Settings:
   - Launch NSM Client - Select this check box if you want to allow users to launch the NSM Client from the main user interface. By default, this check box is clear.
   - View NSM Policy Details from Events interface - Select this check box if you want to allow users to view policy details for the Juniper Networks NSM server from the Log Activity page. By default, this check box is clear.

6 Select the remaining permissions.

   For more information on role permissions, see the *Extreme SIEM Administration Guide*.

NOTE

Make sure you have Events permissions to access the policy details.

7 Complete the steps of the wizard.

8 On the Admin tab, click Deploy Changes.

Setting User Preferences

All users with the View NSM Policy Details from Events interface role permission must enter their user settings to authenticate their user account with the Juniper Networks NSM server. This ensures that appropriate users are able to view policy details for an event.

To configure user details:

1 In the upper-right corner of the Extreme SIEM user interface, click NSM Preferences.

   The NSM User Settings window is displayed.

NOTE

If your administrator has not completed the configuration of the plug-in, an information message is displayed. Contact your system administrator to complete the configuration before continuing. For more information, see Configuring the Server Settings on page 6.

2 Enter values for the following parameters:

- NSM Login - Type your user name, as defined on the Juniper Networks NSM server.
- NSM Password - Type your password, as defined on the Juniper Networks NSM server.
- NSM Domain - Type your domain, as defined on the Juniper Networks NSM server. The default is global.

3 Click Save Changes.

NOTE

If your credentials are rejected by the Juniper Networks NSM server, but you have verified your access information, your IP address may be blocked by the Juniper Networks NSM server as a result of too many failed login attempts. Contact your Juniper Networks NSM server administrator to unblock the following IP address: 127.0.0.1 using the Tools > Manage Blocked Hosts option in the Juniper Networks NSM client.

4 Using the Plug-In

After you have configured and set up the plug-in, you can view policy event information.

This section includes the following topics:

Launching NSM

This section provides information about launching NSM.

To launch NSM:

1 In the upper-right corner of the Extreme SIEM user interface, click Launch NSM.

2 Choose one of the following options:
- If you are using FireFox and this is the first time you are launching NSM, go to step 3.
- If you are using Microsoft Internet Explorer 8.0 or 9.0, with Compatibility View enabled, and this is the first time you are launching NSM, go to step 4.
- If you have previously launched NSM, go to step 5.

3 To launch NSM for the first time using FireFox:
a In the Opening window, select the Open with option.
b Click Browse.
c Select the NSM executable from the appropriate directory:
- For NSM 2010, the file path is c:\Program Files\Network and Security Manager\NSM.exe.
- For previous NSM versions, the file path is c:\Program Files\NSM\NSM.exe.

d Click OK.
e Select the Do this automatically for files like this from now on check box.
f Click OK.

The Juniper Networks - NSM Login is displayed.
g Go to step 5.

4 To launch NSM for the first time using Internet Explorer 8.0 or 9.0, with Compatibility View enabled, you must:
a Create a new association for the .nsm extension and change the extension to access the NSM.exe file. Select the NSM executable from the appropriate directory:
- For NSM 2010, the file path is c:\Program Files\Network and Security Manager\NSM.exe.
- For previous NSM versions, the file path is c:\Program Files\NSM\NSM.exe.

For more information on creating a file association, see your vendor documentation.

The Juniper Networks - NSM Client login is displayed.
b Go to step 5.

5 Type the necessary login credentials for the Juniper Networks Client.

6 Click OK.

The Juniper Networks client is displayed. For more information, see your Juniper documentation.

Viewing Policy Details

After the Juniper Networks NSM Plug-In is installed and configured, you can view policy details using the Log Activity page. However, before you can view policy details, you must add the Policy column to the Log Activity page display.

This section includes the following topics:

Adding the Policy Column

To add the NSM Policy column to the Log Activity page:

1 Click the Log Activity tab.

2 From the Search list box, select New Search.

The New Search window is displayed.

3 From the Available Columns list, select NSM Policy (custom).

4 Select the arrow to move the item to the Column list.

NOTE

For information about additional search parameters, see the *Extreme SIEM Users Guide*.

5 Click Filter.

The Log Activity page displays the Policy (custom) column.

Viewing Policy Details

To view policy details:

1 Click the Log Activity tab.

2 Navigate to the event on which you want to view policy details.

For more information on navigating the Log Activity pane, see the *Extreme SIEM Users Guide*.

3 In the Policy (custom) column of the event you selected in step 2, right-click on the column to access additional menu options.

4 From the menu, select More options > View NSM Policy Details.

The NSM Policy details window is displayed.

NOTE

The More options menu item is not available in Streaming mode.

Each Juniper Networks NSM policy includes groups of rule bases and rules. This window provides details of the selected NSM policy and details of the associated rules for this policy. This window may require several minutes to populate depending on the amount of data.

For more information on the Juniper Networks NSM policy, see your Juniper Networks NSM documentation.