



Security Threat Response Manager

NSM Plug-In User Guide

Release 2009.1

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Published: 2009-10-12

Copyright Notice

Copyright © 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense. The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Reorient or relocate the receiving antenna. Increase the separation between the equipment and receiver. Consult the dealer or an experienced radio/TV technician for help. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Configuring DSMs
Release 2009.1

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

October 2009—Revision 1

The information in this document is current as of the date listed in the revision history.

CONTENTS

ABOUT THIS GUIDE

- Conventions 1
- Technical Documentation 1
- Contacting Customer Support 2

1 INSTALLING THE NSM PLUG-IN

2 SETTING UP THE PLUG-IN

- Configuring the Server Settings 5
- Setting User Permissions 6
- Setting User Preferences 7

3 USING THE PLUG-IN

- Launching NSM 11
 - Launching NSM 11
- Viewing Policy Details 12
 - Adding the Policy Column 12
 - Viewing Policy Details 13




ABOUT THIS GUIDE

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

Conventions

[Table 1](#) lists conventions that are used throughout this guide.

Table 1 Icons

Icon	Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, device, or network.
	Warning	Information that alerts you to potential personal injury.

Technical Documentation

You can access technical documentation, technical notes, and release notes directly from the Juniper Customer Support web site at <https://www.juniper.net/support/>. Once you access the Technical support web site, locate the product and software release for which you require documentation.

Your comments are important to us. Please send your e-mail comments about this guide or any of the Juniper Networks documentation to:

techpubs-comments@juniper.net.

Include the following information with your comments:

- Document title
- Page number

**Contacting
Customer Support**

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

- Open a support case using the Case Management link at <http://www.juniper.net/support>.
- Call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

1

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.

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 Tomcat process automatically restarting. This causes a service disruption while the process restarts.*

To install the Juniper Networks NSM Plug-In:

Step 1 Copy the 2009.1 iso file to /tmp.

Step 2 Navigate to /tmp,

```
cd /tmp
```

Step 3 Enter the following command:

```
mount -t iso9660 -o loop <ISO Filename> /media/cdrom
```

Step 4 Enter the following command

```
rpm -Uvh/media/cdrom/post/qradar/  
nsm_plugin-6.3.0-<build>.i386.rpm:
```

Where <build> is the related STRM build number.

Step 5 Log in to the STRM interface:

```
http://<IP address>
```

Where <IP address> is the IP address of the STRM system.

Step 6 Click the **Admin** tab.

The Admin interface appears.

Step 7 In the navigation pane, click **System Configuration**.

The NSM Plug-in Settings icon appears. You are now ready to setup your plug-in. See [Chapter 2 Setting Up the Plug-In](#).

2

SETTING UP THE PLUG-IN

Before viewing Juniper Networks NSM policy information, you must setup the plug-in settings in the STRM interface. This chapter includes setup information including:

- [Configuring the Server Settings](#)
- [Setting User Permissions](#)
- [Setting User Preferences](#)

Configuring the Server Settings

To configure the Juniper Networks NSM Plug-In settings:



Note: You must have administrative privileges to configure the Juniper Networks NSM server settings. For more information regarding privileges, see the *STRM Administration Guide*.

Step 1 Click the **Admin** tab.

The Admin interface appears.

Step 2 In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

Step 3 In the Plug-In Configuration section, click the **NSM Plug-in Settings** icon.

The NSM Server Settings window appears.

A screenshot of a web-based configuration window titled "NSM Server Settings". The window has a header bar with the title and a help icon. Below the header, there is a descriptive paragraph: "This page contains the settings to configure the system to connect to NSM to allow users to login to retrieve policy & rule information." Underneath, there is a label "NSM Server URL" followed by a text input field containing "https://172.16.76.10:8443". Below the input field, there is a small example text: "Example: (https://192.168.2.1:8443)". At the bottom right of the window, there is a "Save Changes" button.

Step 4 In the NSM Server URL, specify IP address or hostname of the Juniper Networks NSM server to which you want to connect.

Step 5 Click **Save Changes**.

Note:

Setting User Permissions

You must ensure each user that must access plug-in information has the appropriate user role permissions.



Note: You must have administrative privileges to configure the Juniper Networks NSM server settings. For more information, see the *STRM Administration Guide*.

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

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **System Configuration**.
The System Configuration panel appears.
- Step 3** Click the **User Roles** icon.
The Manage User Roles window appears.
- Step 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 the NSM Plug-in Settings permissions, click the edit icon of the desired role.The Manage Role Permissions window appears.

Step 5 Select the desired permissions for the NSM Plug-in Settings:

- **Launch NSM Client** - Select this check box if you want to allow users the ability to Launch the NSM Client from the main interface. By default, the check box is clear.
- **View NSM Policy Details from Events interface** - Select this check box if you want to allow users the ability to view policy details for the Juniper Networks NSM server from the Events interface. By default, the check box is clear.

Step 6 Select the remaining permissions.

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



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

Step 7 Complete the wizard.

Step 8 From the Admin tab menu, 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 ensure the appropriate users are able to view policy details for an event.

To configure user details:

Step 1 In the STRM interface, click **NSM Preferences**.

The NSM User Settings window appears.



Note: If your administrator has not completed the configuration of the plug-in, a message appears. Contact your system administrator to complete the configuration before continuing. See [Configuring the Server Settings](#).

Step 2 Enter values for the parameters:

- **NSM Login** - Specify your username, as defined in the Juniper Networks NSM server.
- **NSM Password** - Specify your password, as defined in the Juniper Networks NSM server.
- **NSM Domain** - Specify your domain, as defined in the Juniper Networks NSM server. The default is global.

Step 3 Click **Save Changes**.



Note: NSM cannot be contacted from the STRM dashboard or the Event page.

If you set NSM as the preference in the STRM dashboard, or view the NSM Policy details from the STRM Event page, an error message appears:

```
NSM cannot be contacted at https://10.205.75.2:8443. Please
verify the URL.
```

Since the SSH certificate connects NSM to STRM, the error could appear either because the SSH certificate on the NSM box has expired or is invalid. Accept the invalid SSH key and continue with the SSH connection.

To do this:

Step 1 Copy the following file from the NSM box:

```
/usr/netscreen/GuiSvr/lib/webproxy/conf/client.truststore
```

Step 2 Go to the following file on the STRM box:

```
/opt/gradar/conf/webplugins/117/client.truststore
```

Step 3 Replace this file on the STRM box with the file from the NSM box.

Step 4 Restart tomcat using the following command:

```
# service tomcat restart
```



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.*

3

USING THE PLUG-IN

Once you have the plug-in configured and setup, you can view policy event information. This chapter provides information on launching and viewing policy details including:

- [Launching NSM](#)
- [Viewing Policy Details](#)

Launching NSM

This section provides information about launching NSM.

Launching NSM To launch NSM:

Step 1 In the STRM interface, click **Launch NSM**.

Step 2 Choose one of the following options:

- If you are using FireFox 3.0 and this is the first time you are launching NSM, go to [Step 3](#).
- If you are using Microsoft Internet Explorer 6.0/7.0 and this is the first time you are launching NSM, go to [Step 4](#)
- If you have previously launched NSM, go to [Step 5](#).

Step 3 To launch NSM for the first time using FireFox 3.0:

- a In the Opening window, select the **Open with** option.
- b Click **Browse**.
- c Select the downloaded plug-in file in the appropriate directory. Typically, this file is located in the c:\\Program Files\\NetScreen-Security Manager\\ directory.
- 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 appears.

g Go to [Step 5](#).

Step 4 To launch NSM for the first time using Internet Explorer 6.0/7.0:

- a From your desktop, select **Start > Control Panel**.

The Control Panel appears.

- b Double-click the **Folder Options** icon.
 - c Click the **File Types** tab.
 - d Create a new association for the .nsm extension and change the extension to access the NSM.exe file.
 - e Click **Ok**.
 - f In the STRM interface, click **Launch NSM**.
 - g In the File Download window, clear the **Always ask before opening this type of file** check box.
 - h Click **Open**.
- The Juniper Networks - NSM Client login appears.
- i Go to [Step 5](#).

Step 5 Enter the necessary log in credentials for the Juniper Networks Client.

Step 6 Click **Ok**.

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

Viewing Policy Details

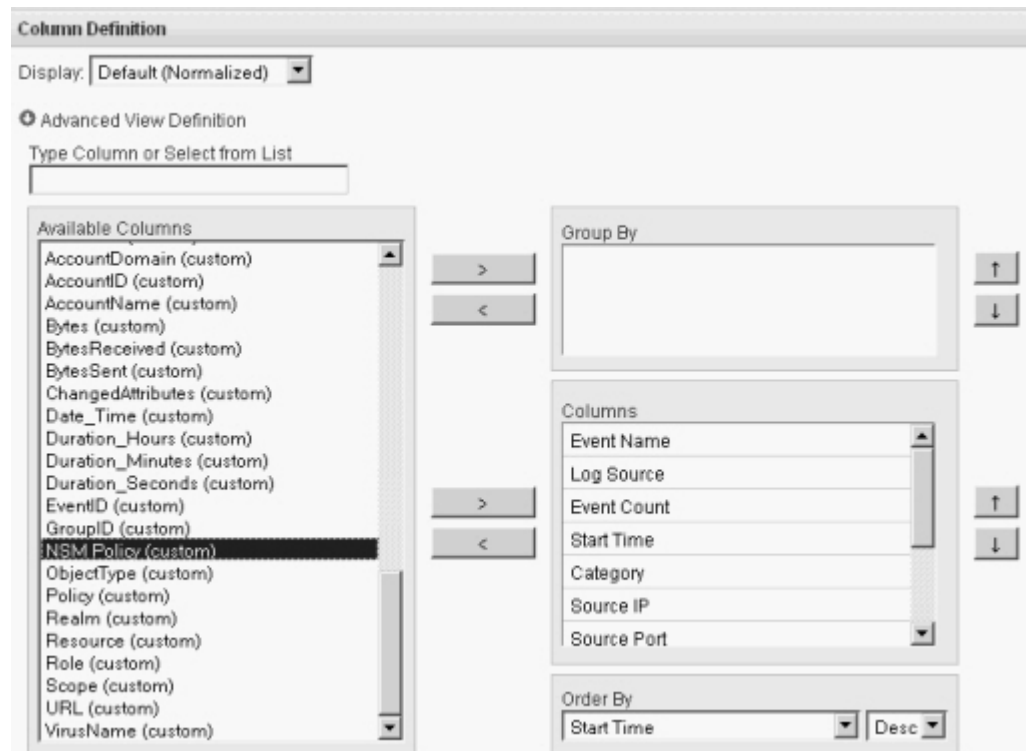
Once the Juniper Networks NSM Plug-In is installed and configured, you can view policy details using the Events interface. However, before you can view policy details, you must add the Policy column to the Events interface display. This section includes information about adding the Policy column and viewing policy details including:

- [Adding the Policy Column](#)
- [Viewing Policy Details](#)

Adding the Policy Column

To add the NSM Policy column to the Events interface display:

- Step 1** Click the **Events** tab.
The Events interface appears.
- Step 2** Using the Search drop-down list box, select **New Event Search**.
The new event search window appears.
- Step 3** Using the Available Columns list, select the **NSM Policy (custom)** item.



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



Note: For information regarding additional search parameters, see the *STRM Users Guide*.

Step 5 Click **Filter/Search**

The Events interface appears with the Policy (custom) column.

Viewing Policy Details

To view policy details:

Step 1 Click the **Events** tab.

The Events interface appears.

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

For more information navigating the Events interface, see the *STRM Users Guide*.

Step 3 In the Policy (custom) column of the event you selected in [Step 2](#), use the right mouse button (right-click) to access additional menu options.

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

The NSM Policy details window appears.



Note: The *More options* menu item is not available in the Streaming mode.

Rule No.	ID	From Zone	Source	To Zone	Destination	Service	Action	Install On	Rule Options	Comments
1	1	trust	any	untrust	any	any	deny	any	Count, Auth by	
2	3	self	any	untrust	any	any	reject	any	Auth by Server	

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

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