IBM Security QRadar
Version 7.2.1

# Juniper Networks NSM Plug-In User Guide

**IBM**

**Note:** Before using this information and the product that it supports, read the information in "Notices and Trademarks" on page 13.

# CONTENTS

# 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 IBM® Security QRadar® Console.

## Technical Documentation

For information on how to access more technical documentation, technical notes, and release notes, see the *Accessing IBM Security QRadar Documentation Technical Note*.
(http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)

## Contacting Customer Support

For information on contacting customer support, see the *Support and Download Technical Note*.
(http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)

## Statement of good security practices

IT system security involves protecting systems and information through prevention, detection, and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

# 1 INSTALLING THE NSM PLUG-IN

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

## NSM Plug-In overview

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.

Ensure that the latest QRadar® patch is installed on your IBM® Security QRadar® Console.

When you install the Juniper Networks NSM Plug-In, the httpd and Tomcat processes automatically restart and cause a service disruption.

## Installing the NSM Plug-In

Use SSH to install the Juniper Networks NSM Plug-In on your QRadar Console.

**About this task**

The target directory (/opt/qradar/conf/webplugins/117/) must exist on your QRadar system. After you install the plug-in, the target directory is automatically created when you log in to the QRadar user interface and click the **NSM Settings Plugin** icon on the **Admin** tab.

If multiple users or remote users view the **Admin** tab, refresh your browser to display the **NSM Plug-in Settings** icon to be displayed

**Procedure**

Step 1   Download the QRadar ISO from the following website:

*http://www.ibm.com/support*

Step 2   Copy the ISO file to your QRadar Console.

Step 3   Using SSH, log in to QRadar as the root user.

Step 4   Type the following command to mount the QRadar ISO file:

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

Where `<path to the QRadar ISO>` is the directory path to where the installation ISO is stored.

**Step 5** Type the following command to install the NSM Plug-in rpm:

```
rpm -Uvh
/media/cdrom/post/qradar/nsm_plugin-7.x.x-<build>.i386.rpm
```

Where `<build>` is the related QRadar build number.

The package manager installs the NSM Plug-in rpm.

**Step 6** To create the target directory:

  **a** Log in to the QRadar user interface:

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

  Where `<IP Address>` is the IP address of the QRadar system.

  **b** Click the **Admin** tab.

  **c** Click the **NSM Plug-in Settings** icon.

**Step 7** Using SSH, log in to QRadar as the root user.

**Step 8** Choose one of the following options:

- To connect QRadar to Juniper NSM 2010 server, you must copy a certificate to QRadar, go to **Step 9**.
- To connect QRadar to any other version of Juniper NSM, go to **Step 11**.

**Step 9** Type the following command to copy the server certificate from your Juniper NSM 2010 server to the QRadar Console:

```
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 2010 server and renamed to nsmPlugin.cert on your QRadar Console.

**Step 10** Type the following command to set the file permissions:

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

**Step 11** Type the following command to restart Tomcat:

```
service tomcat restart
```

**What to do next**

**Setting up the plug-in**

# 2 SETTING UP THE PLUG-IN

The Juniper Networks NSM Plug-in allows IBM® Security 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 SIEM permissions and user roles.

## Configuring the server settings

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

**Procedure**

Step 1  Click the **Admin** tab.

Step 2  In the navigation menu, click **Plug-ins**.

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

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

Step 5  Click **Save Changes**.

## Setting user permissions

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

**Procedure**

Step 1  Click the **Admin** tab.

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

Step 3  In the User Management pane, click the **User Roles** icon.

Step 4  Choose one of the following options:

    a  To create a new role, click **Create Role**.

    b  To edit an existing role to include NSM Plug-in Settings, select the role and click the **Edit** icon.

**Step 5**  Select the user permissions for the NSM Plug-in settings:

- **Launch NSM Client** - Select this check box o allow users to start the NSM Client from the main user interface.

- **View NSM Policy Details from Events interface** - Select this check box to allow users to view policy details for the Juniper Networks NSM server from the **Log Activity** tab.

**Step 6**  Select the remaining permissions. For more information on role permissions, see the *IBM® Security QRadar® Administration Guide*.

**Step 7**  Complete the steps of the wizard.

**Step 8**  On the **Admin** tab, click **Deploy Changes**.

---

**Setting NSM preferences**

f you have the **View NSM Policy Details from Events interface** role permission, configure your NSM settings to authenticate your user account with the Juniper Networks NSM server.

**Before you begin**

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

**About this task**

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 you continue. For more information, see **Configuring the server settings**.

The Juniper Networks NSM server might reject your credentials as a result of too many failed login attempts. If this occurs, contact your Juniper Networks NSM server administrator to unblock the following IP address: 127.0.0.1 by using the **Tools > Manage Blocked Hosts** option in the Juniper Networks NSM client.

**Procedure**

**Step 1**  In the upper-right corner of the user interface, click **NSM Preferences**.

**Step 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.

**Step 3**  Click **Save Changes**.

# 3    USING THE PLUG-IN

After you configure the plug-in, you can view policy event information.

**Starting NSM**    You can start NSM from the IBM® Security QRadar® user interface.

**Procedure**

**Step 1** In the upper-right corner of the user interface, click **Launch NSM**.

**Step 2** Choose one of the following options:

- If you use the Mozilla Firefox web browser and this is the first time that you start NSM, go to **Step 3**.
- If you use the Microsoft® Internet Explorer 8.0 or 9.0 web browser, with Compatibility View enabled, and this is the first time that you are start NSM, go to **Step 4**.
- If you previously launched NSM, go to **Step 5**.

**Step 3** To start NSM for the first time in the Mozilla Firefox web browser:

**a** In the Opening window, select the **Open with** option.

**b** Click **Browse**.

**c** Select the NSM.exe file 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**.

**g** Go to **Step 5**.

**Step 4** To start NSM for the first time in the Internet Explorer 8.0 or 9.0, with Compatibility View enabled:

**a** Create an association for the .nsm extension and change the extension to access the NSM.exe file. Select the NSM.exe 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 about how to create a file association, see your vendor documentation.

**b**   Go to **Step 5**.

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

**Step 6**   Click **OK**.

---

**Viewing policy details**

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

**Adding the policy column**

Use the event search page to add the **NSM Policy (custom)** column to the Log Activity page:

**About this task**

This task includes only the search criteria for displaying **NSM Policy (custom)** column. For information about search parameters, see the *IBM® Security QRadar® Users Guide*.

**Procedure**

**Step 1**   Click the **Log Activity** tab.

**Step 2**   From the **Search** list box, select **New Search**.

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

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

**Step 5**   Click **Filter**.

**Result**

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

**Viewing policy details**

You can view policy details from the Log Activity tab.

**About this task**

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 might require several minutes to populate depending on the amount of data.

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

**Procedure**

**Step 1**  Click the **Log Activity** tab.

**Step 2**  If events are displayed in Real Time (streaming) mode, click the **Pause** icon.

**Step 3**  Right-click the NSM Policy (custom) parameter for the event you want to investigate, and then select **More options > View NSM Policy Details**.

# A  NOTICES AND TRADEMARKS

What's in this appendix:

- **Notices**
- **Trademarks**

This section describes some important notices, trademarks, and compliance information.

## Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing*
*IBM Corporation*
*North Castle Drive*
*Armonk, NY 10504-1785 U.S.A.*

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

*Intellectual Property Licensing*
*Legal and Intellectual Property Law*
*IBM Japan Ltd.*
*19-21, Nihonbashi-Hakozakicho, Chuo-ku*
*Tokyo 103-8510, Japan*

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

*IBM Corporation*
*170 Tracer Lane,*
*Waltham MA 02451, USA*

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance,

compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

**Trademarks**

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at *http://www.ibm.com/legal/copytrade.shtml*.

The following terms are trademarks or registered trademarks of other companies:

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

**Privacy policy considerations**

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

# INDEX

---

**A**
adding
    policy column 10

---

**C**
configure
    server settings 7
conventions 1

---

**I**
installing
    plug-in 3

---

**N**
NSM plug-in
    installing 3
    launching 9

---

**P**
plug-in
    installing 3
    using 9
policy column
    adding 10
policy details
    viewing 10

---

**S**
server settings
    configure 7
setup
    server settings 7
    user permissions 7
    user preferences 8

---

**U**
user permissions
    setting 7
user preferences
    setting 8