IBM Security QRadar Risk Manager
Version 7.1.0 (MR1)

Adapter Configuration Guide

Note: Before using this information and the product that it supports, read the information in “Notices and trademarks” on page 21.

ABOUT THIS GUIDE

The *IBM Security QRadar Risk Manager Configuring Adapters Guide* provides you with information for configuring adapters for integrating firewalls, routers, and switches with IBM Security QRadar Risk Manager.

Intended audience

This guide is intended for the system administrator responsible for configuring device backups or using Configuration Source Management in QRadar Risk Manager. This guide assumes that you have administrative access to IBM Security QRadar SIEM, administrative access to your network devices and firewalls, along with a knowledge of your corporate network and networking technologies.

Documentation conventions

The following conventions are used throughout this guide:

- ▶ Indicates that the procedure contains a single instruction.

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	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)

1 ADAPTERS OVERVIEW

Adapters allow IBM Security QRadar Risk Manager to interrogate and import the configuration parameters of the devices in your network, such as firewalls, routers, and switches. QRadar Risk Manager requests configuration backups from network devices and uses adapters to collect the configurations and turn the information into a format that is unified for device models, manufacturers, and types. The data retrieved from network devices allows QRadar Risk Manager to understand your network Topology and configuration of your network devices. The schedule for network devices is determined by the schedule of backup jobs in the Configuration Source Management on the **Admin** tab of IBM Security QRadar SIEM.

To connect external devices in the network, QRadar Risk Manager must be able to access the devices. Adapters allow you to integrate QRadar Risk Manager with your network devices. This includes having usernames and passwords that allow QRadar Risk Manager to access the device and download configurations.

To integrate network devices with QRadar Risk Manager, perform the process listed below:

1. Configure your network device with appropriate access to QRadar Risk Manager.
2. Install the proper adapter for your network device on your QRadar Risk Manager appliance. For more information, see **Installing an adapter**.
3. Add your network devices to QRadar Risk Manager using Configuration Source Management.
4. Define the communication method (protocol) required for communication to your network devices. For more information, see the *IBM Security QRadar Risk Manager User Guide.*

If your network devices are in different networks where QRadar Risk Manager and your network devices can not communicate, see the Disconnected Configuration Toolkit appendix in the *IBM Security QRadar Risk Manager User Guide*.

Types of adapters

IBM Security QRadar Risk Manager supports the following adapters:

- Check Point SecurePlatform
- Cisco Internet Operating System (IOS)
- Cisco Catalyst (CatOS)
- Cisco Security Appliance
- Juniper Networks ScreenOS
- Juniper Networks JunOS
- Juniper Networks NSM

The Cisco Catalyst (CatOS) adapter allows you to collect device configurations by backing up CatOS network devices viewable by QRadar Risk Manager.

The Cisco Internet Operating System (IOS) adapter allows you to collect device configurations by backing up IOS-based network switches and routers.

The Cisco Security Appliances adapter is used to collect device configurations by backing up Cisco family devices. The Cisco Security Appliances adapter supports the family of Cisco firewalls. For example, a stand-alone Adaptive Security Appliance, a Firewall Service Module (FWSM), a module in a Catalyst chassis, or a legacy Private Internet Exchange (PIX) device.

You can use the QRadar Risk Manager to back up a single Juniper Networks device or obtain device information from a Juniper Networks NSM console.

Before you start adding your devices to QRadar Risk Manager, you need to understand and be aware of supported software versions, credentials, and required commands for your network devices. For more information, see **Supported adapters**.

2 INSTALL ADAPTERS

You can access and download adapters from the Qmmunity website. The RPM files are included in the download. You can contact customer support if you need access to Qmmunity.

The QRadar SIEM Console is the only device that can communicate directly to IBM Security QRadar Risk Manager after the initial connection between both appliances is established.

Installing an adapter

You need to download an adapter to your IBM Security QRadar SIEM Console, and then copy the adapter RPM to IBM Security QRadar Risk Manager.

To install an adapter on QRadar Risk Manager:

Step 1 Download the adapter file from the Qmmunity website to your QRadar SIEM Console.

Step 2 Using SSH, log in to your QRadar SIEM Console as a root user.

a Login as: **root**

b Password: **<password>**

Step 3 Type the following command to copy the adapter file from your QRadar SIEM Console to QRadar Risk Manager.

```
scp <adapter>.rpm root@<IP address>:
```

Where:

<adapter> is the adapter file to copy to QRadar Risk Manager.

<IP address> is the IP address or hostname of QRadar Risk Manager.

For example,

```
scp adapters.cisco.ios-2011_05-205181.noarch.rpm
root@100.100.100.100:
```

Step 4 Type the password for the root user on your QRadar Risk Manager appliance.

The file is copied to your QRadar Risk Manager appliance.

Step 5 Using SSH from your QRadar SIEM Console, log in to your QRadar Risk Manager appliance, as a root user.

a Login as: **root**

b Password: **<password>**

Step 6 Navigate to the root directory containing the adapter file.

Step 7 Type the following command to install the adapter:

```
rpm -Uvh <filename>
```

Where **<filename>** is the RPM name of the adapter.

For example, **rpm -Uvh adapters.cisco.ios-2011_05-205181.noarch.rpm**

Step 8 Type the following command to restart the ziptie-server service and complete the installation:

```
service ziptie-server restart
```

CAUTION

Restarting the service ziptie-server interrupts any device backups in progress from Configuration Source Management.

Uninstalling an adapter

You can uninstall an adapter from QRadar Risk Manager.

To uninstall an adapter from QRadar Risk Manager:

Step 1 Using SSH, log in to QRadar SIEM Console as a root user.

a Login as: **root**

b Password: **<password>**

Step 2 Using SSH from your QRadar SIEM Console, log in to your QRadar Risk Manager appliance, as a root user.

a Login as: **root**

b Password: **<password>**

Step 3 Type the following command to uninstall an adapter:

```
rpm -e <adapter file>
```

Where **<adapter file>** is the name of the adapter file. For example:

```
rpm -e adapters.cisco.ios-2011_05-205181.noarch.rpm
```

3 ADD AND CONFIGURE DEVICES

You can add network devices using Configuration Source Management in IBM Security QRadar SIEM. You can configure the device in IBM Security QRadar Risk Manager after the device is added.

Adding a device

Use Configuration Source Management to add a network device. Once added, a device can be configured.

To add devices that are managed by a Juniper Networks NSM console, see **Adding devices managed by a Juniper Networks NSM console**.

Before you begin

Before you add a device to QRadar SIEM, you need to understand and be aware of the supported software versions, credentials, and required commands for your network devices. For more information, see **Table A-1**, **Adapter integration requirements**.

While the SNMP credentials allow your device to discover a single neighboring device using SNMP discovery, these parameters are optional and are not required to backup a device configuration.

NOTE

These steps provide instructions for adding one type of device. You must repeat these steps for each type of network device that you want to add to QRadar SIEM.

To add a device:

Step 1 Click the **Admin** tab.

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

Step 3 On the Risk Manager pane, click **Configuration Source Management**.

Step 4 On the navigation menu, click **Credentials**.

Step 5 On the Network Groups pane, click **Add a new network group (+)**.

Step 6 Type a name for the network group, and click **OK**.

Step 7 Type the IP address of your device, and click **Add (+)**. Repeat this step for each address that you need to add.

***Note:** Ensure that the addresses that you add appears in the Network address box beside the Add address box.*

You can type an IP address, a range of IP addresses, a CIDR subnet, or a wildcard. For example, to use a wildcard type 10.1.*.* or to use a CIDR use 10.2.1.0/24.

NOTE

Do not replicate device addresses that already exists in other network groups in Configuration Source Management.

Step 8 On the Credentials pane, click **Add a new credential set (+)**.

Step 9 Type a name for the credential set, and click **OK**.

Step 10 Select the name of the credential set that you created.

Step 11 Configure values for the following parameters:

Table 3-1 Parameters for devices

Parameter	Description
Username	Type a valid username to log in to the adapter. For adapters, the username and password provided requires access to several files, such as rule.C, objects.C, implied_rules.C, and Standard.PF.
Password	Type the password for the device.
Enable Password	Type the password for second level authentication. This password is required when the credentials prompt the user credentials for Expert Mode.
SNMP Get Community	Optional parameter. Type the SNMP Get community name.
SNMPv3 Authentication Username	Optional parameter. Type the username you want to use to authenticate SNMPv3.
SNMPv3 Authentication Password	Optional parameter. Type the password you want to use to authenticate SNMPv3.
SNMPv3 Privacy Password	Optional parameter. Type the protocol you want to use to decrypt SNMPv3 traps.

Step 12 Click **OK**.

NOTE

If your device uses a communication protocol with a non-standard port or you need to configure the protocols QRadar Risk Manager uses to communicate with specific IP addresses, you must configure Protocols in Configuration Source Management. For more information, see Configuring Sources in the *IBM Security QRadar Risk Manager Users Guide*.

Step 13 Click **Add Device**.

NOTE

If you are adding multiple IP addresses for network devices, select **Discover Devices** and then type the IP addresses for all devices in the next step.

Step 14 Configure the following parameters:

Table 3-2 Credential Parameters

Parameter	Description
IP Address	Type the IP address for the device.
Adapter	Select the adapter type.

Step 15 Click **Add**.

A blue question mark appears in the in the device list for devices that are not backed up.

Step 16 Select the device that you added to the device list, and click **Backup**.

Step 17 Click **Yes**.

The device configuration is added to QRadar Risk Manager when the backup completes. Repeat these steps for each type of network device that you need to add.

You are now ready to use QRadar Risk Manager with your device.

After you add all the required devices, you can configure protocols. For more information, see the *IBM Security QRadar Risk Manager User Guide.*

Adding devices managed by a Juniper Networks NSM console

Use Configuration Source Management to add all devices from a Juniper Networks NSM console to QRadar Risk Manager.

The Juniper Networks NSM console contains the configuration and device information for all Juniper Networks routers and switches managed by the Juniper Networks NSM console, almost as a file repository for Juniper Networks devices. QRadar Risk Manager can obtain device configurations for all supported Juniper adapters.

Before you begin

Before you start adding your devices to QRadar Risk Manager, you need to understand and be aware of supported software versions, credentials, and required commands for your network devices. Use the information in **Table A-1, "Adapter integration requirements"** to understand these requirements.

Juniper Networks NSM does not support SNMP. For this reason, you do not need to enter any values for the SNMP parameters.

To add devices managed by a Juniper Networks NSM console:

Step 1 Click the **Admin** tab.

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

Step 3 On the Risk Manager pane, click **Configuration Source Management**.

Step 4 On the navigation menu, click **Credentials**.

Step 5 On the Network Groups pane, click **Add a new network group (+)**.

Step 6 Type a name for the network group, and click **OK**.

Step 7 Type the IP address of your device, and click **Add (+)**. Repeat this step for each address that you need to add.

Note: *Ensure that the addresses that you add appear in the Network address box beside the Add address box.*

You can type an IP address, a range of IP addresses, a CIDR subnet, or a wildcard. For example, to use a wildcard type 10.1.*.* or to use a CIDR use 10.2.1.0/24.

Step 8 On the Credentials pane, click **Add a new credential set (+)**.

Step 9 Type a name for the credential set, and click **OK**.

Step 10 Select the name of the credential set that you created.

Step 11 Configure values for the following parameters:

Table 3-1 Parameters for devices

Parameter	Description
Username	Type a valid username to log in to the Juniper NSM web services. For Juniper NSM web services, this username must be able to access the Juniper NSM server.
Password	Type the password for the device.
Enable Password	This parameter is not required for devices managed by a Juniper Networks NSM console.

Note: *Juniper Networks NSM does not support SNMP.*

Step 12 Click **OK**.

Step 13 Click **Discover from NSM**.

Step 14 Configure the following parameters:

Table 3-2 Credential Parameters

Parameter	Description
IP Address	Type the IP address for Juniper Networks NSM console.

Table 3-2 Credential Parameters (continued)

Parameter	Description
Username	Type the username that is required to access the Juniper NSM web services. This username must be able to access the Juniper NSM server.
Password	Type the password that is required to aces the Juniper NSM web services.

Step 15 Click **OK**, and then click **GO** to refresh the device list.

Step 16 Select the device that you added to the device list, and click **Backup**.

Step 17 Click **Yes**.

The device configuration is obtained for all Juniper Network devices managed by the Juniper NSM console.

You are now ready to use QRadar Risk Manager with your device.

After you add all the required devices, you can configure protocols. For more information, see the *IBM Security QRadar Risk Manager User Guide.*

A SUPPORTED ADAPTERS

QRadar Risk Manager integrates with many manufacturers and vendors of security products. Our list of supported adapters and documentation is constantly growing. If an adapter doesn't appear in this document for your network device, contact your sales representative.

The information found in **Table A-1** provides the information necessary to integrate an adapter. The following information for each adapter is provided:

- **Device Support** - Provides the product name and version supported.
- **Supports Neighbor Data** - This parameter indicates if neighbor data is supported for this adapter. You can obtain neighbor data from a device using Simple Network Management Protocol (SNMP) and a command line interface (CLI), if your device supports neighbor data.
- **SNMP Discovery** - Specifies if the device allows discovery using SNMP.
- **Required Credential Parameters** - Specifies the necessary access requirements for QRadar Risk Manager and the device to connect. On the Configuration Source Management window of QRadar Risk Manager, you must configure the necessary device credentials. Make sure the device credentials configured in the QRadar Risk Manager match the credentials configured in the device.
- **Connection Protocols** - Specifies the supported protocols for the network device.
- **Required Commands** - Specifies the list of commands that the adapter requires to log in and collect data. The credentials QRadar Risk Manager uses must have the proper privileges to run the listed commands on the adapter.
- **Files Collected** - Specifies the list of files that the adapter must be able to access. To access these files, the appropriate credentials must be configured for the adapter.

Generic SNMP devices do not have routes and therefore, do not transmit traffic.

Table A-1 Adapter integration requirements

Adapter	Supported Version	Supports Neighbor Data	SNMP Discovery	Required Credential Parameters	Device Access	Required Commands	Files Collected
Check Point Secure Platform Appliances	R65 and above	No	Matches NGX in SNMP sysDescr	Username, Password, and Enable Password (type the expert mode password) ***Note:*** *Credential parameters not required may be left blank*.	• Telnet • SSH	hostname dmidecode ver uptime dmesg route -n show users ifconfig -a echo $FWDIR	rules.C objects.C implied_rules.C Standard.pf snmpd.com
Cisco CatOS		Yes	Matches CATOS or Catalyst Operating System in SNMP sysDescr	Username, Password, and Enable Password ***Note:*** *Credential parameters not required may be left blank.*	• Telnet • SSH	show version whichboot show module show mod ver show system show flash devices show flash ... show snmp ifalias show port ifindex show port ifindex show interface show port show spantree show ip route show vlan show vtp domain show arp show cdp show cam dynamic show port status show counters	

Table A-1 Adapter integration requirements (continued)

Adapter	Supported Version	Supports Neighbor Data	SNMP Discovery	Required Credential Parameters	Device Access	Required Commands	Files Collected
Cisco IOS	10.1 and above for routers, switches, and Aironet	Yes	Matches ISO or Cisco Internet Operation System in SNMP sysDescr	Username, Password, and Enable Password ***Note:*** *Credential parameters not required may be left blank.*	• Telnet • SSH+SCP • TFTP	show version show running-config show snmp show install running show file systems show module show power show inventory show mod version show diagbus show diag show startup-config show access lists show interfaces show ip ospf interface show ip eigrp interface show ip eigrp neighbors show ip route eigrp show object-group show standby show vrrp show glbp show ip ospf show ip protocols show ip eigrp topology show spanning-tree show vlan show vtp status show ip arp show cdp neighbors detail show ipv6 neighbors show mac-address-table dynamic show ip ospf neighbor show eigrp neighbors show ip bgp neighbors set terminal length	

Table A-1 Adapter integration requirements (continued)

Adapter	Supported Version	Supports Neighbor Data	SNMP Discovery	Required Credential Parameters	Device Access	Required Commands	Files Collected
Cisco Security Appliances	• Adaptive Security Appliances (ASA) running Private Internet Exchange (PIX) • ASA Routers or Switches with Firewall Service Modules (FWSM)	Yes	Matches PIX or Adaptive Security Appliance or Firewall Service Module in SNMP sysDescr	Username, Password, and Enable Password ***Note:*** *Credential parameters not required may be left blank.*	• Telnet • SSH+SCP	show pager terminal pager 0 show running-config show version change system change context <admin-context> change context <context> get startup-config show names show ipv6 interface show interface detail show interface terminal pager 24 The show pager command must be enabled to access accounts using QRadar Risk Manager. The terminal pager commands are used to set and reset paging behavior. The change system command is issued to detect if this system has multi-context configurations and to determine the admin-context. The change context command is only required if the preceding command has a multi-context configuration or admin configuration context. The change context <context> command is used for each context on the ASA device.	

Table A-1 Adapter integration requirements (continued)

Adapter	Supported Version	Supports Neighbor Data	SNMP Discovery	Required Credential Parameters	Device Access	Required Commands	Files Collected
Juniper Networks JUNOS	9.x and above	Yes	Matches SNMP sysOID: 1.3.6.1.4.1.2636	Username and Password ***Note:*** *Credential parameters not required may be left blank.*	• Telnet • SSH+SCP	show version show system uptime show chassis hardware show chassis firmware show chassis mac-address show chassis routing-engine show configuration snmp show snmp mib walk system configure show configuration firewall show configuration firewall family inet6 show configuration security show configuration seciruty zones show interfaces show interfaces filters show ospf interface detail show bgp neighbor show configuration routing-option show arp no-resolve show ospf neighbor show rip neighbor show bgp neighbor show ipv6 neighbors	
Juniper Networks NSM	IDP appliances managed using NSM	No	None	Username and Password for admin ***Note:*** *Credential parameters not required may be left blank.*	SOAP over HTTP		

Table A-1 Adapter integration requirements (continued)

Adapter	Supported Version	Supports Neighbor Data	SNMP Discovery	Required Credential Parameters	Device Access	Required Commands	Files Collected
Juniper Networks ScreenOS	Firewalls running ScreenOS	Yes	Matches netscreen or SSG in SNMP sysDescr	Username and Password ***Note:*** *Credential parameters not required may be left blank.*	• Telnet • SSH	set console page 0 get system get config get snmp get memory get file info get file get service get group address **<zone>** **<group>** get address get service group get service group **<variable>** get interface get interface **<variable>** get policy all get policy id **<variable>** get admin user get route get arp get mac-learn get counter statistics interface **<variable>** Where: **<zone>** is the zone data returned from the get config command. **<group>** is the group data returned from the get config command. **<variable>** is a list of returned data from a get service group, get interface, or get policy id command.	

B NOTICES AND TRADEMARKS

What's in this appendix:

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 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 *www.ibm.com/legal/copytrade.shtml*.

INDEX