IBM Security QRadar Risk Manager
Version 7.1.0 (MR1)

User Guide

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

CONTENTS

ABOUT THIS GUIDE

5 USE THE TOPOLOGY

6 USING THE POLICY MONITOR

7 INVESTIGATING CONNECTIONS

8 VIEW DEVICE CONFIGURATIONS

9 MANAGING IBM SECURITY QRADAR RISK MANAGER REPORTS

10 USING SIMULATIONS

11 USING TOPOLOGY MODELS

A POLICY MONITOR QUESTIONS

B VIEWING AUDIT LOGS

ABOUT THIS GUIDE

The *IBM Security QRadar Risk Manager Users Guide* provides information on installing, configuring, and using QRadar Risk Manager.

Intended audience

This guide is intended for the system administrator responsible for configuring IBM Security QRadar Risk Manager in your network. 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 IBM SECURITY QRADAR RISK MANAGER

IBM Security QRadar Risk Manager is a separately installed appliance for monitoring device configurations, simulating changes to your network environment, and prioritizing risks and vulnerabilities in your network. The features of QRadar Risk Manager are managed through your Console using the **Risks** tab on your dashboard.

QRadar Risk Manager leverages data collected by IBM Security QRadar SIEM, configuration data from network and security devices (firewalls, routers, switches, or intrusion prevention systems (IPSs), vulnerability feeds, and third-party security sources. These data sources allow QRadar Risk Manager to identify security, policy, and compliance risks within your network security infrastructure and the probability of those risks being exploited.

QRadar Risk Manager proactively alerts you to discovered risks. These risks are displayed as offenses on the Offenses tab. This data is analyzed and reported in the context of all other data that QRadar SIEM is processing. QRadar Risk Manager allows you to evaluate and manage risk at an acceptable level based on the risk tolerance defined by your company.

You can also use QRadar Risk Manager to query all network connections, view and compare configurations of devices, view and filter the topology model of your network, and simulate and predict possible effects for changing a devices configuration or policies.

QRadar Risk Manager allows you to define a set of policies (or questions) about your network and monitor those for changes. For example, if you want to deny unencrypted protocols in your Demilitarized Zone (DMZ) from the Internet, you can define a Policy Monitor question to detect unencrypted protocols. Submitting the question returns a list of unencrypted protocols communicating from the Internet to your DMZ and allows you to determine which unencrypted protocols are security risks. When the level of acceptable risk is defined, alerts are generated for new risks discovered in the network.

QRadar Risk Manager consists of the following components:

- **Connections**
- **Configuration Monitor**
- **Topology**
- **Policy Monitor**
- **Simulation**
- **QRadar Risk Manager reports**

Connections

Use the Connections page to monitor the network connections of local hosts. You can run queries and reports on the network connections of local hosts based on any applications, ports, protocols, and websites the local hosts have communicated with.

Using the Connections page, you can:

- Search connections
- Search a subset of connections (sub-search)
- View connection information grouped by various options
- Export connections in XML or CSV format
- Use the interactive graph to view connections in your network

For more information on Connections, see Investigating connections.

Configuration Monitor

Use Configuration Monitor to review and compare device configuration, allowing you to enforce security policies and monitor device modifications within your network.

Device configurations may include switches, routers, firewalls, and IPS devices in your network. For each device, you can view device configuration history, interfaces, and rules. You can also compare configurations within a device and across devices.

The device configuration information is also used to create the enterprise-wide representation of your network topology, which allows you to determine allowed and denied activity across your network. Device configuration enables you to identify inconsistencies and configuration changes that introduce risk in your network.

For more information on device configurations, see **View device configurations**.

Topology

Topology is a graphical representation depicting the Network Layer (layer 3 of the Open Systems Interconnection (OSI) model) of your network based on the devices added from Configuration Source Management.

Using the interactive graph in the Topology allows you to view connections between devices, virtualized network security devices that have multiple contexts, assets, Network Address Translation (NAT) devices, NAT indicators and information about NAT mappings. You can search for events, devices, paths, and save network layouts.

In Topology, you can query the Transport Layer (layer 4) and filter network paths based on port and protocol. The graph and connection information is created from detailed configuration information obtained from network devices, such as firewalls, routers, and IPS systems.

For more information on using the Topology, see **Use the topology**.

Policy Monitor

Use Policy Monitor to define specific questions about risk in your network and submit the question to QRadar Risk Manager.

QRadar Risk Manager evaluates the parameters you've defined in your question and returns assets in your network to help you assess risk. The questions are based on a series of tests that can be combined and configured as required. QRadar Risk Manager provides a large number or predefined Policy Monitor questions, and allows the creation of custom questions. Policy Monitor questions can be created for the following situations:

- Communications that have occurred; or
- Possible communications based on the configuration of firewalls and routers
- Actual firewall rules (device tests)

The Policy Monitor uses data obtained from configuration data, network activity data, network and security events, and vulnerability scan data to determine the appropriate response. QRadar Risk Manager provides policy templates to assist you in determining risk across multiple regulatory mandates and information security best practices, such as PCI, HIPPA, and ISO 27001. You can update the templates to align with your corporate defined information security policies. When the response is complete, you can accept the response to the question and define how you want the system to respond to unaccepted results.

The Policy Monitor allows up to 10 questions to be actively monitored. When a question is monitored, QRadar Risk Manager continuously evaluates the question for unapproved results. As unapproved results are discovered, QRadar Risk Manager has the ability to send email, display notifications, generate a syslog event or create an offense in QRadar SIEM.

For more information on the Policy Monitor, see **Using the Policy Monitor**.

Simulation

Use Simulation to define, schedule, and perform exploit simulations on your network.

You can create a simulated attack on your topology based on a series of parameters that are configured in a similar manner to the Policy Monitor. You can create a simulated attack on your current network topology, or create a topology model. A topology model is virtual topology that allows you to make modifications on the virtual topology and simulate an attack. This enables you to simulate how alterations to network rules, ports, protocols, or allowed or denied connections can affect your network. Simulation is a powerful tool to determine the risk impact of proposed changes to your network configuration before the changes are implemented.

After a simulation is complete, you can review the results. If you want to accept the results, you can configure the simulation mode, which allows you to define how you want to respond to unaccepted results.

QRadar Risk Manager allows up to 10 simulations to be actively monitored. When a simulation is monitored, QRadar Risk Manager continuously analyzes the topology for unapproved results. As unapproved results are discovered, QRadar Risk Manager has the ability to send email, display notifications, generate a syslog event or create an offense in QRadar SIEM.

For more information on Simulations, see **Using simulations**.

QRadar Risk Manager reports

Use the Reports tab to view specific reports, based on data available in QRadar Risk Manager, such as connections, device rules, and device unused objects.

The following report options are specific to QRadar Risk Manager:

- **Connections** - A connections report displays connection diagrams for your network devices that occurred during your specified time frame.
- **Device rules** - A device rule report displays the rules configured on your network device during your specified time frame. You can view the following rule types for one or many network devices using this report option:
  - Most used accept rules
  - Most used deny rules
  - Least used accept
  - Least used deny rules
  - Shadowed rules
  - Unused object rules

- **Device unused objects** - A device unused object report produces a table with the name, configuration date/time, and a definition for any object reference groups that are not in use on the device. An object reference group is a generic term used to describe a collection of IP addresses, CIDR addresses, host names, ports, or other device parameters which are grouped together and assigned to rules on the device.

For more information on Reports, see Managing IBM Security QRadar Risk Manager reports.

Supported web browsers

You can access the Console from a standard web browser. When you access the system, a prompt is displayed asking for a username and a password, which must be configured in advance by the QRadar SIEM administrator.

Table 1-1 Supported Web Browsers

Web browser	Supported versions
Mozilla Firefox	• 10.0 Due to Mozilla’s short release cycle, we cannot commit to testing on the latest versions of the Mozilla Firefox browser. However, we are fully committed to investigating any issues that are reported.
Microsoft Windows Internet Explorer, with Compatibility View Enabled	• 8.0 • 9.0 For instructions on how to enable Compatibility View, see **Enable compatibility view for Microsoft Internet Explorer**.

Enable compatibility view for Microsoft Internet Explorer

To enable Compatibility View for Microsoft Internet Explorer web browsers:

Step 1 Press F12 to open the Developer Tools window.

Step 2 From the **Browser Mode** list box, select the version of your web browser.

Step 3 From the **Document Mode** list box, select the version of your web browser.

Step 4 Close the Developer Tools window.

Log In to IBM Security QRadar Risk Manager

To log in to QRadar Risk Manager:

Step 1 Open your web browser.

Step 2 Type the following address in the address bar:

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

Where **`<IP Address>`** is the IP address of the QRadar SIEM system. QRadar Risk Manager is managed using the **Risks** tab of QRadar SIEM.

Step 3 Type the default user name and password.

User name: **`admin`**

Password: **`<password>`**

Where **`<password>`** is the password assigned to you by your Network or QRadar SIEM System Administrator. If you log in and do not see the **Risks** tab, ensure the User Role for Risk Manager is enabled for your account. For more information, see the *IBM Security QRadar Risk Manager Installation Guide*.

Step 4 Click **Login To QRadar**.

NOTE

If you are using a Mozilla Firefox web browser then you must add an exception to Mozilla Firefox to log in to QRadar SIEM. For more information, see your Mozilla Firefox documentation. If you are using a Microsoft Internet Explorer browser, a web site security certificate message is displayed. You must select the **Continue to this website** option to log in to QRadar SIEM.

Unsupported IBM Security QRadar Risk Manager features

QRadar Risk Manager does not support the following features:

- High Availability (HA)
- Dynamic Routing
  - Border Gateway Protocol (BGP)
  - Open Shortest Path First (OSPF)
  - outing Information Protocol (RIP)
  - Intermediate System to Intermediate System (IS-IS)
- IPv6
- Non-contiguous Network Masks
- Store and Forward

  Store and Forward allows you to manage schedules that control when to start and stop forwarding events from your dedicated Event Collector appliances to Event Processors in your deployment. This feature is not supported when using QRadar Risk Manager.

2 THE USER INTERFACE

System administrators interact with IBM Security QRadar Risk Manager by sorting results, investigating IP addresses, and resizing columns.

Use the navigation options to navigate IBM Security QRadar SIEM. Never use the browser **Back** button.

Sort results

On the Connections, Configuration Monitor, Policy Monitor, Simulations, and Topology Model pages, you can sort tables in ascending or descending order by clicking on a column heading.

An arrow at the top of the column indicates the direction of the sort. Click on the heading to toggle the results from descending to ascending order.

For example, to sort connections by the **Last Packet Time** field:

Click the Last Packet Time column heading. An arrow is displayed in the column heading to indicate the results are sorted in descending order. Click the Last Packet Time column heading again to sort the information in ascending order.

Investigate IP addresses

You can right-click on a device IP addresses to further filter the display or access additional information. For example, right-clicking an IP address from the **Device IP** field on the Configuration Monitor page displays the options found in Table 2-2.

Table 2-2 IP Address Options

Menu	Sub-Menu	Sub-Menu	Description
Filter on	Not applicable	Not applicable	Allows you to filter on the selected connection, depending on the selected parameter.
View Connection Events	Not applicable	Not applicable	Allows you to view connections for the selected IP address.

Table 2-2 IP Address Options (continued)

Menu	Sub-Menu	Sub-Menu	Description
More options	Navigate	View By Network	Displays the List of Networks window, which displays the network activity for the network to which the selected IP address is associated.
		View Source Summary	Displays the source summary window, which displays all offenses associated with the selected source.
		View Destination Summary	Displays the destination summary window, which displays all offenses associated with the selected destination.
	Information	DNS Lookup	Searches for DNS entries based on the IP address.
		WHOIS Lookup	Searches for the registered owner of a remote IP address. The default system server is whois.crsnic.net.
		Port Scan	Performs an NMAP scan of the selected IP address. This option is only available if NMAP is installed on your system. For more information about installing NMAP, see your vendor documentation.
		Asset Profile	Displays asset profile information. This menu option is only available when profile data has been acquired either actively (through a scan) or passively (through flow sources). For information, see the *QRadar Administration Guide.*
		Search Events	Allows you to search events.
		Search Flows	Allows you to search for flows.
		Search Connections	Allows you to search connections. For information, see **Investigating connections**.
		Switch Port Lookup	Allows you to determine the switch port on a Cisco IOS device for the selected IP address. This option only applies to switches that are discovered using the Discover Devices option in Configuration Source Management. For more information, see **Discover devices**.
		View Topology	Allows you to view the Topology. For more information, see **Use the topology**.
	TNC Recommendations		Allows you to restrict or deny network access to users based on user name or other credentials.

For more information on customizing the right-click menu, see the *Customizing the Right-Click Menu Technical Note*.

Resize columns

You can resize the width of most table columns in QRadar Risk Manager. Place your mouse over the line that separates the columns and drag the edge of the column to the preferred width.

Columns can also be resized automatically by double-clicking the line separating two columns. This resizes the column to the left of the line to the width of the largest data value in the table.

3 CONFIGURE IBM SECURITY QRADAR RISK MANAGER SETTINGS

You can configure the access settings for QRadar Risk Manager through a web-based system administration from the **Admin** tab of IBM Security QRadar SIEM.

If you have the appropriate permissions you can configure several appliance settings for IBM Security QRadar Risk Manager using a web-based system administration.

Administrators can perform the following tasks:

- Configure devices that QRadar Risk Manager can access through the local firewall. For more information, see **Configure firewall access**.
- Update the email server for QRadar Risk Manager. For more information, see **Update your QRadar Risk Manager set-up**.
- Configure the interface roles for a host. For more information, see **Configure user interface roles**.
- Change the password for a host. For more information, see **Change passwords**.
- Update the system time. For more information, see **Update the system time**.

Configuration changes made through the web-based system administration take place immediately when you save or apply changes.

Configure firewall access

You can configure local firewall access for QRadar Risk Manager, which allows you to enable or disable communications between QRadar Risk Manager and specific IP addresses, protocols, and ports.

You can also define a list of IP addresses allowed to access the web-based system administration. By default, these fields are left blank, which does not restrict communication to QRadar Risk Manager. However, when you add an IP address, only that IP address is granted access to the system. All other IP addresses are blocked.

NOTE

You must include the IP address of the client desktop that you use to access QRadar Risk Manager. Failing to do so might affect connectivity.

To configure firewall access in QRadar Risk Manager, perform the following steps:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System Management** icon.

Step 4 Log in to access the web-based System Administration.

Username: `root`

Password: `<password>`

The username and password fields are case sensitive.

Step 5 From the menu, select **Managed Host Config > Local Firewall**.

Step 6 In the Device Access pane, configure the IP addresses, ports, and protocols you want to add as a local firewall rule in QRadar Risk Manager.

Step 7 In the **IP Address** field, type the IP addresses of the devices you want to access.

Step 8 From the **Protocol** drop-down list box, select the protocol you want to enable access for the specified IP address and port:

- **UDP** - Allows UDP traffic.
- **TCP** - Allows TCP traffic.
- **Any** - Allows any traffic.

Step 9 In the **Port** field, type the port on which you want to enable communications and click **Allow**.

Step 10 Type the IP address of the managed host that you want to allow access to the web-based system administration and click **Allow**.

Only IP addresses listed here have access to the web-based system administration. If you leave the field blank, all IP addresses have access.

Step 11 Click **Apply Access Controls**.

Update your QRadar Risk Manager set-up

The QRadar Risk Manager set-up allows you to define the mail server used for QRadar Risk Manager notifications.

To configure the QRadar Risk Manager mail server address:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System Management** icon.

Step 4 Log in to the System Administration page. The default is:

Username: `root`

Password: **`<password>`**

The username and password are case sensitive.

Step 5 From the menu, select **Managed Host Config > QRM Setup**.

Step 6 In the **Mail Server** field, type the IP address or hostname for the mail server you want QRadar Risk Manager to use.

QRadar Risk Manager uses this mail server to distribute alerts and event messages. To use the mail server provided with QRadar Risk Manager, type **localhost**.

Step 7 Click **Apply Configuration**.

Step 8 Wait for the screen to refresh before attempting to make further changes.

Configure user interface roles

If your appliance contains multiple network interfaces, you can assign specific roles to the network interfaces on each system.

For assistance with determining the appropriate role for each interface, contact Customer Support.

To assign roles to a network interface, perform the following steps:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System Management** icon.

Step 4 Log in to the System Administration window. The default is:

Username: **`root`**

Password: **`<password>`**

The username and password are case sensitive.

Step 5 From the menu, select **Managed Host Config > Network Interfaces.**

Step 6 For each interface listed, select the role you want to assign to the interface using the Role list box.

In most cases, the current configuration is display cannot be edited.

Step 7 Click **Save Configuration**.

Step 8 Wait for the screen to refresh before attempting to make further changes.

Change passwords

To change the root password on QRadar Risk Manager:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System Management** icon.

Step 4 Log in to access the System Administration settings.

Username: `root`

Password: `<password>`

The username and password are case sensitive.

Step 5 From the menu, select **Managed Host Config > Root Password**.

Step 6 In the **New Root Password** field, type the root password used to access the web-based system administration, and then re-type the password in the **Confirm New Root Password** field.

Step 7 Click **Update Password**.

Update the system time

You must contact customer support before updating the system time for the QRadar Risk Manager appliance.

All system time changes must be saved on the Console. The Console then distributes the updated time settings to all of the managed hosts in your deployment.

For more information on configuring the system time on your Console, see the *IBM Security QRadar SIEM Administration Guide*.

To update the time settings for your system, perform the following steps:

Step 1 Click the **Admin** tab.

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

Step 3 Click the **System Management** icon.

Step 4 Log in to access the System Administration settings.

Username: `root`

Password: `<password>`

The username and password are case sensitive.

Step 5 From the menu, select **Managed Host Config > System Time**.

CAUTION

*The time settings window is divided into two sections. You must save each setting before continuing. For example, when you configure System Time, you must click **Apply** within the System Time pane before continuing.*

Step 6 Click **Set time**.

Step 7 In **System Time,** select the current date and time you want to assign to the managed host, and then click **Apply**.

Step 8 In the **Hardware Time** pane, select the current date and time you want to assign to the managed host, and then click **Save**.

4 MANAGE CONFIGURATION SOURCES

Using Configuration Source Management on the **Admin** tab in IBM Security QRadar SIEM, you can configure credentials, add or discover devices, view device configurations, and backup device configurations in QRadar Risk Manager. The data obtained from devices in your network is used to populate the Topology. You must have administrative privileges to access Configuration Source Management functions from the **Admin** tab in QRadar SIEM.

To set-up your configuration sources, you must:

1. Configure your device credentials. For more information, see **Configure credentials**.
2. Discover or import devices. There are two ways to add network devices to QRadar Risk Manager; discover devices using Configuration Source Management or Import a list of devices from a CSV file using Device Import. For more information, see **Discover devices** and **Import devices**.
3. Obtain device configuration information from each of your devices. For more information, see **Obtain device configuration**.
4. Ensure all updates to device configurations are captured. For more information, see **Manage backup jobs**.
5. Set up the discovery schedule to ensure new devices are automatically discovered. For more information, see **Configure the discovery schedule**.

Using Configuration Source Management, you can also:

- Add, edit, search, and delete configuration sources. For more information, see **Manage devices**.
- Configure or manage communication protocols for your devices. For more information, see **Configure protocols**.

NOTE

If you are using the Juniper NSM device, you must also obtain configuration information.

For detailed information about adapters used to communicate with devices from specific manufacturers, see *IBM Security QRadar Risk Manager Configuring Adapters Guide*.

Configure credentials

Administrators must configure credentials to allow QRadar Risk Manager to connect to devices in the network. Credentials allow QRadar Risk Manager to access and download the configuration of devices such as firewalls, routers, switches, or IPSs.

Configuration Source Management allows an administrator to input device credentials, allowing QRadar Risk Manager to gain access to a specific device. Individual device credentials can be saved for a specific network device, or if multiple network devices use the same credentials, you can assign credentials to a group.

For example, if all firewalls in the organization have the same username and password then the credentials are associated with the address sets for all the firewalls and used to backup device configurations for all firewalls in your organization.

If a network credential is not required for a specific device, the parameter can be left blank in Configuration Source Management. For a list of required adapter credentials, see the *IBM Security QRadar Risk Manager Configuring Adapters Guide*.

You can assign different devices in your network to network groups, allowing you to group together credential and address sets for your devices.

A credentials set contains information such as username, and password values for a set of devices.

An address set is a list of IP addresses that define a group of devices that share the same set of credentials.

Each network group can have multiple credential and address sets. You can also configure your QRadar Risk Manager to prioritize how each network group is evaluated. The network group at the top of the list has the highest priority. The first network group that matches the configured IP address are included as candidates when backing up a device. A maximum of three credential sets from a network group are considered.

For example, if your configuration includes these two network groups:

- Network Group 1 includes two credential sets
- Network Group 2 includes two credential sets

QRadar Risk Manager attempts to compile a list of a maximum of three credential sets. Since Network Group 1 is higher in the list, both of the credential sets in Network Group 1 are added to the list of candidates. Since three credential sets are required, the first credential set in the Network Group 2 is added to the list.

When a credential set successfully accesses a device, QRadar Risk Manager uses that credential set for subsequent attempts to access the device. If the credentials on that device change, the authentication fails when attempting to access the device. Then, on the next authentication attempt, the QRadar Risk Manager reconciles the credentials again to ensure success.

To configure device credentials:

Step 1 Click the **Admin** tab.

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

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

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

Step 5 On the **Network Groups** pane, click the **Add (+)** icon.

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

Step 7 Move the network group you want to have first priority to the top of the list. You can use the **Move Up** and **Move Down** arrow icons to prioritize a network group.

Step 8 In the **Add Address** field, type the IP address or CIDR range that you want to apply to the network group, then click the **Add (+)** icon.

You can type an IP address range using a dash or wildcard (*****) to indicate a range, such as 10.100.20.0-10.100.20.240 or 1.1.1*. If you type 1.1.1.*, all IP addresses meeting that requirement are included.

Repeat for all IP addresses you want to add to the address set for this network group.

NOTE

When configuring the address set with Juniper Networks NSM or a generic XML adapter, you must type the IP address range or CIDR address range for all the devices managed by Juniper Networks NSM or files for devices in the repository.

Step 9 In the **Credentials** pane, click the **Add (+)** icon.

Step 10 Type a name for the new credential set, and then click **OK**.

Step 11 Type values for the parameters:

Table 4-1 Credential Parameters

Parameter	Description
Username	Type the username for the credential set. ***Note:*** *If you are using a Juniper Networks NSM or a generic XML adapter, type a username that can access the Juniper NSM server or a username that can access the file repository that contains your SED files.*
Password	Type the password for the credential set. ***Note:*** *If you are using Juniper Networks NSM or a generic XML adapter, type the password for the Juniper NSM server or the password to log in to the file repository that contains your SED files.*

Table 4-1 Credential Parameters (continued)

Parameter	Description
Enable Username	Type the username for second level authentication for the credential set.
Enable Password	Type the password for second level authentication for the credential set.
SNMP Get Community	Type the SNMP Get community.
SNMPv3 Authentication Username	Type the username you want to use to authenticate SNMPv3.
SNMPv3 Authentication Password	Type the password you want to use to authenticate SNMPv3.
SNMPv3 Privacy Password	Type the protocol you want to use to decrypt SNMPv3 traps.

Step 12 Move the credential set you want to make first priority to the top of the list. Use the **Move Up** and **Move Down** arrow icons to prioritize a credential set.

Step 13 Repeat for each credential set that you want to add.

Step 14 Click **OK**.

Discover devices

The discovery process uses the Simple Networks Management Protocol (SNMP) and command line (CLI) to discover network devices. After you configure an IP address or CIDR range, the discovery engine performs a TCP scan against the IP address to determine if port 22, 23, or 443 are monitoring for connections. If the TCP scan is successful, and SNMP query is configured to determine the type of device, the SNMP Get Community String is used based on the IP address.

QRadar Risk Manager uses this information to determine which adapter the device should be mapped to when added. QRadar Risk Manager connects to the device and collects a list of interfaces and neighbor information, such as CDP, NDP, or ARP tables. The device is then added to the inventory.

The configured IP address used to initiate the discovery process may not be the assigned IP address for the new device. QRadar Risk Manager adds a device using the IP address for the lowest numbered interface on the device (or lowest loopback address, if any).

Also, if you use the **Crawl the network from the addresses defined above** check box, the IP address of the neighbors collected from the device are re-introduced into the discovery process and the process repeats for each IP address.

NOTE

When performing a device discovery, any device that is not supported but responds to SNMP is added with the Generic SNMP adapter. If you want to perform a path filter through the device with simulated routes, you must manually remove the device

To discover devices:

Step 1 Click the **Admin** tab.

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

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

Step 4 TOn the navigation menu, click **Discover Devices**.

Step 5 Type an IP address or CIDR range.

This IP address or CIDR range indicates the location of devices you want to discover.

Step 6 Click the **Add (+)** icon.

Step 7 If you want to also search for devices in the network from the defined IP address or CIDR range, select the **Crawl the network from the addresses defined above** check box. This check box is selected by default.

Step 8 Click **Run**.

Import devices

Use Device Import to bulk add a list of adapters and their network IP addresses to the Configuration Source Manager using a comma-separated value file (.CSV). The device import list can contain up to 5000 devices, but the list must contain one line for each adapter and its associated IP address in the import file.

For example,

```
<Adapter::Name 1>,<IP Address>
<Adapter::Name 2>,<IP Address>
<Adapter::Name 3>,<IP Address>
```

Where:

`<Adapter::Name>` contains the manufacturer and device name, such as Cisco::IOS.

`<IP Address>` contains the IP address of the device, such as 191.168.1.1.

Table 4-2 Device Import Examples

Manufacturer	Name	Example <Adapter::Name>,<IP Address>
Check Point	SecurePlatform	CheckPoint::SecurePlatform,10.1.1.4
Cisco	IOS	Cisco::IOS,10.1.1.1
Cisco	Cisco Security Appliance	Cisco::SecurityAppliance,10.1.1.2
Cisco	CatOS	Cisco::CatOS, 10.1.1.3
Generic	SNMP	Generic::SNMP,10.1.1.8
Juniper Networks	Junos	Juniper::JUNOS,10.1.1.5

Import a CSV file

You can import a master device list to Configuration Source Management using a CSV (comma-separated values) file.

If you import a list of devices to QRadar Risk Manager, then make a change to an IP address in the CSV file you can duplicate a device accidently in the Configuration Source Management list. For this reason, delete a device from Configuration Source Management before re-importing your master device list.

To import a master device list, perform the following steps:

Step 1 Click the **Admin** tab.

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

Step 3 In the **Plug-Ins** pane, click **Device Import**.

Step 4 Click **Browse**.

Step 5 Locate your CSV file, click **Open**.

Step 6 Click **Import Devices**.

You are now ready to manage devices you have imported. For more information, see **Manage devices**.

If an error displays, then you need to review your CSV file to correct errors, and re-import the file. An import of the CSV file might fail if the device list is structured incorrectly or if the device list contains incorrect information. For example, your CSV file might be missing colons or a command, there could be multiple devices on a single line, or an adapter name might have a typo.

If the device import aborts, then no devices from the CSV file are added to Configuration Source Management.

Manage devices

Using the Devices tab in the Configuration Source Management window, you can manage the devices in your network. Using the Devices tab, you can:

- View all existing devices. For more information, see **View devices**.
- Add a new device. For more information, see **Add a device**.
- Edit an existing device. For more information, see **Edit devices**.
- Delete a device. For more information, see **Delete a device**.
- Search existing devices. For more information, see **Filter the device list**.
- Obtain device configuration for a device. For more information, see **Obtain device configuration**.
- Collect data from a device. For more information, see **Collect neighbor data**.

If you want to discover all devices in your deployment, see **Discover devices**.

View devices

The Devices tab displays all the devices in your deployment. To view devices:

Step 1 Click the **Admin** tab.

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

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

Step 4 Click the **Devices** tab.

The following table describes the parameters on the **Devices** tab:

Table 4-3 Devices Parameters

Parameter	Description
Backup Status	The following icons display the status of the last backup attempt of a device by QRadar Risk Manager: • **Red Exclamation Point** - Indicates an error occurred during the last backup attempt of the device. • **Green Check Mark** - Indicates the device back up completed successfully. • **Yellow Warning Indicator** - Indicates that a warning or exception occurred during a device backup that caused the back up to fail. The most common issue with warning indicators is invalid device credentials. The error message can be viewed by clicking **View Error**. • **Blue Question Mark** - Indicates that no known backup archive exists for this device.
IP Address	The management IP address of the device.
Hostname	The hostname of the device.
Adapter	The adapter name for the device.
Model	The model of the device.

Step 5 To view detailed information for a device configuration, select the device you want to view and click **Open**.

The following table provides information about the Properties pane:

Table 4-4 Properties Parameters

Parameter	Description
IP Address	The IP address of the device. This value is configured when the device is added to Configuration Source Management.
Adapter	The adapter used for the device. This value is configured when the device is added to Configuration Source Management.
Hostname	The hostname of the device, as obtained from the device. This value is obtained from the device during the backup process.
Make	The vendor name for the device. This value is obtained from the device during the backup process.
Model	The model of the device. This value is obtained from the device during the backup process.
Software Version	The currently running software version for the device. This value is obtained from the device during the backup process.
Serial Number	The serial number of the device. This value is obtained from the device during the backup process.
Device Type	The type of device, for example, a router. This value is obtained from the device during the backup process.
Show historical configurations	The check box if you want to view all the recorded revisions. A revision is only recreated when the content of the configuration file changes. Clear the check box if you only want to view the most recent revision of the configuration file.

The following table provides information about the Configurations pane:

Table 4-5 Configurations Parameters

Parameter	Description
Config	The name of the configuration file, as obtained from the device during the backup process. This list may include multiple entries, which includes a revision history.
Date	The date that the configuration file was generated as a result of the backup process. If the backup process did not detect any configuration changes since the last backup process, the date indicates the date of the previous backup. The date only updates to the latest backup when configuration changes are detected.

Add a device

QRadar Risk Manager enables you to add individual network devices and the adapter using Configuration Source Management. The following section instructs you on adding an individual device to the device list in Configuration Source Management.

For information on “bulk adding” multiple devices using a CSV file, see **Import devices**.

To add an individual device, perform the following steps:

Step 1 Click the **Admin** tab.

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

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

Step 4 On the navigation pane, click **Add Device**.

Step 5 Configure values for the parameters:

- **IP Address** - Type the management IP address of the device.
- **Adapter** - From the **Adapter** drop-down list box, select the adapter you want to assign to this device.

Step 6 Click **Add**.

If necessary, click **Go** to refresh the adapter list.

Edit devices

Editing a device enables you to correct the IP address or adapter type if there is an error or your if your network has changed and you need to re-assigned an IP address.

To edit a device, perform the following steps:

Step 1 Click the **Admin** tab.

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

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

Step 4 Select the device you want to edit.

Step 5 Click **Edit**.

Step 6 Configure values for the parameters:

- **IP Address** - Type the IP address you want to assign to this device.
- **Adapter** - From the **Adapter** drop-down list box, select the adapter you want to assign to this device.

Step 7 Click **Save**.

Delete a device

You can delete a device from QRadar Risk Manager. A deleted device is removed from Configuration Source Management, Configuration Monitor, and Topology.

After you delete a device, the process to remove the device from the Topology may require several minutes.

To delete a device from Topology:

Step 1 Click the **Admin** tab.

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

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

Step 4 Click the **Devices** tab.

Step 5 Select the device you want to delete.

Step 6 Click **Remove**.

Step 7 Click **Yes** to delete the device.

Filter the device list

QRadar Risk Manager can handle up to 5000 network devices in Configuration Source Management. Large numbers of network devices can make scrolling through the device list extremely tedious. To reduce the effort required to find a device in the list, a filter is available to the left of the device list.

To reset a filter, select **Interface IP Address**, clear the **IP/CIDR** address, then click **Go**.

To filter your device list:

Step 1 Click the **Admin** tab.

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

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

Step 4 Click the **Devices** tab.

Step 5 Using the drop-down list box to the left side of the device list, select a filter:

Table 4-6 Device Filters

Search Option	Description
Interface IP Address	Filters for devices that have an interface matching either an IP address or CIDR range. Type the IP address or CIDR range on which you want to search in the **IP/CIDR** field. For example, if you type a search criteria of 10.100.22.6, the search results return a device with an IP address of 10.100.22.6. If you type a CIDR range of 10.100.22.0/24, all devices in the 10.100.22.* are returned.
Admin IP Address	Filters the device list based on the administrative Interface IP address. An administrative IP address is the IP address that uniquely identifies a device. Type the IP address or CIDR range on which you want to search in the **IP/CIDR** field.

Table 4-6 Device Filters (continued)

Search Option	Description
OS Version	Filters the device list based on the operating system version devices are running. Select values for the following parameters: • **Adapter** - Using the drop-down list box, select the type of adapter you want to search. • **Version** - Using the drop-down list box, select the search criteria for the version. For example, greater than, less than, or equal to the specified value. Type the version number in the field on which you want to search. If you do not select a search option for Version, the results include all devices that are configured with the selected adapter, regardless of version.
Model	Filters the device list based on the vendor and model number. Configure values for the following parameters: • **Vendor** - Using the drop-down list box, select the vendor you want to search. • **Model** - Type the model you want to search.
Hostname	Filters the device list based on the hostname. Type the hostname on which you want to search in the **Hostname** field.

Step 6 Click **Go**.

All search results matching your criteria are displayed in the table.

Obtain device configuration

After you configure credential sets and address sets to access network devices, you must backup your devices to download the device configuration so QRadar Risk Manager can include the device information in the Topology. The process of backing up a device to obtaining a device configuration can be completed for a single device in the device list, or you can backup all devices from the **Devices** tab.

For more information about scheduling automated backups of device configurations from the **Jobs** tab, see **Manage backup jobs**.

Step 1 Click the **Admin** tab.

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

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

Step 4 Click the **Devices** tab.

Step 5 Choose one of the following options:

a If you want to obtain the configuration for all devices, click **Backup All** in the navigation pane. Go to Step 7.

b If you want to obtain the configuration for a specific device, select the individual device. To select multiple devices to backup, hold down the CTRL key and select all necessary devices. Go to Step 6.

Step 6 Click **Backup**.

Step 7 Click **Yes** to continue.

Step 8 If necessary, click **View Error** to view the details of an error. After correcting the error, click **Backup All** in the navigation pane.

For more information about viewing the details of network device backups, see **View device configurations**.

Collect neighbor data

Use the discovery process to obtain neighbor data from a device using SNMP and a command line interface (CLI). Neighbor data is used in the Topology to draw the connection lines to display the graphical topology map of your network devices. The discover button allows you to select single or multiple devices and update the neighbor data for a device. This information is used to update the connection lines for one or many devices in the Topology.

To obtain neighbor data from a device:

Step 1 Click the **Admin** tab.

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

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

Step 4 Click the **Devices** tab.

Step 5 Select the device for which you want to obtain data. To select multiple devices, hold down the CTRL key and select all necessary devices.

Step 6 Click **Discover**.

Step 7 Click **Yes** to continue.

If you select multiple devices, then the discover process can take several minutes to complete.

Select **Run in Background** to work on other QRadar Risk Manager or QRadar SIEM tasks.

Collect data from a file repository

You can use QRadar Risk Manager to obtain device XML SED files or input files containing basic device configuration from a network file repository. The file repository hosting the files must support the FTP or SFTP protocol. QRadar Risk Manager obtains device information from all SED XML files located in the remote file directory of the file repository.

The Configuration Collection Toolkit allows a host to collect XML SED files and act as a file repository for QRadar Risk Manager or create a bridge to disconnected devices in your network. For more information, see **Configuration Collection Toolkit**.

To collect data from a file repository:

Step 1 Click the **Admin** tab.

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

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

Step 4 Click the **Devices** tab.

Step 5 Select **Discover from Repository**.

Step 6 Configure values for the following parameters:

- **Protocol** - From the **Protocol** drop-down list box, select **FTP** or **SFTP** as the communications protocol to access your configuration file repository.
- **IP Address** - Type the configuration file repository IP address.
- **Remote Path** - Type the remote file path to the directory containing your SED XML files. The default file path for SED files is **`<install directory>/output`**.

  Where **`<install directory>`** is the location of the extracted **`ziptie-adapter.<date>-<build>.zip`**.
- **Username** - Type the username required to log in to the system hosting the configuration file repository.
- **Password** - Type the password required to log in to the system hosting the the configuration file repository.

Step 7 Click **OK** to discover a device from a repository.

If successful, a log message is displayed detailing the source connection and the discovered SED XML files.

Step 8 Click **Go** to refresh the device list.

Manage backup jobs

A job refers to a backup job, which enables you to automatically backup configuration information for all devices in the **Devices** tab on a schedule. Using the **Jobs** tab from the Configuration Source Management, you can create backup jobs for all devices, or individual groups of devices in Configuration Source Management.

Any backup job that you define in the Configuration Source Management page does not affect your QRadar SIEM backup configuration using the **Backup and Recovery** icon in the **Admin** tab. The Backup and Recovery functionality obtains configuration information and data for QRadar SIEM. The Backup job in the Configuration Source Management page for QRadar Risk Manager only obtains information for external devices.

View backup jobs

Jobs created in QRadar Risk Manager are displayed on the **Jobs** tab along with the details, such as the job name, the group of devices assigned to the job, the job type and any additional comments added by the user who created the backup job.

To view backup jobs:

Step 1 Click the **Admin** tab.

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

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

Step 4 Click the **Jobs** tab.

The **Jobs** tab is displayed showing all current backup jobs and the associated settings.

Table 4-7 Backup Jobs Parameters

Parameter	Description
Job Type Icon	Indicates the icon representing the job type.
Name	Indicates the name of the backup job.
Group	Indicates the group to which this backup job was assigned.
Type	Indicates the type of backup job. This is the backup job.
Comment	Indicates any comment provided for this job.

Step 5 Double-click any job you want to view in greater detail.

The following table provides job information:

Table 4-8 Job Parameters

Parameter	Description
Name	Indicates the name of the backup job.
Group	Indicates the group to which the backup job is assigned.
Comment	Indicates any comments associated with this backup job.

Add a backup job

To add a backup job, perform the following steps:

Step 1 Click the **Admin** tab.

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

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

Step 4 Click the **Jobs** tab.

Step 5 Select **New Job > Backup**.

Step 6 Configure values for the following parameters:

- **Job Name** - Type the name you want to apply to this job.
- **Group** - From the **Group** drop-down list box, select the group to which you want to assign this job.

  If there are no groups in the drop-down list box, you can type a group name. Assigning a job to a group allows you to sort the jobs.

- **Comment** - Optional. Type any comment you want to associate with this backup job. You can type up to 255 characters in your description of the backup job.

Step 7 Click **OK**.

The job is displayed in the list on the Job Details pane.

Step 8 Select the search method:

- **Static list** - A static list enables you to search for devices using several options. Using the static list option, you can define the specific devices on which you want to run the job. Go to Step 9.
- **Search** - Type an IP address or CIDR range that you want to include in the job. Once you define the search criteria, the search for devices is performed once the job is run. This ensures that any new devices are included in the job. Go to Step 10.

Step 9 If you chose Static list, define the search criteria:

a Click the **Devices** tab.

b From the drop-down list box on the **Devices** tab, select the search criteria:

Table 4-9 Search Criteria

Search Option	Description
Interface IP Address	Allows you to search for devices that have an interface matching either an IP address or CIDR range. Type the IP address or CIDR range on which you want to search in the **IP/CIDR** field. For example, if you type a search criteria of 10.100.22.6, the search results returns a device with an IP address of 10.100.22.6. If you type a CIDR range of 10.100.22.0/24, all devices in the 10.100.22.* are returned.
Admin IP Address	Allows you to search for all devices that have an administrative interface IP address that matches the query. An administrative IP address is the IP address that uniquely identifies a device. Type the IP address or CIDR range on which you want to search in the **IP/CIDR** field.

Table 4-9 Search Criteria (continued)

Search Option	Description
OS Version	Allows you to search for devices based on the operating system version devices are running. Select values for the following parameters: • **Adapter** - Using the drop-down list box, select the type of adapter you want to search. • **Version** - Using the drop-down list box, select the search criteria for the version. For example, greater than, less than, or equal to the specified value. Type the version number in the field on which you want to search. If you do not select a search option for Version, the results include all devices that are configured with the selected adapter, regardless of version.
Model	Allows you to search for devices based on the model number. Configure values for the following parameters: • **Vendor** - Using the drop-down list box, select the vendor you want to search. • **Model** - Type the model you want to search.
Hostname	Allows you to search for devices based on the hostname. Type the hostname on which you want to search in the **Hostname** field.

c Click **Go**.

The search results is displayed.

d In the **Devices** tab, select the devices you want to include in the job.

e In the Job Details pane, click **Add selected from device view search**.

The selected devices appear in the Devices pane.

Step 10 If you chose Search, define the criteria:

a Click the **Devices** tab.

The Devices tab is displayed.

b Using the drop-down list box in the **Devices** tab, select the search criteria:

Table 4-10 Search Criteria

Search Option	Description
Interface IP Address	Allows you to search for devices that have an interface matching either an IP address or CIDR range. Type the IP address or CIDR range on which you want to search in the **IP/CIDR** field. For example, if you type a search criteria of 10.100.22.6, the search results return a device with an IP address of 10.100.22.6. If you type a CIDR range of 10.100.22.0/24, all devices in the 10.100.22.* range are returned.
Admin IP Address	Allows you to search for all devices that have an administrative interface IP address that matches the query. An administrative IP address is the IP address that uniquely identifies a device. Type the IP address or CIDR range on which you want to search in the **IP/CIDR** field.
OS Version	Allows you to search for devices based on the operating system version devices are running. Select values for the following parameters: • **Adapter** - Using the drop-down list box, select the type of adapter you want to search. • **Version** - Using the drop-down list box, select the search criteria for the version. For example, greater than, less than, or equal to the specified value. Type the version number in the field on which you want to search. If you do not select a search option for Version, the results include all devices that are configured with the selected adapter, regardless of version.
Model	Allows you to search for devices based on the model number. Select values for the following parameters: • **Vendor** - Using the drop-down list box, select the vendor you want to search. • **Model** - Type the model you want to search.
Hostname	Allows you to search for devices based on the hostname. Type the hostname on which you want to search in the **Hostname** field.

c Click **Go**.

The search result is displayed.

d In the Job Details pane, click **Use search from devices view**.

The search parameters appear in the Devices pane. This search criteria is used to determine devices associated with this job.

Step 11 Define the job schedule:

a Click **Schedule**.

b Configure values for the following parameters:

- **Name** - Type a name for the schedule configuration.
- **Start time** - Select a time and date you want to start the backup process. The time must be specified in military time.
- **Frequency** - Select the frequency you want to associate with this schedule. The options are:

  Once - Select this option if you want to run this job once.

  Daily - Select the number of days between the jobs. The default is 1.

  Weekly - Select the day of the week that want to run the job.

  Monthly - Select the frequency and the day of the month you want to run the job.

  Cron - Type a cron expression, which is interpreted in Greenwich Mean Time (GMT). For assistance, contact your administrator.
- **Specify End Date** - Optional. Select a date to end the job schedule.

c Click **Save** in the Trigger pane.

The schedule configuration is displayed in the Triggers column. The Triggers for a job represents the job's schedule. You can have multiple schedules configured. For example, you can configure two schedule options so a job runs every Monday and the first of every month.

d Repeat steps a to c.

Step 12 If you want to run the job immediately, click **Run Now**.

Step 13 Click **Yes** to continue.

Edit a backup job

To edit a job:

Step 1 Click the **Admin** tab.

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

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

Step 4 Click the **Jobs** tab.

Step 5 Double-click the job you want to edit.

Step 6 The current values for the job are displayed:

- **Job Name** - The name assigned to this job is displayed. This parameter is not editable.
- **Group** - The group assigned to this job is displayed. This parameter is not editable.
- **Comment** - The comments attached to this backup job are displayed. This parameter is not editable.

Step 7 Select the devices on which you want to run the job:

a Choose the search option from the **Selection Type** parameter.

- **Static List** - Allows you to search for specific devices using several options: Go to Step 9.
- **Search** - Type an IP address or CIDR range that you want to include in the job. Go to Step 10.

The search parameters is displayed.

Step 8 If you chose Static List, define the search criteria:

a Click the **Devices** tab.

b Using the drop-down list box in the **Devices** tab, select the search criteria

Table 4-11 Search Criteria

Search Option	Description
Interface IP Address	Allows you to search for devices that have an interface matching either an IP address or CIDR range. Type the IP address or CIDR range on which you want to search in the **IP/CIDR** field. For example, if you type a search criteria of 10.100.22.6, the search results return a device with an IP address of 10.100.22.6. If you type a CIDR range of 10.100.22.0/24, all devices in the 10.100.22.* range are returned.
Admin IP Address	Allows you to search for all devices that have an administrative interface IP address that matches the query. An administrative IP address is the IP address that uniquely identifies a device. Type the IP address or CIDR range on which you want to search in the **IP/CIDR** field.
OS Version	Allows you to search for devices based on the operating system version devices are running. Select values for the following parameters: • **Adapter** - Using the drop-down list box, select the type of adapter you want to search for. • **Version** - Using the drop-down list box, select the search criteria for the version. For example, greater than, less than, or equal to the specified value. Type the version number in the field on which you want to search. If you do not select a search option for Version, the results include all devices that are configured with the selected adapter, regardless of version.
Model	Allows you to search for devices based on the model number. Configure values for the following parameters: • **Vendor** - Using the drop-down list box, select the vendor you want to search for. • **Model** - Type the model you want to search for.

Table 4-11 Search Criteria (continued)

Search Option	Description
Hostname	Allows you to search for devices based on the hostname. Type the hostname on which you want to search in the **Hostname** field.

c Click **Go**.

d From the **Devices** tab, select the devices you want to include in the job.

e On the **Job Details** pane, click **Add selected from device view search**.

Step 9 If you chose Search, define the criteria:

a Click the **Devices** tab.

b Using the drop-down list box, select the search criteria.

Table 4-12 Search Criteria

Search Option	Description
Interface IP Address	Allows you to search for devices that have an interface matching either an IP address or CIDR range. Type the IP address or CIDR range on which you want to search in the **IP/CIDR** field. For example, if you type a search criteria of 10.100.22.6, the search results return a device with an IP address of 10.100.22.6. If you type a CIDR range of 10.100.22.0/24, all devices in the 10.100.22.* range are returned.
Admin IP Address	Allows you to search for all devices that have an administrative interface IP address that matches the query. An administrative IP address is the IP address that uniquely identifies a device. Type the IP address or CIDR range on which you want to search in the **IP/CIDR** field.
OS Version	Allows you to search for devices based on the operating system version devices are running. Select values for the following parameters: • **Adapter** - Using the drop-down list box, select the type of adapter you want to search. • **Version** - Using the drop-down list box, select the search criteria for the version. For example, greater than, less than, or equal to the specified value. Type the version number in the field on which you want to search. If you do not select a search option for Version, the results include all devices that are configured with the selected adapter, regardless of version.

Table 4-12 Search Criteria (continued)

Search Option	Description
Model	Allows you to search for devices based on the model number. Configure values for the following parameters: • **Vendor** - Using the drop-down list box, select the vendor you want to search. • **Model** - Type the model you want to search.
Hostname	Allows you to search for devices based on the hostname. Type the hostname on which you want to search in the **Hostname** field.

c Click **Go**.

d On the Job Details pane, click **Use search from devices view**.

The search parameters appear in the Devices pane. This search criteria is used to determine devices associated with this job.

Step 10 Define the job schedule:

a Click **Schedule**.

The Schedule pane is displayed.

b If you want to remove a schedule option, select the schedule. Click **Remove**.

c If you want to edit an existing schedule option, select the schedule and edit the values as necessary:

- **Name** - Type a name for the schedule configuration.
- **Start time** - Select a time and date you want to start the backup process. The time must be specified in military time.
- **Frequency** - Select the frequency you want to associate with this schedule. The options are:

  Once - Select this option if you want to run this schedule once.

  Daily - Select the number of days between the jobs. The default is 1.

  Weekly - Select the day of the week that want to run the job.

  Monthly - Select the frequency and the day of the month you want to run the job.

  Cron - Type the Greenwich Mean Time (GMT) that you want to run the job. QRadar Risk Manager uses Quarts 1.6.1 for expression format.
- **Specify End Date** - Type a date to end the job schedule.

d Click **Save**.

The schedule configuration is displayed in the Triggers column.

e Repeat steps a to c.

Step 11 Click **Run Now**.

Step 12 Click **Yes** to continue.

Rename a backup job

To rename a backup job:

Step 1 Click the **Admin** tab.

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

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

Step 4 Click the **Jobs** tab.

Step 5 Select the backup job you want to rename.

Step 6 Click **Rename**.

The Rename Job window is displayed.

Step 7 Configure values for the following parameters:

- **Job Name** - Type a new name for the job.
- **Group** - Using the **Group** drop-down list box, select the group to which you want to assign this job. You can also specify a new group name.

Step 8 Click **OK**.

Delete a backup job

To delete a backup job:

Step 1 Click the **Admin** tab.

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

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

The Configuration window is displayed.

Step 4 Click the **Jobs** tab.

Step 5 Select the backup job you want to delete.

Step 6 Click **Delete**.

Configure protocols

For QRadar Risk Manager to communicate with devices, you must define the communication method (protocol) required for communication to your network devices. QRadar Risk Manager provides default protocol configuration for your system. If you need to define protocols, you can define protocols to allow QRadar Risk Manager to obtain and update device configuration. Many network environments have different communication protocols of different types or functions of the device. For example, a router might use a different protocol than the firewalls in the network. For a list of supported protocols by device manufacturer, see the *Configuring Adapters Guide*.

QRadar Risk Manager uses protocol sets to define groups of protocols for a set of devices that require a specific communication protocol. You can assign devices to network groups, which allows you to group together protocol sets and address sets for your devices.

Protocol sets area a named set of protocols for a set of devices that require specific protocol credentials.

Address sets are IP addresses that define the network group.

To configure protocols, perform the following steps:

Step 1 Click the **Admin** tab.

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

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

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

Step 5 To configure a new network group:

a In the **Network Groups** pane, click the **Add (+)** icon.

b Type a name for a network group.

c Click **OK**.

The network group is added and the address set parameters are displayed.

d Use the **Move Up** and **Move Down** icons to prioritize the network groups.

Move the network group you want to have first priority to the top of the list.

Step 6 To configure the address set:

a In the **Add Address** field, type the IP address or CIDR range that you want to apply to the network group, then click the **Add (+)** icon.

For example, type an IP address range using a dash or wildcard (*) to indicate a range, such as 10.100.20.0-10.100.20.240 or 1.1.1*. If you type 1.1.1.*, all IP addresses meeting that requirement are included.

b Repeat for all IP addresses you want to add to the address set for this network group.

Step 7 To configure the protocol set:

a In the **Network Groups** pane, ensure the network group you want to configure protocols for is selected.

b Select any check boxes to apply a protocol to the range of IP addresses assigned to the network group you created.

Clearing the check box turns off the communication option for the protocol when attempting to backup a network device.

c For each protocol selected, configure values for the following parameters:

Table 4-13 Protocol Parameters

Protocol	Parameter
SSH	Configure the following parameters: • **Port** - Type the port on which you want the SSH protocol to use when communicating with and backing up network devices. The default SSH protocol port is 22. • **Version** - Select the version of SSH that you want this network group to use when communicating with network devices. The available options are as follows: **Auto** - This option automatically detects the SSH version to use when communicating with network devices. **1** - Use SSH-1 when communicating with network devices. **2** - Use SSH-2 when communicating with network devices.
Telnet	Type the port number you want the Telnet protocol to use when communicating with and backing up network devices. The default Telnet protocol port is 23.
HTTPS	Type the port number you want the HTTPS protocol to use when communicating with and backing up network devices. The default HTTPS protocol port is 443.
HTTP	Type the port number you want the HTTP protocol to use when communicating with and backing up network devices. The default HTTP protocol port is 80.
SCP	Type the port number you want the SCP protocol to use when communicating with and backing up network devices. The default SCP protocol port is 22.
SFTP	Type the port number you want the SFTP protocol to use when communicating with and backing up network devices. The default SFTP protocol port is 22.
FTP	Type the port number you want the FTP protocol to use when communicating with and backing up network devices. The default SFTP protocol port is 22.
TFTP	The TFTP protocol does not have any configurable options.

Table 4-13 Protocol Parameters (continued)

Protocol	Parameter
SNMP	Configure the following parameters: • **Port** - Type the port number you want the SNMP protocol to use when communicate with and backing up network devices. • **Timeout(ms)** - Select the amount of time, in milliseconds, that you want to use to determine a communication timeout. • **Retries** - Select the number of times you want to attempt to retry communications to a device. • **Version** - Select the version of SNMP you want to use for communications. The options are v1, v2, or v3. • **V3 Authentication** - Select the algorithm you want to use to authenticate SNMP traps. • **V3 Encryption** - Select the protocol you want to use to decrypt SNMP traps.

d Use the **Move Up** and **Move Down** icons to prioritize the protocols.

Move the protocol that you want to have first priority to the top of the list.

Step 8 Click **OK**.

Configure the discovery schedule

You can configure a discovery schedule to populate ARP, MAC tables, and neighbor information for your devices. The discovery schedule also allows new devices to be automatically added to the inventory.

To configure the discovery schedule:

Step 1 Click the **Admin** tab.

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

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

Step 4 On the navigation menu, click **Schedule Discovery.**

Step 5 Select the **Enable periodic discovery** check box to enable schedule discovery.

Step 6 Configure values for the following parameters:

- **Start time** - Select the date and time you want to schedule the discovery process.
- **Schedule** - Select the interval for which you want to schedule the discovery process. The options are:
  - **Once** - Select this option to run this discovery process once.
  - **Daily** - Select the number of days between the discovery process.
  - **Weekly** - Select the days of the week that you want to schedule the discovery.

  - **Monthly** - Select the interval and day/date monthly time intervals that you want to schedule the discovery process.
  - **Cron** - Type the expression required (in GMT) to use cron for the schedule process.
- **Specify End Date** - Optional. Select the end date that you want to end the schedule discovery process.
- **Crawl and discover new devices** - Select the check box if you want the discovery process to discover new devices. Clear the check box if you do not want to add new devices to the inventory.

Step 7 Click **OK**.

5 USE THE TOPOLOGY

The Topology page opens by default when you access the **Risks** tab. The topology model enables you to view, filter, and interact with a graph that depicts the physical connectivity of your layer 3 network topology. This graph is created from detailed configuration information obtained from network devices, such as firewalls, routers, switches, and Intrusion Prevention System (IPS) systems. You can hover over connections lines to display network connection information. The search feature allows you to filter the topology for potential attack paths on allowed protocols, ports, or vulnerabilities, view the traffic flow between devices or subnets, and device rules.

The Topology enables you to:

- Visualize specific network paths and traffic direction for advanced threat analysis.
- Incorporate passive IPS security maps into the topology graph.
- Customize the topology layout, including user-defined network groups.
- Create search filters for your network topology based on protocols, ports, or vulnerabilities.
- View detailed connection information between devices and subnets.
- View device rules on topology connections with the allowed ports and protocols.
- View Network Address Translation (NAT) devices, NAT indicators and information about NAT mappings.
- View virtualized network security devices that have multiple-contexts.

Only TCP, UDP, and ICMP protocols are represented in the topology model when viewing the allowed ports and protocols between devices.

View the topology

By default, the topology is displayed with grouping applied to your network. If you have a previously saved layout and are returning to the Topology, the saved layout is displayed.

To view the topology, perform the following steps:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Topology**.

The topology graph depicts subnets, devices, and firewalls using the following icons:

Table 5-1 Graph icons

Icon	Description
Cloud	The cloud icon depicts a subnet of your network.
Brick Wall	The brick wall icon depicts firewall and IPS devices.
Router	The router icon depicts routers or unclassified devices. If a gateway address does not appear for a device, the Topology graph displays the text Unclassified Device below the router icon. Unclassified devices assume the IP address of the gateway and manage subnets specified in the routes.
Circle	The circle icon depicts a collapsed group node. The number inside the group name identifies how many devices are contained in the group.
Switch	The switch icon depicts a switch in the topology.
Multi-context device	The multi-context device icon depicts a device that contains multiple contexts.
NAT Indicator	The green dot is a NAT indicator that displays when a topology search finds a path that contains source or destination translations.

Using the topology

If you previously configured saved search criteria as the default, the results of that search are automatically displayed in the topology. For more information on saving search criteria, see Search the topology.

Use the toolbar

The topology graph includes several menu options including:

Table 5-2 Topology toolbar options

Menu Option	Description
Search	From the **Search** drop-down list box, select an option to perform advanced searches on your topology. Options include: • **New Search** - Select this option to create a new event search. • **Edit Search** - Select this option to select and edit an event search.
Quick Searches	From the **Quick Searches** drop-down list box, you can run previously saved searches. Options are only displayed when you have saved search criteria and select the **Include in my Quick Searches** check box.
Save	Click **Save** to save your current Topology including the position of the items, the applied filter, zoom scale, graph position, and group expansions. The next time you log in to the Topology, the saved layout is displayed.
Reset Layout	Click **Reset Layout** to reset the topology layout to the previously saved arrangement. This includes the previously saved filters, group expansions, and node positions. However, the Reset Layout option does not affect node groups.
Undo	Click **Undo** to revert the last topology action. This includes collapsing the last node expansion, creating a group, removing a group, expanding a group, or moving a node. If you want to undo multiple actions, click the **Undo** button for each action you want to reverse.
Group Nodes	Click **Group Nodes** to group selected nodes. After nodes are placed in a group, you can expand and collapse the entire group. For more information, see Group nodes.
Download	Click **Download** to save the current topology as a JPEG image file.

Use the topology model

Using the topology model, you can access the following graphical features:

Table 5-3 Topology Model Graphical Features

If you want to	Then
View additional details about a subnet	Move the pointer of your mouse over the subnet. The configuration information is displayed.
View additional details about a device	Move the pointer of your mouse over the device. The configuration information is displayed.
View additional details about a connection	Move the pointer of your mouse over a connection line between a device, group, or subnet to view connection details. Multiple curved edges between a device and a subnet indicate that a device or a set of contexts have multiple interfaces on the same subnet.

Table 5-3 Topology Model Graphical Features

If you want to	Then
View additional details about a multi-context device	Move the pointer of your mouse over the multi-context device. The configuration information is displayed.
Distribute nodes	To distribute devices, groups, firewalls, or subnets on the graph, use the pointer of your mouse to drag the node to the preferred location.
Zoom in or zoom out	Use the slider on the top left of the graph to scale the graph. ***Note:*** *You can also use your mouse wheel to scale the graph.*
Pan left, right, up or down	Left-click the white-space of the topology model and drag your cursor to pan a direction. ***Note:*** *You can also use the bounding box in the lower right corner to pan in any direction of the topology model.*

Use the right-Click menu Options

In the topology, you can right-click an event to access additional event filter information.

Table 5-4 Right-click topology options

If you want to	Then
Search Connections	For any subnet in the topology, right-click and select **Search Connections**. This creates a search where the source or destination is the IP address of the subnet you selected. You can add additional search parameters and click **Search** to view the results.
View configuration information for a device.	Move your mouse over the device, right-click and select **View Device Configuration**. This information is obtained from the device. For more information device configurations, see View device configurations.
View configuration information for a multi-context device.	Move your mouse over the device, right-click and select **View Device Configuration**. This displays a list of the contexts that belong to the multi-context device, and includes basic device configuration information. You can view detailed device configuration information for a context if you double-click on a context in the list.

Table 5-4 Right-click topology options (continued)

If you want to	Then
Search for events	Move the pointer of your mouse over a device or subnet in the topology. Right-click and select **Search Events**. • If you search events on a subnet, the search parameters are populated with the source and destination address in the search filter. • If you search events on a device that is mapped to a log source, an event search is populated with the log source name and IP address in the search filter. This enables you to search for events tied to the device from the Topology. If a device is not mapped to a log source, the **Search Events** option is not available. For more information, see Log source mapping.
Search for flows associated with a subnet	Move your mouse button over the subnet. Right-click and select **Search Flows**. The Flow Search window is displayed. For more information on searching flows, see the *IBM Security QRadar SIEM Users Guide*.
View asset profile information for a subnet	Move the pointer of your move over the subnet, right-click and select **View Assets**. The Assets List window displays the list of assets for the subnet. For more information about assets, see the *IBM Security QRadar SIEM Users Guide*.
Expand a grouped node	For any grouped node you want to expand, right-click on the group and select **Expand Group**. You can also double-click a group to expand the node. For more information on grouping nodes, see Group nodes.
Collapse a grouped node	For any grouped node you want to collapse, right-click on a device that belongs to the group and select **Collapse to Group**. For more information on grouping nodes, see Group nodes.
Remove a grouped node	For any grouped node you want to collapse, right-click on a node that belongs to a group and select **Remove Group**. For more information on grouping nodes, see Group nodes.
Add an IPS connection between two devices.	If your Topology includes an IPS device, move the pointer of your mouse over a connection line that links a device node with a subnet node. Right-click and select **Add IPS**. See Add an Intrusion Prevention System (IPS).

Table 5-4 Right-click topology options (continued)

If you want to	Then
Remove an IPS	Move the pointer of your mouse over the connection line that links a device node and a subnet node that includes the IPS. Right-click and select **Remove IPS**. This menu is only displayed if an IPS exists on the connection.

Search the topology

You can search the topology for devices by host, network, or path. These search options can then be narrowed by IP address, CIDR, protocol, source or destination IP addresses or destination ports. The search results in a filtered topology view that matches your search criteria.

You can view an existing topology or load a previously saved topology and search the saved view. A topology that is filtered by a search displays the name of the search filter in yellow below the Current Topology menu bar.

If a path is searched, the traffic direction, allowed or partially allowed protocols, and device rules are displayed. Additionally, a NAT indicator displays on the topology graph if your search finds a path that contains source or destination translations. For more information, see NAT indicators in search results.

To search the topology:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Topology**.

Step 3 From the **Search** drop-down list box, select **New Search**.

The Saved Searches window is displayed.

Step 4 Choose one of the following filter options:

- **None** - Clears the existing search filter on the Topology.
- **Hosts** - Filter the topology model based on hosts, select **Host** and specify the IP address of the host.

  A host filter returns results that include all surrounding devices that communicate with the host IP address. The connection lines between devices and subnets displays the interface information for the connection. If the host does not match an interface on a device, but is included in the subnet, the filter returns the subnet and all connected devices.
- **Network** - To filter the topology model based on network specific filters, select the **Network Filter** option and specify the IP address or CIDR range. Multiple addresses can be entered using a comma-separated list.

  A network filter returns results that include any networks in the CIDR range. To search multiple CIDR addresses, separate the CIDR addresses using a comma.
- **Path** - To filter the topology model based on path filters, select the **Path Filter** option and configure the following parameters:

A path filter includes all subnets and devices between the source and destination that are also allowed to communicate using the specified protocols and ports. Connection details are displayed by moving your mouse over the connection lines, along with arrows representing the direction of traffic and device rules, if available. A NAT indicator displays on the topology graph if your search finds a path that contains source or destination translations.

The following table displays the filter options when you perform a topology path search:

Table 5-5 Path Filter Options

Parameter	Description
Source IP/CIDR	Type the IP address or CIDR range on which you want to filter the topology model. Separate multiple entries using a comma separated list.
Destination IP/CIDR	Type the destination IP address or CIDR range on which you want to filter the topology model. Separate multiple entries using a comma separated list.
Protocol	Optional. Using the drop-down list box, select the protocol you want to use to filter the topology model. The options are: • Any Protocol (default) • TCP • UDP • ICMP ***Note:*** *Only TCP, UDP, and ICMP protocols are represented in the topology model.*
Destination Port	Optional. Type the destination port on which you want to filter the topology model. Separate multiple ports using a comma separated list.
Vulnerabilities	This parameter is only displayed if your topology includes an IPS. To filter using vulnerabilities: **1** Click **Vulnerabilities**. **2** Using the **Search By** drop-down list box, select the vulnerability option on which you want to search. The options include: OSVDB Title, CVE ID, Bugtraq ID, or OSVDB ID. **3** Type or select a search parameter. **4** Click **Search**. Search results appear in the Search Results box. **5** For any results on which you want to filter the topology, select the value in the Search Results box. Click **Add**. **6** Repeat for all results on which you want to filter. **7** Click **Submit**.

Step 5 Click **Search**.

NOTE

To edit an existing search filter, select **Search > Edit Search** from the Topology toolbar.

NAT indicators in search results

A NAT indicator, which is a solid green dot, displays on the topology graph if your search finds a path that contains source or destination translations.

A NAT indicator indicates that the destination IP address that was specified in the path filter might not be the final destination. You can hover over the indicator to view the following information about the translations.

Table 5-6 Information available from the NAT indicator

Parameter	Description
Source	The translated source IP or CIDR.
Source Port(s)	The translated source ports, if applicable.
Translated Source	The result of the translation that was applied to the source.
Translated Source Port(s)	The result of the translation that was applied to the source port(s), if applicable.
Destination	The translated destination IP or CIDR.
Destination Port(s)	The translated destination ports, if applicable.
Translated Destination	The result of the translation that was applied to the destination.
Translated Destination Port(s)	The result of the translation that was applied to the destination port(s), if applicable.
Phase	The routing phase when the translation was applied. Translation are applied either pre- or post-routing.

Group nodes

You can group nodes based on selected nodes or specified filter criteria. This section provides information on grouping nodes, including:

- Grouping nodes. See Grouping nodes.
- Removing a node group. See Remove group nodes.
- Expanding a group of nodes. See Expand group nodes.

Grouping nodes

To group nodes:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Topology**.

Step 3 Choose one of the following options:

a If you want to group selected nodes in your topology, go to Step 4.

b If you want to group nodes based on a filter criteria, go to Step 5.

Step 4 To group selected nodes:

a Press the Ctrl key and select each node you would like to include in a group.

b Click **Group Nodes.**

c In the Group Name parameter, type the name of the group you want to create.

d Select the **Group Selected** option.

e Click **OK**.

Step 5 To group nodes based on a filter criteria:

a Click **Group Nodes.**

b In the Group Name parameter, type the name of the group you want to create.

NOTE

A group name is limited to a maximum of 50 characters.

c Select the **Group By Filter** option.

d Configure values for the following parameters:

- **IP/CIDR** - Type an IP address or CIDR range for the nodes you want to group.
- **Adapter Type** - From the **Adapter Type** drop-down list box, select the adapter on which you want to group the nodes.

e Click **OK**.

The group is displayed in the current topology with a circle around the grouped node center.

Remove group nodes

To remove a node grouping:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Topology**.

Step 3 In the Current Topology, select the circle that indicates the group node you want to remove.

Step 4 Right-click and select **Remove group**.

The nodes that were previously grouped display the individual devices in the Topology.

Expand group nodes

To expand a node grouping:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Topology**.

Step 3 In the Current Topology, select the circle that indicates the group node you want to expand.

Step 4 Right-click and select **Expand group**.

Add an Intrusion Prevention System (IPS)

If your Configuration Source Management list includes an Intrusion Prevention System (IPS) device, you can add an IPS to a connection that links a device node with a subnet node. Adding an IPS connection is useful to determine the location of the IPS if the device is passive.

To add an IPS, perform the following steps:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Topology**.

Step 3 Move your mouse pointer over the connection line that links a device node and a subnet node.

Step 4 Right-click the connection line, select the **Add IPS** option.

Step 5 Using the drop-down list boxes, select the device and interfaces to add the IPS connection to your topology.

Step 6 Click **OK**.

The Topology page is displayed with the IPS between your selected device and subnet.

Remove an Intrusion Prevention System (IPS)

To remove an IPS connection between a device and subnet:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Topology**.

Step 3 Move your mouse pointer over the connection line that links a device node and a subnet node.

Step 4 Right-click the connection line, select the **Remove IPS idp** option.

Step 5 Click **OK**.

The Topology page refreshes with the IPS device removed.

6 USING THE POLICY MONITOR

The Policy Monitor enables an organization to define specific risk questions about the network to assess or monitor risk based on the analysis of risk indicators. Risk indicators include:

- Network activity - measures risk based on network communications that have occurred in the past.
- Configuration/Topology - measures risk based on possible communications and network connections.
- Vulnerabilities - measures risk based on your network configuration and vulnerability scan data collected from network assets.
- Firewall rules - measures risk based on the enforcement or absence of firewall rules applied across the network.

The Policy Monitor enables users to define tests based on the risk indicators, then restrict the test results to filter the query for specific results or violations. Questions can be created for assets or devices/rules to expose security professionals to risks in their networks. Once a question about an asset or a device/rule is submitted to the Policy Monitor, QRadar Risk Manager returns results specified by the level of risk. The Policy Monitor allows you to approve results returned from assets or define how you want the system to respond to unapproved results.

The results allow users to assess risk cases for many varied security scenarios, for example:

- Assessing if users have communicated using forbidden protocols.
- Assessing if users on specific networks can communicate to forbidden networks or assets.
- Assessing if firewall rules meet corporate policy.
- Prioritizing vulnerabilities by assessing which systems can be compromised due to network configuration.

To configure your policy monitor questions, you must:

Step 1 Define policies by creating questions. See **Creating a question**.

Step 2 Assess adherence to a policy. See **Submitting a question**.

Step 3 Accept specific risks. See **Approving question results**.

Step 4 Monitor newly introduced risks. See **Monitoring questions**.

Using the Policy Monitor

From the main toolbar on the Policy Monitor page, you can access the following options.

Table 6-1 Toolbar Options

Option	Description
Group	Allows you to view questions based on a group. Using the **Group** drop-down list box, select the group for the questions you want to view.
Groups	Allows you to configure groups for questions. See **Grouping questions**.
Monitor	Allows you to monitor a question, which ensures that an event is generated as a result of a question change. See **Monitoring questions**.
Events	Allows you to view the events that have been generated as a result of the selected question. This option is only active if the selected question is in monitor mode. For information about events, see the *QRadar Users Guide.*
Offenses	Allows you to view the offense that have been generated as a result of the selected question. This option is only active if the selected question is in monitor mode and the results are correlated by question. For information about offenses, see the *IBM Security QRadar SIEM Users Guide.*
Actions	The **Actions** drop-down list box allows you to perform the following actions: • **New** - Allows you to create a new question. See **Creating a question**. • **Duplicate** - Allows you to copy a question. See **Copying a question**. • **Edit** - Allows you to edit a question. See **Editing a question**. • **Delete** - Allows you to delete a question. See **Deleting a question**. • **Assign Groups** - Allows you to assign a question to a group. See **Assigning an item to a group**.

Viewing questions

The Policy Monitor provides a list of default question templates to assess and monitor the risk to your network.

To view the default questions:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

Step 3 From the **Groups** drop-down list box, select the group of questions you want to display.

The chosen group of questions is displayed in the Questions table, providing the following information:

Table 6-2 Questions Parameters

Parameter	Description
Name	The name associated with this question.
Group	The group or groups associated with the question.
Return Type	The type of question. The options are: • Assets • Devices/Rules
Importance Factor	The level of importance assigned to the question. The range is 1 to 10, with 10 being the most important.
Monitored	Indicates if the question is in monitor mode.
Created By	The user who created the question.
Modified By	The last user to modify the question.

Step 4 Select the question you want to view.

The description of the question is displayed in the Description field.

Managing questions

You can manage questions in Policy Monitor by creating, submitting, approving, editing, copying and deleting them. This section includes information on the following:

Creating a question

To create a question:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

Step 3 From the **Actions** drop-down list box, select **New**.

Step 4 In the **What do you want to name this question?** field, type a name for the question.

Step 5 From the **What type of data do you want to return?** drop-down list box, select the type of data you want to return.

When a question is submitted, it searches the Topology based on the data type you select. The options are:

- **Assets** - Identifies assets on the network that violate a defined policy or which introduced risk into the environment. Go to **Step 6**.
- **Devices/Rules** - Identifies rules in a device that violate a defined policy or which introduce risk into the environment. Go to **Step 7**.

Step 6 If you selected **Assets** as the type of data to return, use the **Evaluate On** drop-down list box to specify the type of communications you want this question to consider. The options include:

- **Actual Communication** - Includes any assets on which communications have been detected using connections.
- **Possible Communication** - Includes any assets on which communications are allowed through your network topology, such as firewalls. Possible Communication questions allow you to review if specific communications are possible on assets, regardless of whether or not a communication has been detected.

Step 7 From the **Importance Factor** drop-down list box, select the level of importance you want to associate with this question.

The Importance Factor is used to calculate the Risk Score and define the number of results returned for a question. The range is 1 (low importance) to 10 (high importance). The default is 5.

Table 6-3 Importance Factor Results Matrix

Importance Factor	Returned Results for Asset Tests	Returned Results for Device/Rule Tests
1 (low importance)	10,000	1,000
10 (high importance)	1	1

For example, a policy question that states **have accepted communication from the internet and include only the following networks (DMZ)** would require a high importance factor of 10 since any results to the question is unacceptable due to the high risk nature of the question. However, a policy question that states “have accepted communication from the internet and include only the following inbound applications(P2P)” might require a lower importance factor since the results of the question does not indicate high risk but you may monitor this communication for informational purposes.

Step 8 To specify the time range for the question, choose one of the following options:

a To specify an interval, select the **Interval** option, then using the drop-down list box, select the time frame for the question.

The options are: Last Hour, Last 24 hrs, Last 7 days, and Last 30 days.

b To specify a fixed time interval, select **Fixed**, then use the date and time options to apply a time range to the question.

Step 9 From the **Which tests do you want to include in your question?** field, select the **+** sign beside the tests you want to include. Asset tests are divided into the following two categories:

- **Contributing tests** - A contributing test uses the question parameters to examine the risk indicators specified in the question and generate risk data results that can be further filtered using a restrictive test. The following rules apply to contributing tests:
  - Contributing tests are displayed in the window **Which tests do you want to include in your question?** by default.
  - Contributing tests return data based on assets detected that match the test question.
- **Restrictive tests** - A restrictive test is used to narrow the results returned by a contributing test question. The following rules apply to restrictive tests:
  - Restrictive tests only appear in the **Which tests do you want to include in your question?** window once a contributing test has been added.
  - Restrictive tests can only be added once a contributing test is included in the question.
  - The Question Editor window does not allow a restrictive test question to be saved if you remove or delete the contributing test question.

For more information on contributing and restrictive tests, see **Submitting a question**.

NOTE

Device/Rules questions look for violations in rules and policy and do not have restrictive test components.

Step 10 Configure the parameters for your tests.

Configurable parameters appear bolded and underlined. Click each parameter to view the available options for your question.

NOTE

Policy Monitor questions created for assets or devices/rules evaluate in a top down manner. When creating your Policy Monitor questions the order of the question can impact the results.

Step 11 In the groups area, select any check boxes to assign this question to a group.

For more information on grouping questions, see **Grouping questions**.

Step 12 Click **Save Question**.

To submit the question, see **Submitting a question**.

Submitting a question

After you create a question, you can submit the question to determine the risk associated with this question. To submit a question:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

Step 3 Select the question you want to submit.

Step 4 Click **Submit Question**.

The results are displayed. The information that is displayed depends on the configuration of the question:

- **Devices** - For more information, see **Device/Rule Results**.
- **Assets** - For more information, see **Asset Results**.

If you submit a question and then perform changes that affect the tests associated with the question, these changes may take up to an hour to appear.

The following table provides device results:

Table 6-4 Device/Rule Results

Parameter	**Description**
Risk Score	The level of risk associated with this question. Risk score is calculated based on the number of results and Importance Factor assigned to this question. The calculation is based on the following values: • The asset weight of assets/devices returned in the results of a question. For more information on assets, see the *IBM Security QRadar SIEM Users Guide.* • The importance factor of the question. For more information about the Importance Factor, see **Creating a question**. • The number of results returned as a result of the question.
Device IP	The IP address of the device.
Device Name	The name of the device, as obtained from the configuration monitor.
Device Type	The type of device, as obtained from the asset profile. For more information about asset profiles, see the *IBM Security QRadar SIEM Users Guide.*
List	The name of the rule from the device.
Entry	The entry number of the rule.
Action	The action associated with the relevant rule from the device. The options are: permit, deny, or NA.

Table 6-4 Device/Rule Results (continued)

Parameter	Description
Source Service(s)	The source ports and the comparison associated with the relevant rule from the device in the following format: **`<comparison>:<port>`** Where **`<comparison>`** could include one of the following options: • eq - Equal • ne - Not equal • lt - Less than • gt - Greater than For example, if the parameter indicates ne:80, any port other than 80 applies to this source service. If the parameter indicates lt:80, the range of applicable ports is 0 to 80. This parameter displays the source port for the device rule. If no port exists for this device rule, the term NA is displayed.
Destination Service(s)	The destination ports and the comparison associated with the relevant rule from the device in the following format: **`<comparison>:<port>`** Where **`<comparison>`** may include one of the following options: • eq - Equal • ne - Not equal • lt - Less than • gt - Greater than For example, if the parameter indicates ne:80, any port other than 80 applies to this destination service. If the parameter indicates lt:80, the range of applicable ports is 0 to 80. This parameter displays the destination port for the device rule. If no port exists for this device rule, the term NA is displayed.
Source(s)	The source network associated with this asset.
Destination(s)	The destination network associated with the relevant rule from the device.
Protocol(s)	The protocol or group of protocols associated with the relevant rule from the device.
Signature(s)	The signature for this device, which is only displayed for a device rule on an IP device.

The following table provides asset results:

Table 6-5 Asset Results

Parameter	Description
Risk Score	Risk score is calculated based on the number of results and Importance Factor assigned to this question. The risk score indicates the level of risk associated with this question. For more information about the Importance Factor, see **Creating a question**.
IP	The IP address of the asset.
Name	The name of the asset, as obtained from the asset profile. For more information about asset profiles, see the *QRadar Users Guide.*
Weight	The weight of the asset, as obtained from the asset profile. For more information about asset profiles, see the *QRadar Users Guide.*
Destination Port(s)	The list of destination ports associated with this asset, in context of the question tests. If there are multiple ports associated with this asset and question, this field indicates Multiple and the number. The list of ports is obtained by filtering the connections associated with this question to obtain all unique ports where the asset has either been the source, destination, or the connection. Click **Multiple (N)** to view the connections. This display provides the aggregated connections by port, filtered by the asset IP address, and based on the time interval specified in the question.
Protocol(s)	The list of protocols associated with this asset, in context of the question tests. If there are multiple protocols associated with this asset and question, this field indicates Multiple and the number. The list of protocols is obtained by filtering the connections associated with this question to obtain all unique protocols where the asset has either been the source, destination, or the connection. Click **Multiple (N)** to view the Connections. This display provides the aggregated connections by protocol, filtered by the asset IP address, and based on the time interval specified in the question.
Flow App(s)	The list of applications associated with this asset, in context of the question tests. If there are multiple applications associated with this asset and question, this field indicates Multiple and the number. The list of applications is obtained by filtering the connections associated with this question to obtain all unique applications where the asset has either been the source, destination, or the connection. Click **Multiple (N)** to view the Connections. This display provides the aggregated connections by applications, filtered by the asset IP address, and based on the time interval specified in the question.

Table 6-5 Asset Results (continued)

Parameter	Description
Vuln(s)	The list of vulnerabilities associated with this asset, in context of the question tests. If there are multiple vulnerabilities associated with this asset and question, this field indicates Multiple and the number. The list of vulnerabilities is obtained using a list of all vulnerabilities compiled from relevant tests and using this list to filter the vulnerabilities detected on this asset. If no vulnerabilities are specified for this question, then all vulnerabilities on the asset are used to compile this list. Click **Multiple (N)** to view the Assets. This display provides the aggregated connections by vulnerability, filtered by the asset IP address, and based on the time interval specified in the question.
Flow Count	The total flow count associated with this asset, in context of the question tests. The flow count is determined by filtering the connections associated with this question to obtain the flow count total, where asset has either been the source, destination, or the connection.
Source(s)	The list of source IP addresses associated with this asset, in context of the question tests. If there are multiple source IP addresses associated with this asset and question, this field indicates Multiple and the number. The list of source IP addresses is obtained by filtering the connections associated with this question to obtain all unique source IP addresses where the asset is the destination of the connection. Click **Multiple (N)** to view the Connections. This display provides the aggregated connections by source IP addresses filtered by the asset IP address based on the time interval specified in the question.
Destination(s)	The list of destination IP addresses associated with this asset, in context of the question tests. If there are multiple destination IP addresses associated with this asset and question, this field indicates Multiple and the number. The list of destination IP addresses is obtained by filtering the connections associated with this question to obtain all unique destination IP addresses where the asset is the source of the connection. Click **Multiple (N)** to view the Connections. This display provides the aggregated connections by destination IP addresses filtered by the asset IP address based on the time interval specified in the question.
Flow Source Bytes	The total source bytes associated with this asset, in context of the question test. The source bytes is determined by filtering the connections associated with this question to obtain the source byte total where asset is the source of the connection.

Table 6-5 Asset Results (continued)

Parameter	Description
Flow Destination Bytes	The total destination bytes associated with this asset, in context of the question test. The destination bytes is determined by filtering the connections associated with this question to obtain the destination byte total where asset is the destination of the connection.

Approving question results

The results returned from submitting a Policy Monitor question allows a user to evaluate the list of assets or device rules returned to determine the level of risk involved. Approving a question result is similar to tuning your system to inform QRadar Risk Manager that the asset associated with the question result is safe or can be ignored in the future. When a user approves an asset result, the Policy Monitor will see that asset result as approved, and when the Policy Monitor question is submitted or monitored in the future, the asset is not listed in the question results. The approved asset does not appear in the results list for the question unless the approval is revoked. The Policy Monitor records the user, IP address of the device, reason for approval, the applicable Device/Rule, and the date and time for your organization's security administrators.To approve question results:

Step 1 In the results table, select the check box next to the results you want to accept.

For more information on submitting a question to obtain results, see **Submitting a question**

Step 2 Choose one of the following options:

a If you want to approve all the results, click **Approve All**.

A confirmation message is displayed. You must confirm your selections before continuing.

b If you want to approve specific results, select the check box next to the results to accept, then click **Approve Selected**.

The Approval Note window is displayed.

Step 3 Type the reason for approval.

Step 4 Click **OK**.

A confirmation window is displayed.

Step 5 Click **OK**.

Step 6 To view the approved results for the question, click **View Approved**.

The Approved Question Results window provides the following information:

Table 6-6 Approved Question Results Parameters

Parameter	Description
Device/Rule	For a Device/Rule question result, this indicates the device associated with this result.

Table 6-6 Approved Question Results Parameters (continued)

Parameter	Description
IP	For an asset question result, this indicates the IP address associated with the asset.
Approved By	The user that approved the results.
Approved On	The date and time the results were approved.
Notes	Displays the text of notes associated with this result as specified in **Step 3**.

NOTE

If you want to remove approvals for any result, select the check box for each result for which you want to remove approval and click **Revoke Selected**. To remove all approvals, click **Revoke All**.

Editing a question

To edit a question:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

Step 3 Select the question you want to edit.

Step 4 From the **Actions** drop-down list box, select **Edit**.

Step 5 Update parameters, as necessary.

For more information on the Question Editor parameters, see **Creating a question**.

Step 6 Click **Save Question**.

Copying a question

To copy a question:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

Step 3 Select the question you want to copy.

Step 4 From the **Actions** drop-down list box, select **Duplicate**.

Step 5 Type a name that you want to assign to the copied question.

Step 6 Click **OK**.

Step 7 Edit the question, as required.

For information on editing a question, see **Editing a question**.

Deleting a question

To delete a question:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

Step 3 Select the question you want to delete.

Step 4 From the **Actions** drop-down list box, select **Delete**.

A confirmation window is displayed.

Step 5 Click **OK**.

Monitoring questions

If you want to generate an event when the results of a question change, you can configure a question to be monitored. When you select a question to be monitored, QRadar Risk Manager continually analyzes the question to determine if the results of a question change. If QRadar Risk Manager detects a result change, an offense can be generated to alert you to a deviation in your defined policy. QRadar Risk Manager can monitor the results of 10 questions in monitor mode.

A question in monitor mode defaults to a time range of 1 hour. This value overrides the time value set when the question was created. For more information on creating a question, see **Creating a question**.

To configure a question to be monitored:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

Step 3 Select the question you want to monitor.

Step 4 Click **Monitor**.

Step 5 Configure values for the parameters:

Table 6-7 Monitor Question Results Parameters

Parameter	Description
Event Name	Specify the name of the event you want to display in the **Log Activity** and **Offenses** tabs.
Event Description	Specify a description for the event. The description is displayed in the Annotations of the event details.

Table 6-7 Monitor Question Results Parameters (continued)

Parameter	Description
Event Details	Configure the following options: • **High-Level Category** - From the drop-down list box, select the high-level event category you want this rule to use when processing events. • **Low-Level Category** - From the drop-down list box, select the low-level event category you want this rule to use when processing events. For more information on event categories, see the *QRadar Users Guide*. • **Ensure the dispatched event is part of an offense (Correlate By:)** - Select this check box if you want, as a result of this monitored question, the events forwarded to the Magistrate component. If no offense has been generated, a new offense is created. If an offense exists, the event is added. If you select the check box, the following option becomes available: **Question/Simulation** - All events from a question are associated to a single offense. **Asset** - A unique offense is created (or updated) for each unique asset. • **Dispatch question passed events** - Select this check box to forward events that pass the policy monitor question to the Magistrate component.
Additional Actions	Select the check boxes to indicate the additional actions to be taken when an event is received. The options include: • **Email** - Select this check box and type the email address(es) to send notification if the event generates. Separate multiple email addresses using a comma. • **Send to Syslog** - Select this check box if you want to log the event. By default, the check box is clear. For example, the syslog output may resemble: **`Sep 28 12:39:01 localhost.localdomain ECS: Rule 'Name of Rule' Fired: 172.16.60.219:12642 -> 172.16.210.126:66666, Event Name: SCAN SYN FIN, QID: 1000398, Category: 1011, Notes: Event description`** • **Notify** - Select this check box if you want events that generate as a result of this monitored question to appear in the System Notifications item in the Dashboard. For more information on the **Log Activity** tab and the QRadar SIEM Dashboard, see the *IBM Security QRadar SIEM Users Guide.*

Table 6-7 Monitor Question Results Parameters (continued)

Parameter	Description
Enable Monitor	Select this check box if you want to monitor the question. This check box is selected by default. If you do not want to monitor a question, clear the check box.

Step 6 Click **Save Monitor**.

Grouping questions

You can group and view your questions based on your chosen criteria. Categorizing your questions allows you to efficiently view and track your questions. For example, you can view all questions related to compliance.

As you create new questions, you can assign the question to an existing group. For information on assigning a group, see **Managing questions**.

Viewing groups

To view questions using groups:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

Step 3 From the **Group** drop-down list box, select the group you want to view.

The list of items assigned to that group display.

Creating a group

To create a group:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

Step 3 Click **Groups**.

Step 4 From the menu tree, select the group under which you want to create a new group.

Step 5 Click **New**.

Step 6 Configure values for the following parameters:

- **Name** - Specify the name you want to assign to the new group. The name can be up to 255 characters in length.
- **Description** - Specify a description you want to assign to this group. The description can be up to 255 characters in length.

Step 7 Click **OK**.

Step 8 If you want to change the location of the new group, click the new group and drag the folder to the chosen location in your menu tree.

Step 9 Close the Groups window.

Editing a group

To edit a group:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

Step 3 Click **Groups**.

Step 4 From the menu tree, select the group you want to edit.

Step 5 Click **Edit**.

Step 6 Update values for the parameters, as required:

- **Name** - Type the name you want to assign to the new group. The name can be up to 255 characters in length.
- **Description** - Type a description you want to assign to this group. The description can be up to 255 characters in length.

Step 7 Click **OK**.

Step 8 If you want to change the location of the group, select the group and drag the folder to the preferred location in the menu tree.

Step 9 Close the Groups window.

Copying an item to another group

Using Question Groups, you can copy a question to one or more groups.

To copy a question:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

Step 3 Click **Groups**.

Step 4 From the menu tree, select the question you want to copy to another group.

Step 5 Click **Copy**.

Step 6 Select the check box for the group to which you want to copy the question.

Step 7 Click **Assign Groups**.

Step 8 Close the Groups window.

Deleting an item from a group

To delete a question from a group:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

Step 3 Click **Groups**.

Step 4 From the menu tree, select the top level group.

Step 5 From the list of groups, select the group you want to delete.

Step 6 Click **Remove**.

Step 7 Click **OK**.

Step 8 If you want to change the location of the new group, click the new group and drag the folder to the preferred location on your menu tree.

Step 9 Close the Groups window.

Assigning an item to a group

To assign a question to a group:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

Step 3 Select the question you want to assign to a group.

Step 4 Using the **Actions** drop-down list box, select **Assign Groups**.

Step 5 Select the group to which you want the question assigned.

Step 6 Click **Assign Groups**.

Policy Monitor use cases

The Policy Monitor offers many options when creating questions to analyze your network for risk. The Policy Monitor examples below outline some common use cases you can use in your network environment. The following use case questions are outlined:

- Asset test for actual communications for DMZ restricted protocols. See **Actual communication for DMZ allowed protocols**.
- Asset test for possible communications on mission critical server. See Asset test for possible communication on protected assets.
- Device test for detecting when a firewall rule allows access a dangerous protocol. See **Device/Rule test communication on Internet access**.

Actual communication for DMZ allowed protocols

In most organizations network traffic crossing the DMZ will be restricted to only well known and trusted protocols, such as HTTP or HTTPS on specified ports. From a risk perspective, it is important to continuously monitor traffic in the DMZ to ensure that only trusted protocols are present. QRadar Risk Manager accomplishes this by creating a Policy Monitor question based on an asset test for actual communications.

There are several ways a Policy Monitor question can be generated for this use case objective. Since we know network policy only allows a few trusted protocols, we will select an option to create our Policy Monitor question based on the known list of trusted protocols for the DMZ.

To create a Policy Monitor question for the DMZ:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

Step 3 From the **Actions** drop-down list box, select **New**.

Step 4 Configure the following values:

- a **What do you want to name this question?** - Type a name for the Policy Monitor question.
- b **What type of data do you want to return?** - Select **Assets**.
- c **Evaluate On** - Select **Actual Communication**.
- d **Importance Factor** - Specify a level of importance to associate with your Policy Monitor question.
- e **Time Range** - Specify the time range for the question.

Step 5 Using the **Which tests do you want to include in your question?** field, select the **+** sign beside the following tests:

- a Select the contributing test **have accepted communication to destination networks**.

  When the test is displayed in the **Find Assets that** window, the configurable parameters display bolded and underlined. Once you've added a contributing test, then restrictive tests are displayed and can be added.
- b Click **destination networks** to further configure this test and specify your DMZ as the destination network.
- c Select the restrictive test **and exclude the following inbound ports**.
- d Click **ports**.

  The Specify Parameter window is displayed.
- e Type **80**, and click **Add**.
- f Type **443,** and click **Add**.

Step 6 Click **Save Question**.

Step 7 Select the Policy Monitor DMZ question you created.

Step 8 Click **Submit Question**.

Step 9 Review the results to see if any protocols other than port 80 and port 443 are communicating on the network.

Step 10 Optional. After the results have been properly tuned, you can monitor your DMZ question by putting the question into monitoring mode

For more information, see **Monitoring questions**.

Asset test for possible communication on protected assets

All organizations have networks that contain critical servers where traffic is monitored and only accessible by trusted employees. From a risk perspective, it is important to know which users within your organization can communicate with critical network assets. QRadar Risk Manager accomplishes this task by creating a Policy Monitor question based on an asset test for possible communications.

There are several ways a Policy Monitor question can be generated for this use case objective. You could look at all the connections to the critical server over time, but you might be more concerned that regional employees are not accessing these critical servers. To accomplish this, you can create a Policy Monitor question that looks at the topology of the network by IP address.

To create a Policy Monitor question by IP address:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

Step 3 From the **Actions** drop-down list box, select **New**.

Step 4 Configure the following values:

- **a** **What do you want to name this question?** - Specify a name for the Policy Monitor question.
- **b** **What type of data do you want to return?** - Select **Assets**.
- **c** **Evaluate On** - Select **Possible Communication**.
- **d** **Importance Factor** - Specify a level of importance to associate with your Policy Monitor question.
- **e** **Time Range** - Specify the time range for the question.

Step 5 From the **Which tests do you want to include in your question?** window, select the **+** sign beside the following tests:

- **a** Select the contributing test **have accepted communication to destination asset building blocks**.

  When the contributing test is displayed in the **Find Assets that** field, the configurable parameters appear bolded and underlined. Once you've added a contributing test, restrictive tests are available.
- **b** Click **asset building blocks** to further configure this test and specify **Protected Assets**.

NOTE

To define your network remote assets, you must have previously defined your remote assets building block.

- **c** Select the restrictive test **and include only the following IP address**.
- **d** Click **IP Address**.

  The Specify Parameter window is displayed.
- **e** Specify the IP address range or CIDR address of your remote network.

Step 6 Click **Save Question**.

Step 7 Select the Policy Monitor question you created for protected assets.

Step 8 Click **Submit Question**.

The results are displayed.

Step 9 Review the results to see if any protected asset has accepted communication from an unknown IP address or CIDR range.

Step 10 Optional. After the results have been properly tuned you can monitor your protected assets by putting the question into monitoring mode. If a protected asset is connected to by an unrecognized IP address, then QRadar Risk Manager can generate an alert.

For more information, see **Monitoring questions**.

Device/Rule test communication on Internet access

Device tests identify rules in a device that violate a defined policy or changes that introduced risk into the environment. From a network perspective, it is important to know which device rules could have changed and alert you to the rule so it can be corrected. A very common occurrence is when servers that didn't previously have Internet access is granted access due to a firewall change on the network. QRadar Risk Manager can monitor for rule changes on network devices by creating a Policy Monitor question based on the device rules.

There are several ways a Policy Monitor question can be generated for this use case objective. In this example, you will create a Policy Monitor question that looks to see what devices have access to the internet.

To create a Policy Monitor question by IP address:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Policy Monitor**.

Step 3 From the **Actions** drop-down list box, select **New**.

Step 4 Configure the following values:

a **What do you want to name this question?** - Specify a name for the Policy Monitor question.

b **What type of data do you want to return?** - Select **Device/Rules**.

c **Importance Factor** - Specify a level of importance to associate with your Policy Monitor question.

Step 5 From the **Which tests do you want to include in your question?** window, select the **+** sign and add the following tests **allow connection to the internet**.

NOTE

Device/Rules questions look for violations in rules and policy and do not have restrictive test components.

Configurable parameters appear bolded and underlined.

Step 6 Click **Save Question**.

Step 7 Select the Policy Monitor question you created for monitoring device rules.

Step 8 Click **Submit Question**.

Step 9 Review the results to see if any rules allow access to the internet.

Step 10 Optional. After the results have been properly tuned you can monitor your protected assets by putting the question into monitoring mode.

For more information, see **Monitoring questions**.

7 INVESTIGATING CONNECTIONS

A connection is a recording of a communication (including denied communications) between two unique IP addresses over a specific destination port, as detected over a specific time interval (the default is 1 hour). If two IP addresses communicate many times over the same interval on a port, only one communication is recorded, but the bytes communicated and the number of flows are totalled with the connection. At the end of the interval, the connection information is accumulated over the interval and is stored in the database.

Connections allows you to monitor and investigate network device connections or perform advanced searches. You can use the connections to:

- Search connections
- Search a subset of connections (sub-search)
- View connection information grouped by various options
- Export connections in XML or CSV format

Using the Connections toolbar

Using the toolbar, you can access the following options:

Table 7-1 Toolbar Options

Option	Description
Search	From the **Search** drop-down list box, select an option to perform advanced searches on your connections. Options include: • **New Search** - Allows you to create a new search. • **Edit Search** - Allows you to select and edit a search. • **Manage Search Results** - Allows you to view and manage search results. See Managing search results. For more information about the search feature, see Using the search feature.
Quick Searches	From the **Quick Searches** drop-down list box, you can run previously saved searches. Options are only displayed when you create a search and select the **Include in my Quick Searches** check box.
Add Filter	Click **Add Filter** to add a filter to the current search results.

Table 7-1 Toolbar Options (continued)

Option	Description
Save Criteria	Click **Save Criteria** to save the current search criteria.
Save Results	Click **Save Results** to save the current search results. This option is only displayed after a search is complete.
Cancel	Click **Cancel** to cancel a search in progress.
False Positive	Click **False Positive** to mark a search result as a false positive. You can use the False Positive Tuning function to tune out false positive events from created offenses
Actions	The **Actions** drop-down list box allows you to perform the following actions: • **Show All** - Removes all filters on search criteria and presents all connections. • **Print** - Allows you to print the connections displayed in the window. • **Export to XML** - Allows you to export connections in XML format. See Exporting connections. • **Export to CSV** - Allows you to export connections in CSV format. See Exporting connections. • **Delete** - Allows you to delete a search result. See Deleting a Search. • **Notify** - Allows you to specify that you want a notification email on completion of the selected search(es). This option is only enabled for searches in progress.

Viewing connections

To view connections:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Connections**.

If you previously saved a search to be the default, the results for that saved search are displayed. By default, the Connections window displays the following graphs:

- Records matched over time chart provides time series information that shows the number of connections based on time.
- Connections graph that provides a visual representation of the connections retrieved.

For more information about the graphs, see Using the graphs. For more information on saving search criteria, see Saving search criteria.

Step 3 Using the **View** drop-down list box, select the time frame you want to display.

The Connections window displays the following information:

Table 7-2 Connections Window - Default

Parameter	Description
Current Filters	The top of the table displays the details of the filter applied to the search result. To clear these filter values, click **Clear Filter.** ***Note:*** *This parameter only displays after you apply a filter.*
View	Allows you to specify the time range you want to filter. Using the drop-down list box, select the time range you want to filter.
Current Statistics	Current statistics include: • **Total Results** - The total number of results that matched your search criteria. • **Data Files Searched** - The total number of data files searched during the specified time span. • **Compressed Data Files Searched** - The total number of compressed data files searched within the specified time span. • **Index File Count** - The total number of index files searched during the specified time span. • **Duration** - The duration of search. ***Note:*** *Current Statistics are a useful troubleshooting tool. When you contact Customer Support to troubleshoot an issue, you could be asked to supply current statistic information. Click the arrow next to Current Statistics to display or hide the statistics.*
Charts	Displays charts representing the records matched by the time interval and/or grouping option. Click **Hide Charts** if you want to remove the graph from your display. For more information about configuring charts, see Using the graphs. ***Note:*** *If you use Mozilla Firefox as your browser and the Adblock Plus browser extension is installed, the charts do not display. For the charts to appear, you must remove the Adblock Plus browser extension. For more information, see your browser documentation.*
Last Packet Time	The Last Packet time is the date and time of the last processed packet for this connection.
Source Type	The Source Type is the source type for this connection. The options are: Host or Remote.
Source	The source of this connection. The options are: • **IP address** - The IP address for the source of this connection. The IP address is displayed if the Source Type is Host. • **Country** - The source country (with the country flag) for this connection. The country flag is only displayed if the Source Type is remote.
Destination Type	The destination type for this connection. The options are: Host or Remote.

Table 7-2 Connections Window - Default (continued)

Parameter	Description
Destination	The IP address for the type of host, including the country flag. The options are: • **IP address** - The IP address for the destination of this connection. The IP address is displayed if the Destination Type is Host. • **Country** - The destination country (with the country flag) for this connection. The country flag is only displayed if the Destination Type is remote.
Protocol	The protocol used for this connection.
Destination Port	The destination port for this connection.
Flow Application	The flow application that generated the connection.
Flow Source	The source of flows associated with this connection. This parameter only applies to accepted connections.
Flow Count	The total number of flows associated with this connection.
Flow Source Bytes	The total number of flow source bytes associated with this connection.
Flow Destination Bytes	The total number of destination bytes associated with this connection.
Log Source	The source of events that have contributed to this connection.
Event Count	The total number of events detected for the connection.
Connection Type	The type of connection. The options are: • **Allow** - Allows the connection. • **Deny** - Denies the connection.

Using the graphs

The Connections window allows you to view connection data using various chart options. By default, you can view data using the following chart types:

- **Records matched over time** - Indicates the number of connections based on time. See Using the time series graph.
- **Connection graph** - Provides a visual representation of the connection retrieved. If you want to further investigate connections using the connection graph, see Using the connection graph.

The following graph options are available for grouped connections as the result of a search. For more information on searching connections, see Using the search feature.

- **Table** - Displays data in a table.
- **Bar** - Displays data in a bar chart.
- **Pie** - Displays data in a pie chart.

⚠ **CAUTION**

If you use Mozilla Firefox as your browser and an Adblock Plus browser extension is installed, the charts might not display properly. For the charts to appear, you must remove the Adblock Plus browser extension if it is installed. For more information on removing add-ons, see your browser documentation.

Using the time series graph

Time series charts are graphical representations of your connections over time; peaks and valleys that display, depict high and low connection activity. Time series charts are useful for short-term and long-term trending of data. Using time series charts, you can access, navigate, and investigate connections from various views and perspectives.

To configure time series charts:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Connections**.

The Connections window is displayed.

If you previously saved a search to be the default, the results for that saved search display. If the search includes Group By options selected in the Advanced View Definitions box, the Time Series chart is not available. You must clear the search criteria before continuing. For more information on saving search criteria, see Saving search criteria.

Step 3 In the charts pane, click the **Configuration** icon.

The **Chart Type** drop-down list box is displayed.

Step 4 Using the **Chart Type** drop-down list box, select **Time Series**.

The time series chart is displayed.

Step 5 Using the interactive time series charts, you can navigate through a time line to investigate connections.

The following table provides functions you can use to view time series charts including:

Table 7-3 Time Series Charts Functions

If you want to	Then
View connections in greater detail	Magnifying the data in a time series chart allows you to investigate smaller time segments of the connections. You can magnify the time series chart using one of the following options: • Press the Shift key and click on the chart at the time you want to investigate. • Press the Ctrl and Shift keys while you click and drag the mouse pointer over the range of time you want to view. • Move your mouse pointer over the chart and press the Up arrow on your keyboard. • Move your mouse pointer over the chart and then use your mouse wheel to zoom in (roll the mouse wheel up). After you magnify a time series chart, the chart refreshes to display a smaller time segment.
View a larger time span of connections	Including additional time ranges in the time series chart allows you to investigate larger time segments or return to the maximum time range. You can view a time range using one of the following options: • Click **Max** at the top left corner of the chart or press the Home key to return to the maximum time range. • Move your mouse pointer over the chart and press the down arrow on your keyboard. • Move your mouse pointer over the plot chart and then use your mouse wheel to zoom out (roll the mouse wheel down).
Scan the chart	To view the chart to determine information at each data point: • Click and drag the chart to scan the time line. • Press the Page Up key to move the time line a full page to the left. • Press the left arrow key to move the time line one half page to the left. • Press the Page Down key to move the time line a full page to the right. • Press the right arrow key to move the time line one half page to the right

Step 6 To refresh the information in the graph, click **Update Details**.

Using the connection graph

The connection graph provides a visual representation of the connections in your network. The graph that is displayed in the Connections window is not interactive, however, if you click the graph, the Radial Data Viewer window is displayed. The Radial Data Viewer window allows you to manipulate the graph, as required.

By default, the graph displays your network connections as follows:

- Only allowed connections are displayed.
- All local IP addresses are collapsed to show only leaf networks.
- All country nodes are collapsed to a node named Remote Countries.
- All remote network nodes are collapsed to one node named Remote Networks.
- Preview thumbnail view of the graph displays a portion of the main graph. This is useful for large graphs.

The Radial Data Viewer includes several menu options, including:

Table 7-4 Radial Data Viewer Menu Options

Menu Option	Description
Connection Type	By default, the radial graph displays accepted connections. If you want to view denied connections, select **Deny** from the **Connection Type** drop-down list box.
Undo	Collapses the last node expansion. If you want to undo multiple expansions, click the **Undo** button for each expansion.
Download	Allows you to save the graph as a JPEG image.

The following table provides additional functions to view connections including:

Table 7-5 Radial Data Viewer Functions

If you want to...	Then...
Zoom in or zoom out	Use the slider on the top-right side of the graph to change the scale. ***Note:*** *You can also use your mouse wheel to scale the graph.*
Distribute nodes on the graph to view additional details	To distribute nodes on the graph, use your mouse to drag the node to the preferred location.
Expand a network node	For any network node you want to expand to view assets for that node, double-click the node. The node expands to include the specific assets to which that node was communicating. By default, this expansion is limited to the first 100 assets of the network.

Table 7-5 Radial Data Viewer Functions (continued)

If you want to...	Then...
View additional details regarding a connection	Move the pointer of your mouse over the connection line to view additional details. If the connection is between a network node to a remote network or remote country, right-click to display the following menu: • **Source** - For information regarding the Source menu, see Using the Connections toolbar. • **View Flows** - Select to filter the display. The search window is displayed. For more information, see the *IBM Security QRadar SIEM Users Guide*. If the connection is between two IP addresses, the source, destination, and port information is displayed when you click the connection line.
Determine the amount of data involved in the connection	The thickness of the line in the graph indicates the amount of data involved in the connection. A thicker line indicates a greater amount of data. This information is based on the amount of bytes involved in the communication
Highlight a connection path	Move the pointer of your mouse over the connection line. If the connection is allowed, the path highlights green. If the connection is denied, the path highlights red.
Determine the connection path for a particular node	Move the pointer of your mouse over the node. If the node is allowed, the path to the node and the node highlight in green. If the node is denied, the path to the node and the node highlights in red.
Change graph view	Using the preview thumbnail, move the thumbnail to the portion of the graph you want to display.

Using Pie, Bar, and Table Charts

To view connections data using a pie, bar, or table chart:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Connections**.

If you previously saved a search to be the default, the results for that saved search is displayed. For more information on saving search criteria, see Saving search criteria.

Step 3 Perform a search.

For more information about searching, see Using the search feature.

NOTE

The pie, bar, and table chart options only appear if the search includes Group By options selected in the Advanced View Definition options. For more information, see Using the search feature.

Step 4 In the charts pane, click the **Configuration** icon.

Configuration options are displayed.

Step 5 Configure the parameters:

Table 7-6 Chart Menu Options

Parameters	Description
Value to Graph	Using the **Value to Graph** drop-down list box, select the object type to which you want to graph on the chart. Options include all normalized and custom flow parameters included in your search parameters.
Chart Type	Using the **Chart Type** drop-down list box, select the chart type you want to view. Options include: • **Table** - Displays data in a table. • **Bar** - Displays data in a bar chart. • **Pie** - Displays data in a pie chart.

Step 6 Click **Save**.

The chart refreshes, displaying the chart according to your configuration changes. The data does not refresh automatically, unless your search criteria is displayed to automatically display details. See Using the search feature.

Step 7 To refresh the data, click **Update Details**.

Using the search feature

The Search feature allows you to search connections using specific criteria and display connections that match the search criteria in a results list. You can create a new search or load a previously saved set of search criteria.

Searching connections

To search connections:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Connections**.

The Connections window is displayed. If you previously saved a search to be the default, the results for that saved search is displayed.

Step 3 Using the **Search** drop-down list box, select **New Search**.

The Search window is displayed.

Step 4 If you want to load a previously saved search, use one of the following options:

a From the **Group** drop-down list box, select the group to which the saved search is associated.

b From the Available Saved Searches list, select the saved search you want to load.

c In the **Type Saved Search or Select from List** field, type the name of the search you want to load. From the Available Saved Searches list, select the saved search you want to load.

d Click **Load**.

After you load the saved search, the Edit Search pane is displayed.

e In the Edit Search pane, select the options you want for this search:

Table 7-7 Edit Search Options

Parameter	**Description**
Include in my Quick Searches	Select the check box if you want to include this search in your Quick Search items.
Include in my Dashboard	Select the check box if you want to include the data from your saved search in your Dashboard. This parameter is only available if the search is grouped. ***Note:*** *For more information about the QRadar SIEM Dashboard, see the IBM Security QRadar SIEM Users Guide.*
Set as Default	Select the check box if you want to set this search as your default search.
Share with Everyone	Select the check box if you want to share these search requirements with all other QRadar Risk Manager users.

Step 5 In the Time Range pane, select an option for the time range you want to capture for this search:

a Choose one of the following options.

Table 7-8 Edit Search Options

Parameter	**Description**
Recent	Using the drop-down list box, specify the time range you want to filter.
Specific Interval	Using the calendar, specify the date and time range you want to filter.

b If you are finished configuring the search and want to view the results, click **Search**.

Step 6 In the Search Parameters pane, define your specific search criteria:

a Using the first drop-down list box, select an attribute on which you want to search. For example, Connection Type, Source Network, or Direction.

b Using the second drop-down list box, select the modifier you want to use for the search. The list of modifiers that appear depends on the attribute selected in the first list.

c In the text field, type specific information related to your search.

d In the Value field, select the modifier you want to use for the search. The list of modifiers that appear depends on the selected attribute in the Type drop-down list box.

e Click **Add Filter**.

f Repeat steps a through e for each filter you want to add to the search criteria.

g If you are finished configuring the search and want to view the results, click **Search**. Otherwise, proceed to next step.

The filter is displayed in the Current Filters text box.

Step 7 If you want to automatically save the search results when the search is completed, select the **Save results when search is complete** check box and specify a name.

Step 8 If you are finished configuring the search and want to view the results, click **Search**. Otherwise, proceed to next step.

Step 9 Using the Column Definition pane, define the columns and column layout you want to use to view the results:

a Using the **Display** list box, select the view you want to associate with this search.

b Click the arrow next to Advanced View Definition to display advanced search parameters. Click the arrow again to hide the parameters.

c Customize the columns to display in the search results:

Table 7-9 Advanced View Definition Options

Parameter	Description
Type Column or Select from List	Filters the columns in the Available Columns list. Type the name of the column you want to locate or type a keyword to display a list of column names that include that keyword. For example, type **Source** to display a list of columns that include Source in the column name.
Available Columns	Lists available columns associated with the selected view. Columns that are currently in use for this saved search are highlighted and displayed in the **Columns** list.
Add and remove column buttons (top set)	The top set of buttons allows you to customize the **Group By** list. • **Add Column** - Select one or more columns from the **Available Columns** list and click the **Add Column** button. • **Remove Column** - Select one or more columns from the **Group By** list and click the **Remove Column** button.
Add and remove column buttons (bottom set)	The bottom set of buttons allows you to customize the **Columns** list. • **Add Column** - Select one or more columns from the **Available Columns** list and click the **Add Column** button. • **Remove Column** - Select one or more columns from the **Columns** list and click the **Remove Column** button.

Table 7-9 Advanced View Definition Options (continued)

Parameter	Description
Group By	Specifies the columns from which the saved search groups the results. You can further customize the **Group By** list using the following options: • **Move Up** - Select a column and move it up through the priority list using the **Move Up** icon. • **Move Down** - Select a column and move it down through the priority list using the **Move Down** icon. The priority list specifies in which order the results are grouped. The search results will group by the first column in the **Group By** list and then group by the next column on the list.
Columns	Specifies columns chosen for the search. The columns are loaded from a saved search. You can customize the **Columns** list by selecting columns from the **Available Columns** list. You can further customize the **Columns** list by using the following options: • **Move Up** - Select a column and move it up through the priority list using the move up button. • **Move Down** - Select a column and move it down through the priority list using the move down button. If the column type is numeric or time *and* there is an entry in the **Group By** list, the column includes a drop-down list box to allow you to choose how you want to group the column.
Order By	Using the first list box, specify the column by which you want to sort the search results. Then, using the second list box, specify the order you want to display for the search results: **Descending** or **Ascending**.

Step 10 Click **Search**.

The search results are displayed.

Saving search criteria

To save the specified search criteria for future use:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Connections.**

The Connections window is displayed.

Step 3 Perform a search. See Searching connections.

The search results appear.

Step 4 Click **Save Criteria**

The Save Search window is displayed.

Step 5 Configure values for the following parameters:

Table 7-10 Save Search Parameters

Parameter	Description
Search Name	Type a name you want to assign to this search criteria.
Assign Search to Group(s)	Select the check box for the group you want to assign to this saved search. If you do not select a group, this saved search is assigned to the Other group by default.
Timespan options	Choose one of the following options: • **Recent** - Using the drop-down list box, specify the time range you want to filter. • **Specific Interval** - Using the calendar, specify the date and time range you want to filter.
Include in my Quick Searches	Select the check box if you want to include this search in your Quick Search items, which is available from the **Search** drop-down list box.
Include in my Dashboard	Select the check box if you want to include the data from your saved search in your Dashboard. For more information on the Dashboard, see the *IBM Security QRadar SIEM Users Guide*. ***Note:*** *This parameter is only displayed if the search is grouped.*
Set as Default	Select the check box if you want to set this search as your default search.
Share with Everyone	Select the check box if you want to share these search requirements with all other QRadar Risk Manager users.

Step 6 Click **OK**.

Performing a sub-search

Each time you perform a search, QRadar SIEM searches the entire database for connections that match your criteria. This process may take an extended period of time depending on the size of your database.

The sub-search feature allows you to perform searches within a set of completed search results. The sub-search function allows you to refine your search results without requiring you to search the database again. This feature is not available for grouped searches or searches in progress.

To perform a sub-search, perform the following steps:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Connections.**

The Connections window is displayed.

Step 3 Perform a search.

For more information, see Searching connections.

Step 4 Wait until the search has completed.

The search results are displayed. Additional searches use the dataset from the previous search when sub-searches are performed.

Step 5 To add a filter, perform the following steps:

a Click **Add Filter**.

The Add Filter window is displayed.

b Using the first drop-down list box, select an attribute on which you want to search.

c Using the second drop-down list box, select the modifier you want to use for the search. The list of modifiers that appear depends on the attribute selected in the first list.

d In the text field, type specific information related to your search.

e Click **Add Filter**.

You can also right-click on a connection to select a Filter on option.

NOTE

If the search remains in progress, partial results are displayed.

The Original Filter pane indicates the filter from which the original search was based. The Current Filter pane indicates the filter applied to the sub-search.

NOTE

You can clear sub-search filters without restarting the original search. Click the Clear Filter link next to the filter you want to clear. If you clear a filter from the Original Filter pane, the original search is relaunched.

Step 6 Click **Save Criteria** to save the sub-search.

For more information, see Saving search criteria.

NOTE

If you delete the original search, you can access the saved sub-search. If you add a filter, the sub-search searches the entire database since the search function no longer bases the search on a previously searched dataset.

Managing search results

You can perform multiple connection searches while navigating to other interfaces. You can configure the search feature to send you an email notification when a search is complete. At any time while a search is in progress, you can view partial results of a search in progress.

Viewing Managed Search Results

To manage search results, perform the following steps:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Connections**.

The Connections window is displayed.

Step 3 From the menu, select **Search > Manage Search Results**.

The search results window displays the following parameters:

Table 7-11 Manage Search Results Window

Parameter	**Description**
Flags	Indicates that an email notification is pending for when the search is complete.
User	The name of the user who started the search.
Name	The name of the search, if the search has been saved. For more information on saving a search, see Saving Search Results.
Started On	The date and time the search was started.
Ended On	The date and time the search ended.
Duration	The amount of time the search took to complete. If the search is currently in progress, the Duration specifies how long the search has been processing to date. If the search was canceled, the Duration parameter specifies the period of time the search function was processing before it was canceled.
Expires On	The date and time an unsaved search result will expire. A saved search does not expire.
Status	The status of the search. The options are: • **Queued** - Indicates that the search is queued to start. • **<percent>% Complete** - The progress of the search in terms of percentage complete. You can click the link to view partial results. • **Sorting** - Indicates that the search has finished collecting results and is currently preparing the results for viewing. • **Canceled** - Indicates that the search has been canceled. You can click the link to view the results that were collected prior to the cancellation. • **Completed** - Indicates that the search is complete. You can click the link to view the results. See Viewing connections.
Size	The file size of the search result set.

The search results toolbar provides the following options:

Table 7-12 Manage Search Results Toolbar

Parameter	**Description**
New Search	Click **New Search** to create a new search. When you click this button, the search window is displayed. For more information, see Searching connections.
Save Results	Click **Save Results** to save search results. For more information, see Saving Search Results. ***Note:*** *This option is only enabled when you have selected a row in the Manage Search Results list.*

Table 7-12 Manage Search Results Toolbar (continued)

Parameter	Description
Cancel	Click **Cancel** to cancel searches that are in progress or are queued to start. For more information, see Canceling a Search.
Delete	Click **Delete** to delete a search result. For more information, see Deleting a Search.
Notify	Select the search(es) for which you want to receive notification, and then click **Notify** to enable email notification when the search is complete.
View	From the drop-down list box, specify which searches results you want to list in the search results window. The options are: • Saved Search Results • All Search Results • Canceled/Erroneous Searches • Searches in Progress

Saving Search Results

To save search results, perform the following steps:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Connections.**

The Connections window is displayed.

Step 3 Perform a connection search or sub-search. For more information on how to perform a connection search, see Searching connections.

For more information about how to perform a sub-search, see Performing a sub-search.

Step 4 From the Search Results window, select **Search > Manage Search Results** and select a search result.

Step 5 Click **Save Results**.

NOTE

The Save Results button is enabled only when the search is complete or if the search was canceled while in progress.

The Save Search Result window is displayed.

Step 6 Type a name for the search results.

Step 7 Click **OK**.

The saved search results displays the name in the **Name** column of the Manage Search Results window.

Canceling a Search

To cancel a search, perform the following steps:

Step 1 From the Manage Search Results window, select the queued or in progress search result you want to cancel.

NOTE

You can also cancel a search from the partial results search using the Cancel Search button.

Step 2 Click **Cancel Search**.

NOTE

You can select multiple searches to cancel.

A confirmation window is displayed.

Step 3 Click **Yes**.

If the search was in progress when canceled, the results that were accumulated until the cancellation are maintained.

Deleting a Search

To delete a search, perform the following steps:

Step 1 From the Manage Search Results window, select the search result you want to delete.

Step 2 Click **Delete**.

A confirmation window is displayed.

Step 3 Click **Yes**.

The search is removed from the search results window.

Exporting connections

You can export connections in Extensible Markup Language (XML) or Comma Separated Values (CSV) format.

To export connections, perform the following steps:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, click **Connections.**

The Connections window is displayed.

a If you want to export the connection in XML format, select **Actions > Export to XML**.

b If you want to export the connection in CSV format, select **Actions > Export to CSV**.

The status window is displayed.

Step 3 If you want to resume your activities, click **Notify When Done**.

When the export is complete, you receive notification that the export is complete. If you did not select **Notify When Done**, the status window disappears when the export is complete.

8 VIEW DEVICE CONFIGURATIONS

You can view configuration information for devices in your network on the Configuration Monitor page.

Use this page to compare network device configurations, view existing rules, the event count for triggered rules, and a history of rules for devices in your topology.

NOTE

It is important for rule searching and event counts that devices in QRadar Risk Manager are properly mapped to the log sources for the devices. For information on mapping log sources, see **Log source mapping**.

Device configurations

You can view information about devices in your Topology, such as routers, firewalls, and switches.

You can also perform a device search and create or edit a log source mapping. For more information, see **Creating a log source mapping**.

There are two levels of information displayed on the configuration monitor page: basic and detailed.

Basic device information contains a list of all devices in the configuration monitor and basic details about the device, such as IP address, device contexts, adapter information, and the time of the last configuration backup. Each context in a multiple-context device is displayed as a separate row in the list. There is also a separate row that represents the Admin context of the multiple-context device.

Detailed device information contains detailed configuration information for a specific device, such as information on device rules, interfaces, adapter information, and specialized searches for you device from the toolbar.

Viewing basic device configurations

Use the default configuration to view a list of devices and basic identifying information.

To view a basic device configuration:

Step 1 Click the **Risks** tab.

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

The list of configured devices is displayed and includes the following configuration information.

Table 8-1 Configuration Monitor Parameters

Parameter	Description
Device IP	The management IP address of the device.
Context	The name of the device context.
Hostname	The hostname of the device.
Adapter	The adapter name associated with this device.
Type	The type of device. For example, firewall, router, or IPS.
Vendor	The vendor for the device.
Model	The model number for the device.
Log Source(s)	If a log source is configured in QRadar SIEM, the following information is provided: • The log sources mapped to the current device. • The username in parenthesis of the user that mapped the log source to a device. If the device was auto-mapped, then auto-mapped is displayed.
Config Obtained On	The date and time that the configuration was obtained for this device.

Viewing detailed device configurations

You can double-click on a device in the Configuration Monitor list to view detailed information for the specific network device. The detailed information for the device provides configuration information, such as configured rules, interface, event counts, configuration history, and advanced rule searching.

You can filter by events, offenses, history, and view device connections in the Topology.

To view the detailed device configuration, perform the following steps:

Step 1 Click the **Risks** tab.

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

Step 3 Double-click any device to view the detailed configuration information.

Step 4 The Device toolbar provides the following functions:

Table 8-2 Device Toolbar Functionality

Button	Function
Interfaces	Allows you to view a list of interfaces for this device. This information is obtained from the device configuration.
Rules	Allows you to view a list of rules obtained from the device configuration. The Rules pane provides a search function that allows searching for specific device rules. For more information, see **Searching rules**.
NAT	Allows you to view a list of NAT rules for the device.
History	Allows you to view a history of configuration backup information from Configuration Source Management and provides a comparison of current and previous device configurations.
Events	Allows you to view all events associated with this device. For more information on the **Log Activity** tab, see the *IBM Security QRadar SIEM Users Guide*.
Offenses	Allows you to view all offenses associated with this device. For more information on the **Offenses** tab, see the *IBM Security QRadar SIEM Users Guide*.
Topology	Allows you to view the Topology with a filter displaying devices and subnets that are communicating to your device in the topology model. For more information on the topology model, see **Use the topology**.
Print	Allows you to print the device details.

The device table provides a detailed summary of information for your device:

Table 8-3 Detailed Configuration Monitor Information

Parameter	Description
IP/Context	The first entry provides the management IP address of the device. When a multiple-context device exists, the second entry provides the name of the device context. Otherwise, N/A displays.
Current Interfaces	The number of network interfaces on the device. Detailed interface information can be viewed using one of the following methods: • To view advanced interface information, select **Interfaces** from the Device toolbar. • To view advanced interface information, from the **Current Interfaces** field, click the interface number displayed.

Table 8-3 Detailed Configuration Monitor Information

Parameter	Description
Current Rules	The number of rules that are configured on the device. Detailed rule information can be viewed using one of the following two methods: • To view rule information, select **Rules** from the Device toolbar. • To view rule information from the **Current Rules** field, click the rule number displayed.
Current NAT Rules	The number of NAT rules that are configured on the device. Detailed rule information can be viewed using one of the following two methods: • To view rule information, select **NAT** from the Device toolbar. • To view rule information from the **Current NAT** field, click the rule number displayed.
Config Obtained On	The date and time that the configuration was obtained for this device.
Current Log Source(s)	If a log source is configured in QRadar SIEM, the following information is provided: • The names of any log sources mapped to the current device. • The username, in parenthesis, of the user that mapped the log source to a device. If the device was auto-mapped, then auto-mapped is displayed. For more information on log source mapping, see **Log source mapping**.
Hostname	The hostname of the device.
Adapter	The adapter name associated with this device.
Type	The type of device. For example, firewall, router, switch, or IPS/IDP.
Vendor	The vendor for the device.
Model	The model number for the device.

Step 5 Click **Interfaces** to view a detailed list of interface information for your device.

Table 8-4 Interface Parameters

Parameter	Description
Name	The name of the interface as named on the device.
IF Index	The IFIndex as associated to the interface.

Table 8-4 Interface Parameters (continued)

Parameter	Description
Status	The current status of the interface. The options are: • **Up** - The device interface is working properly. • **Down** - The device interface is disabled or not working properly.
Type	The type of interface, for example, Ethernet or Software Loopback.
CIDR	The CIDR range for the interface.
MAC	The MAC address associated with the interface.
Speed (bps)	The speed of the interface, in bits per second (bps).
MTU	The maximum transmission unit for the interface.

The following table provides additional functions available in the Interface table.

Table 8-5 Interface Table Functions

Function	Description
Search	Type an IP address or CIDR range to filter the Interface table. • If you specify a single IP address, all interfaces with a matching host IP address is displayed. • If you specify a CIDR range, all interfaces with a CIDR range matching or containing the filter CIDR is displayed.

Step 6 Click **Rules** to view the list of rules for this device.

Table 8-6 Rules Parameters

Parameter	Description
Status	The status of the rules on the device. Rules that have been status messages are displayed in this column, such as shadowed or deleted rules. If an icon is displayed in the **Status** column, then more information is available by hovering your mouse over the status icon.
Config Date/Time	The date and time that the configuration was obtained for this device. ***Note:*** *If a rule contains multiple configurations, the field displays Multiple(n), where n represents the number of configurations that have been coalesced. Placing your cursor over the Multiple(n) value displays all of the rules that have been coalesced together.*
List	The name of the Access Control List (ACL) is displayed, as defined in the device. An ACL is a collection of individual rules.
Entry	The order number of the rule you are searching for.

Table 8-6 Rules Parameters (continued)

Parameter	Description
Action	The action associated with this rule. The options are: • **Accept** - The device permits the packet. • **Deny** - The device denies the packet. • **Forward** - The packet was forwarded by the device. • **Next** - The rule is evaluated against the next ACL. • **None** - The rule is evaluated against the next ACL.
Source(s)	The source for the rule, for example, IP address, group, or hostname.
Source Service(s)	The source service for the rule. This parameter includes a collection of port ranges, such as 100-200, and/or port expressions, such as 80(TCP). If the port is negated, the port information also includes an exclamation mark and may be surrounded by parenthesis, for example, !(100-200) or !80(TCP).
Destination(s)	The destination for the rule, for example, IP address, group, or hostname.
Destination Service(s)	The destination service for the rule. This parameter includes a collection of port ranges, such as 100-200, and/or port expressions, such as 80(TCP). If the port is negated, the port information also includes an exclamation mark and may be surrounded by parenthesis, for example, !(100-200) or !80(TCP).
Protocol(s)	The protocol or group of protocols associated with this rule.
Signature(s)	The vulnerability information associated with this rule as defined by the IPS device.
Event Count	The number of events that have been triggered by the rule are displayed.

Step 7 Click **NAT** to view the list of NAT rules for this device.

Table 8-7 NAT Parameters

Parameter	Description
List	The name of the list in which this NAT rule belongs.
Entry	The order number of the rule you are searching for.
Phase	Specifies when to trigger this NAT rule. For example, before or after routing.
Type	Specifies how the translations are applied for the NAT rule; static or dynamic.
Source(s)	The source that triggers this rule. For example, IP address, group, or hostname.
Source Service(s)	The source service that triggers this rule.
Destination(s)	The destination that triggers this rule. For example, IP address, group, or hostname.

Table 8-7 NAT Parameters (continued)

Parameter	Description
Destination Service(s)	The destination service that triggers this rule.
Protocol(s)	The protocol or group of protocols associated with this rule.
Source Translation(s)	The translations that can be applied to the source(s).
Source Port Translation(s)	The translations that can be applied to the source port(s).
Destination Translation(s)	The translations that can be applied to the destination(s).
Destination Port Translation(s)	The translations that can be applied to the destination port(s).
Config Date/Time	The date and time that the rule was backed up.

Viewing device configuration history

As QRadar Risk Manager backs up devices over time the configurations are retained, which allows you to view the historical changes to the device. Historical device configurations can be used to compare changes between backups on a single device or compare configurations between devices. Comparing device configurations allow you to view device rules in a normalized comparison view or by viewing the raw device configuration. The Normalized Device Configuration is a graphical comparison view that provides rules added, deleted, or modified between devices. The Raw Device Configuration is an XML or plain text view of the device file.

Viewing a single device history

To view the configuration history of a single network device, perform the following steps:

Step 1 Click the **Risks** tab.

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

Step 3 Double-click a configuration to view the detailed device information.

Step 4 Click **History**.

Table 8-8 Device Backup History Parameters

Parameter	Description
Configuration	The configuration provides the type of files stored in QRadar Risk Manager for your network device. The common configuration types can include: • **Standard-Element-Document** - Standard-Element Document (SED) files are XML data files that contain information on your network device. Individual SED files are viewed in their raw XML format. If an SED is compared to another SED file, then the view is normalized to display the rule differences. • **Config** - Configuration files are provided by certain network devices depending on the device manufacturer. A configuration file can be viewed by double-clicking on the config file. ***Note:*** *Depending on the information the adapter collects for your device, several other configuration types may be displayed. These files are displayed in plain text view when double-clicked.* ***Note:*** *The plain text view supports find (Ctrl +f), paste (Ctrl+v), and copy (Ctrl+C) from the browser window.*
Date Obtained	The date that the device configuration was last backed up from Configuration Source Management.

Step 5 From the History pane, select a configuration.

Step 6 Click **View Selected**.

Comparing configurations

Device configurations can be compared to each other by comparing multiple backups on a single device or by comparing one network device backup to another.

To compare device configurations, perform the following steps:

Step 1 Click the **Risks** tab.

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

Step 3 Double-click any device to view the detailed configuration information.

Step 4 Click **History** to view the history for this device.

Step 5 Select your comparison type from the table below:

Table 8-9 Device Comparisons

If you want to	Then
Compare two configurations on a single device	To compare two configurations on a single device: **1** Select a primary configuration. **2** Press the Ctrl key and select a second configuration for comparison. **3** From the History pane, click **Compare Selected**. If the comparison files were Standard-Element-Documents (SEDs), then Normalized Device Configuration Comparison window is displayed with a table showing rule differences between the backups. When comparing normalized configurations, the color of the text indicates the following: • **Green Dotted Outline** - Indicates a rule or configuration that was added to the device. • **Red Dashed Outline** - Indicates a rule or configuration that was deleted from the device. • **Yellow Solid Outline** - Indicates a rule or configuration that was modified on the device. **4** Optional. To view the raw configuration differences, click **View Raw Comparison**. ***Note:*** *If the comparison was a config file or another backup type, then the raw comparison is displayed.*

Table 8-9 Device Comparisons (continued)

If you want to	Then
Compare two configurations on different devices	To compare two configurations on separate devices, you must mark a configuration for comparison on one device, then compare a device backup to the marked configuration. To compare device configurations: **1** Select a primary configuration from a device. **2** Click **Mark for Comparison**. **3** From the navigation menu, select **All Devices** to return to the device list. **4** Double-click the device to compare and click **History**. **5** Select a configuration that you want to compare with the marked configuration. **6** Click **Compare with Marked**. If the comparison files were Standard-Element-Documents (SEDs), then the Normalized Device Configuration Comparison window is displayed with a table showing rule differences between the backups. When comparing normalized configurations, the color of the text indicates the following: • **Green Dotted Outline** - Indicates a rule or configuration that was added to the device. • **Red Dashed Outline** - Indicates a rule or configuration that was deleted from the device. • **Yellow Solid Outline** - Indicates a rule or configuration that was modified on the device. **7** Optional. To view the raw configuration differences, click **View Raw Comparison**. ***Note:*** *If the comparison was a config file or another backup type, then the raw comparison is displayed.*

Searching devices

The Configuration Monitor provides a search feature to locate devices you've added using Configuration Source Management. The device configuration search provides the ability to search devices using a specified time frame, then filter by the IP/CIDR address, context, hostname, adapter, vendor, type, or model.

To search the device for detailed rule information:

Step 1 Click the **Risks** tab.

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

Step 3 From the **Search** list box, select a search option:

Table 8-10 Search Options

Parameter	Description
New Search	Start a new search for a device.
Edit Search	Edit an existing device search. This option allows you to modify a search to add or remove parameters. Additional search parameters are included as current search filters in the results.

Step 4 Configure values for your device search:

Table 8-11 Device Search Criteria

Parameter	Description
Config Obtained Date/Time Range	Select a time range to search for devices. The search is based on the timestamp for the last time a device configuration was backed up in Configuration Source Management. The following options are available: • **Current** - Search for devices based on the most recent device configuration backup. • **Interval** - Search for devices using a predefined time interval. Devices that have configuration backups within the specified interval are included in the results and filtered by any additional search options. The interval includes a minimum time interval of the last hour to a maximum interval of the last 30 days. • **Specific** - Search for devices using a configuration within a specific date and time frame. Devices that have configuration backups within the specified interval are included in the results and filtered by any additional search options.
IP/CIDR	Type the IP/CIDR address of the device you are searching for from the device list.
Hostname	Type the hostname of the device you are searching for from the device list. This parameter supports alphanumeric characters, dashes (-), or periods (.).
Type	Select the type of device you are searching for in the device list. The search types include: • Router • Firewall • Switch • IPS/IDS
Context	Type the name of the context.

Table 8-11 Device Search Criteria (continued)

Parameter	Description
Adapter	Select the adapter type you are searching for from the list. The options include: • Check Point SecurePlatform • Cisco IOS • Cisco Security Appliance • Generic XML • Juniper JunOS • Juniper NSM • Juniper Screen OS
Vendor	Select the vendor name of the device you are searching for from the device list. This parameter supports alphanumeric characters, dashes (-), or periods (.).
Model	Type the model of the device you are searching for from the device list. This parameter supports alphanumeric characters, dashes (-), or periods (.).

Step 5 Click **Search**.

Searching rules

The Configuration Monitor provides a search feature to locate rules that have changed on the devices in your topology. Rule searching can only be performed from the Rules pane, which is located in the detailed device view of the Configuration Monitor. Rule searching provides a method for discovering rule changes that occur between device configuration backups.

NOTE

The results returned for a rule search is based on the Configuration Source Management backup of your device. We recommend you schedule device backups with your firewall policy update window. This allows QRadar Risk Manager to have the latest rule information when rule searches are performed.

To search a device for detailed rule information:

Step 1 Click the **Risks** tab.

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

Step 3 Double-click a device from the Configuration Monitor.

Step 4 Click **Rules**.

Step 5 From the Rules pane, select the **Search** list box and choose a search option:

Table 8-12 Search Options

Parameter	Description
New Search	Start a new rule search.
Edit Search	Edit an existing rule search. This option allows you to modify a search to add or remove parameters. Additional search parameters are included as current search filters in the results.

Step 6 Configure values for your rule search:

Table 8-13 Search Criteria Parameters

Parameter	Description
Config Obtained Date/Time Range	Select a time interval or range to search for devices based on a time frame or the last time a device configuration was changed or device specification (model, vendor, etc.). The following options are available: • **Current** - Search for devices from the most recent device configuration backup. • **Interval** - Search for rules using a configuration from a predefined time interval. The interval includes a minimum time interval of the last hour to a the maximum interval of the last 30 days. • **Specific** - Search for rules using a configuration within a specific date and time frame.
Status	Select any check box for the rule status you want to include in the rule search. The options include: • **Shadowed** - A shadowed rule is a rule that can never trigger. In most cases, shadowed rules are due to a prior ACL in the rule list for the device covering the same network traffic. • **Deleted** - A deleted rule is a rule that has been deleted within the time frame of your search. • **Other** - Rules that are marked other include rules that do not have any status or rules that are a subset of a shadowed or deleted rule.
List	Type the name of the Access Control List (ACL), as defined in the device. An ACL is a collection of individual rules.
Entry	Type the order number of the rule entry for the device. Only numeric values can be typed in the **Entry** field. The ACL of the device is searched for the rule order you specify.

Table 8-13 Search Criteria Parameters (continued)

Parameter	Description
Action	The action associated with this rule. The options are: • **Accept** - The device permits the packet. • **Deny** - The device denies the packet. • **Forward** - The packet was forwarded by the device. • **Next** - The rule is evaluated against the next ACL. • **None** - The rule is evaluated against the next ACL.
Protocol	The protocol or group of protocols associated with this rule. ***Note:*** *Only TCP, UDP, and ICMP protocols return event counts when searching rules in QRadar Risk Manager. The other protocols return matching rules when searched, but not event counts.*
Source/Destination	Type an IP address, CIDR address, host name, or object group reference for the source or destination of the rule. • If you type a host name, or object group reference name, a text search is performed for the source or destination of the rule. The search results contain any rules that match the text you entered. • If you type a CIDR address in your rule search, the results returned are rules that contain an exact CIDR address match or rules where the CIDR address is part of a larger CIDR address group.
Service	Type a value to search on the service for the rule. The service can include ports or object group references. For example, the service can include a collection of port ranges, such as 100-200, or port expressions, such as 80(TCP). If the port is negated, the port information also includes an exclamation mark and may be surrounded by parenthesis, for example, !(100-200) or !80(TCP).
Signature(s)	The vulnerability information associated with this rule as defined by the IPS device.
Event Count	Select an operator and type a numeric value to search for a matching event count within the configuration search time frame. ***Note:*** *Selecting a protocol other than TCP, UDP, or ICMP may not return an event count.*
Order By	Select order you of the search results. The options include: • **Device Rule Order** - Sort the search results by the numeric order of the ACL rule entry. • **Event Count** - Sorts the search results by the number of events.

Table 8-13 Search Criteria Parameters (continued)

Parameter	Description
Asc	The search results are sorted in an ascending manner, for example, 1 to 5.
Desc	The search results are sorted in an descending manner, for example, 5 to 1.

Step 7 Click **Search**.

Log source mapping

QRadar Risk Manager automatically identifies and maps devices to the log source providing events in QRadar SIEM. This allows an administrator to verify that all devices configured in QRadar Risk Manager are mapped to the correct log source. A maximum of 255 devices can be mapped to a log source in QRadar Risk Manager, but devices can have multiple log sources.

Log Source Mapping provides administrators with the following:

- The Log Source(s) column provides information on which log source is mapped to a particular device.
- The ability to see which devices are mapped to more than one log source.
- Identifies if a log source map is unmapped, added or edited by an administrator, or if QRadar Risk Manager mapped the log source to a device automatically.
- Allows the **Search Events** right-click option in the Topology.
- Provides information on event counts when rules are searched on specific devices.

The Configuration Monitor displays the following information in the Log Source(s) column:

- **Auto-Mapped** - The term (Auto-mapped) is displayed in the Log Source(s) column when QRadar Risk Manager identified the log source and mapped the log source to the device automatically.
- **Username** - If an administrator manually added or edited a log source, QRadar Risk Manager identifies the administrator by username in parenthesis.
- **Blank** - If QRadar Risk Manager is unable to identify a log source for the device, the Log Source(s) column shows no value.

Creating a log source mapping

To create a log source mapping in QRadar Risk Manager:

Step 1 Click the **Risks** tab.

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

Step 3 Select the device without a log source.

Step 4 Click **Create/Edit Mapping**.

The Create/Edit Mapping window is displayed.

Step 5 From the **Log Source** drop-down list box, select a group.

Step 6 Select a log source.

Step 7 Click **Add**.

Step 8 Click **Save**.

Editing an incorrect log source mapping

Editing a log source does not prevent QRadar Risk Manager from remapping a log source. If you want to prevent an incorrect log source from automatically remapping, you must delete the log source mapping and select the **Do not allow this mapping to be auto-mapped again** check box.

For information about deleting a log source mapping, see **Deleting a Log Source Mapping**.

To edit an incorrect log source mapping in QRadar Risk Manager:

Step 1 Click the **Risks** tab.

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

Step 3 Select the device with an incorrect log source mapping.

Step 4 Click **Create/Edit Mapping**.

Step 5 From the **Mapping Log Sources** window, select the log source that is improperly mapped.

Step 6 Click **Remove Selected**.

Step 7 From the **Log Source** drop-down list box, select a group.

Step 8 Select the correct log source to map.

Step 9 Click **Add**.

Step 10 Click **Save**.

Deleting a Log Source Mapping

To delete a log source mapping from a device:

Step 1 Click the **Risks** tab.

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

Step 3 Select the device with an incorrect log source mapping.

Step 4 Click **Delete Mapping**.

In the Delete Mapping window, the **Do not allow this mapping to be auto-mapped again** check box is available.

- If you select the **Do not allow this mapping to be auto-mapped again** check box to prevent QRadar Risk Manager from attempting to map the log source to a device in the future.

- If you clear the **Do not allow this mapping to be auto-mapped again** check box, then QRadar Risk Manager attempts to re-map the log source to a device in the future.

Step 5 Click **Delete** to confirm.

Printing device configuration

To print device configuration, perform the following steps:

Step 1 Click the **Risks** tab.

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

Step 3 Double-click a device from the Configuration Monitor.

Step 4 From the Device pane, click **Print**.

9 MANAGING IBM SECURITY QRADAR RISK MANAGER REPORTS

You can create, edit, distribute, and manage reports for your network devices using IBM Security QRadar Risk Manager. Detailed reports on firewall rules and connections between devices are often required to satisfy various regulatory standards, such as PCI compliance.

QRadar Risk Manager provides the following additional report options:

- Detailed reports on connections between your devices.
- Detailed reports for the firewall rules on your device.
- Detailed reports for unused objects on your device.

Create QRadar Risk Manager reports

You can use the Report Wizard to create a new report. The Report Wizard provides a step-by-step guide on how to design, schedule, and generate reports. The wizard uses the following key elements to help you create a report:

- **Layout** - Position and size of each container
- **Container** - Placeholder and location for content in your report
- **Content** - Defines the report data QRadar Risk Manager includes in chart for the container

When you select the layout of a report, consider the type of report you want to create. For example, do not choose a small chart container for graph content that displays a large number of objects. Each graph includes a legend and a list of networks from which the content is derived; choose a large enough container to hold the data.

The scheduled time must elapse for reports that generate weekly or monthly before the generated report returns results. For a scheduled report, you must wait the scheduled time period for the results to build. For example, a weekly search requires 7 days to build the data. This search returns results after 7 days elapse.

Table 9-14 Report intervals for QRadar Risk Manager reports

Report interval	Description
Manual	Generates a report one time without a reoccurring schedule.

Table 9-14 Report intervals for QRadar Risk Manager reports

Report interval	Description
Hourly	Schedules the report to generate hourly. If you choose the **Hourly** option, further configuration is required. From the list boxes, select a time frame to begin and end the reporting cycle. A report is generated each hour within this time frame. Time is available in 30-minute increments. The default hourly report is scheduled to run at 1:00 a.m.
Daily	Schedules the report to generate daily. For each chart on a report, you can select the previous 24 hours of the day, or select a specific time frame from the previous day. If you choose the **Daily** option, further configuration is required. Select the check box beside each day you want to generate a report. Also, you can use the list box to select a time to begin the reporting cycle. Daily reports can be scheduled in 30-minute increments. The default daily report is scheduled to run at 1:00 a.m.
Weekly	Schedules the report to generate weekly. If you choose the **Weekly** option, further configuration is required. Select the day you want to generate the report. The default is Monday. From the list box, select a time to begin the reporting cycle. Weekly reports can be scheduled in 30-minute increments. The default weekly report is scheduled to run at 1:00 a.m.
Monthly	Schedules the report to generate monthly. If you choose the **Monthly** option, further configuration is required. From the list box, select the date you want to generate the report. The default is the first day of the month. Also, use the list box to select a time to begin the reporting cycle. Monthly reports can be scheduled in 30-minute increments. The default monthly report is scheduled to run at 1:00 a.m.

The following types of charts are available for QRadar Risk Manager.

Table 9-15 Types of QRadar Risk Manager charts

Report type	Description
Connections	A connections report displays connection diagrams for your network devices that occurred during your specified time frame.
Device rules	A device rule report displays the rules configured on your network device during your specified time frame.

Table 9-15 Types of QRadar Risk Manager charts

Report type	Description
Device unused objects	A device unused object report produces a table with the name, configuration date/time, and a definition for any object reference groups that are not in use on the device. An object reference group is a generic term used to describe a collection of IP addresses, CIDR addresses, host names, ports, or other device parameters which are grouped together and assigned to rules on the device.

An example of Device unused objects is as follows. Check Point devices support grouping IP addresses together in network objects. Network objects can then be assigned to rules within the Check Point device. If a change is made on the network object, the change is implemented on all rules that reference the network object. When the device configuration for a Check Point device is normalized by QRadar Risk Manager, network objects are translated into object reference groups. Not all devices support the notion of an object reference group.

Creating a report

You can create reports for a specific interval and can choose a chart type. A report can consist of several data elements and can represent network and security data in a variety of styles, such as tables, line charts, pie charts, and bar charts.

To create a report:

Step 1 Click the **Reports** tab.

Step 2 From the **Actions** list box, select **Create**.

Step 3 Click **Next** to move to the next page of the Report Wizard.

Step 4 Select the frequency for the reporting schedule.

Step 5 In the Allow this report to generate manually pane, select **Yes** to enable or **No** to disable manual generation of this report.

Step 6 Click **Next**.

Step 7 Configure the layout of your report:

a From the **Orientation** list box, select the page orientation.

b Select a layout option for your QRadar Risk Manager report.

c Click **Next**.

Step 8 Specify values for the following parameters:

- **Report Title** - Type a report title. The title can be up to 100 characters in length. Do not use special characters.
- **Logo** - From the list box, select a logo. The QRadar logo is the default logo. For more information about branding your report, see the *IBM Security QRadar SIEM Administrator Guide*.

Step 9 To configure each container in the report:

a. From the **Chart Type** list box, select one of the QRadar Risk Manager specific reports.

b. Configure the report data for your chart.

   For detailed information about configuring your chart, see **Configuring charts**.

c. Click **Save Container Details**.

d. If required, repeat steps **a** to **c** for all containers in your report layout.

e. Click **Next**.

Charts displayed on the preview page do not display actual data. This is only a graphical representation of the layout you have configured.

Step 10 Click **Next** to move to the next step of the Report Wizard.

Step 11 Select the check boxes for the report formats. You can select multiple options.

Device Rules and Unused Object Rules reports only support the PDF, HTML, and RTF report formats.

Step 12 Click **Next**.

Step 13 Select the distribution channels you want for your report.

Table 9-16 Generated Report Distribution Options

Options	Description
Report Console	Select this check box to send the generated report to the **Reports** tab. This is the default distribution channel.
Select the users that should be able to view the generated report.	This option is only displayed after you select the **Report Console** check box. From the list of users, select the QRadar Risk Manager users you want to grant permission to view the generated reports. ***Note:*** *You must have appropriate network permissions to share the generated report with other users. For more information about permissions, see the IBM Security QRadar SIEM Administration Guide.*
Select all users	This option is only displayed after you select the **Report Console** check box. Select this check box if you want to grant permission to all QRadar Risk Manager users to view the generated reports. ***Note:*** *You must have appropriate network permissions to share the generated report with other users. For more information about permissions, see the IBM Security QRadar SIEM Administration Guide.*
E-mail	Select this check box if you want to distribute the generated report using e-mail.

Table 9-16 Generated Report Distribution Options (continued)

Options	Description
Enter the report distribution e-mail address(es)	This option is only displayed after you select the **E-mail** check box. Type the e-mail address for each generated report recipient; separate a list of e-mail addresses with commas. The maximum characters for this parameter is 255. ***Note:*** *E-mail recipients receive this e-mail from no_reply_reports@qradar.*
Include Report as attachment (non-HTML only)	This option is only displayed after you select the **E-mail** check box. Select this check box to send the generated report as an attachment.
Include link to Report Console	This option is only displayed after you select the **E-mail** check box. Select this check box to include a link the Report Console in the e-mail.

Step 14 Click **Next**.

Step 15 Configure values for the following parameters:

Table 9-17 Finishing Up Parameters

Parameter	Description
Report Description	Type a description for this report. The description is displayed on the Report Summary page and in the generated report distribution e-mail.
Groups	Select the groups to which you want to assign this report. For more information about groups, see Managing Reports in the *IBM Security QRadar SIEM Administration Guide*.
Would you like to run the report now?	Select this check box if you want to generate the report when the wizard is complete. By default, the check box is selected.

Step 16 Click **Next** to view the report summary.

You can select the tabs available on the summary report to preview the report selections.

Step 17 Click **Finish**.

The report immediately generates. If you cleared the **Would you like to run the report now** check box on the final page of the wizard, the report is saved and generates as scheduled.

The report title is the default title for the generated report. If you re-configure a report to enter a new report title, the report is saved as a new report with the new name; however, the original report remains the same.

Configuring charts

The chart type determines the data configured and displayed in the chart. You can create several charts for specific to data collected by devices in QRadar Risk Manager.

The following chart types are specific to QRadar Risk Manager:

- Connections
- Device Rules
- Device Unused Objects

Connections

You can use the Connections chart to view network connection information. You can base your charts on data from saved connection searches from the Risks tab. This allows you to customize the data that you want to display in the generated report. You can configure the chart to plot data over a configurable period of time. This functionality helps you to detect connection trends.

▶ To configure a Connections Chart container, configure values for the following parameters:

Table 9-18 Connections Chart Parameters

Parameter	Description
Container Details - Connections	
Chart Title	Type a chart title to a maximum of 100 characters.
Chart Sub-Title	Clear the check box to change the automatically created sub-title. Type a title to a maximum of 100 characters.
Graph Type	From the list box, select the type of graph to display on the generated report. Options include: • **Bar** - Displays the data in a bar chart. This is the default graph type. This graph type requires the saved search to be a grouped search. • **Line** - Displays the data in a line chart. • **Pie** - Displays the data in a pie chart. This graph type requires the saved search to be a grouped search. • **Stacked Bar** - Displays the data in a stacked bar chart. • **Stacked Line** - Displays the data in a stacked line chart. • **Table** - Displays the data in table format. The **Table** option is only available for the full page width container only.
Graph	From the list box, select the number of connections to be displayed in the generated report.

Table 9-18 Connections Chart Parameters (continued)

Parameter	Description
Manual Scheduling	The Manual Scheduling pane is displayed only if you selected the **Manually** scheduling option in the Report Wizard. To create a manual schedule: **1** From the **From** list box, type the start date you want for the report, or select the date using the **Calender** icon. The default is the current date. **2** From the list boxes, select the start time you want for the report. Time is available in half-hour increments. The default is 1:00 a.m. **3** From the **To** list box, type the end date you want for the report, or select the date using the **Calender** icon. The default is the current date. **4** From the list boxes, select the end time you want for the report. Time is available in half-hour increments. The default is 1:00 a.m.
Hourly Scheduling	The Hourly Scheduling pane is displayed only if you selected the **Hourly** scheduling option in the Report Wizard. Hourly Scheduling automatically graphs all data from the previous hour.
Daily Scheduling	The Daily Scheduling pane is displayed only if you selected the **Daily** scheduling option in the Report Wizard. Choose one of the following options: • **All data from previous day (24 hours)** • **Data of previous day from** - From the list boxes, select the period of time you want for the generated report. Time is available in half-hour increments. The default is 1:00 a.m.
Weekly Scheduling	The Weekly Scheduling pane is displayed only if you selected the **Weekly** scheduling option in the Report Wizard. Choose one of the following options: • **All data from previous week** • **All Data from previous week from** - From the list boxes, select the period of time you want for the generated report. The default is Sunday.
Monthly Scheduling	The Monthly Scheduling pane is displayed only if you selected the **Monthly** scheduling option in the Report Wizard. Choose one of the following options: • **All data from previous month** • **Data from previous month from the** - From the list boxes, select the period of time you want for the generated report. The default is 1st to 31st.

Table 9-18 Connections Chart Parameters (continued)

Parameter	Description
Graph Content	
Group	From the list box, select a saved search group to display the saved searches belonging to that group in the **Available Saved Searches** list box.
Type Saved Search or Select from List	To refine the **Available Saved Searches** list, type the name of the search you want to locate in the **Type Saved Search or Select from List** field. You can also type a keyword to display a list of searches that include that keyword. For example, type `DMZ` to display a list of all searches that include DMZ in the search name.
Available Saved Searches	Provides a list of available saved searches. By default, all available saved searches are displayed, however, you can filter the list by selecting a group from the **Group** list box or typing the name of a known saved search in the **Type Saved Search or Select from List** field.
Create New Connection Search	Click **Create New Connection Search** to create a new search.

Device Rules

You can use the Device Rules chart to view firewall rules and the event count of firewall rules triggered in your network. Device Rule reports allows you to create a report for the following firewall rules:

- Most active accept device rules
- Most active deny device rules
- Least active accept device rules
- Least active deny device rules
- Unused device rules
- Shadowed device rules

The reports that you generate allow you to understand what rules are accepted, denied, unused, or untriggered across a single device, a specific adapter, or multiple devices. Reports allow QRadar Risk Manager to automate reporting about the status of your device rules and display the reports on the QRadar SIEM Console.

This functionality helps you identify how rules are used on your network devices.

▶ To create a Device Rules Chart container, configure values for the following parameters:

Table 9-19 Device Rules Chart Parameters

Parameter	Description
Container Details - Device Rules	
Limit Rules to Top	From the list box, select the number of rules to be displayed in the generated report. For example, if you limit your report to the top 10 rules, then create a report for most used accept rules across all devices, the report returns 10 results. The results contain a list of the 10 most used accept rules based on the event count across all devices that are visible to QRadar Risk Manager.

Table 9-19 Device Rules Chart Parameters (continued)

Parameter	Description
Type	Select the type of device rules to display in the report. Options include: • **Most Used Accept Rules** - Displays the most used accept rules by event count for a single device or a group of devices. This report lists the rules with highest accepted event counts, in descending order, for the time frame you specified in the report. • **Most Used Deny Rules** - Displays the most used deny rules by event count for a single device or a group of devices. This report lists the rules with the highest deny event counts, in descending order, for the time frame you specified in the report. • **Unused Rules** - Displays any rules for a single device or a group of devices that are unused. Unused rules have zero event counts for the time frame you specified for the report. • **Least Used Accept Rules** - Displays the least used accept rules for a single device or a group of devices. This report lists rules with the lowest accept event counts, in ascending order, for the time frame you specified in the report. • **Least Used Deny Rules** - Displays the least used deny rules for a single device or a group of devices. This report lists rules with the lowest denied event counts, in ascending order, for the time frame you specified in the report. • **Shadowed Rules** - Displays any rules for a single device that can never trigger because the rule is blocked by a proceeding rule. The results display a table of the rule creating the shadow and any the rules that can never trigger on your device because they are shadowed by a proceeding rule on the device. ***Note:*** *Shadowed rule reports can only be run against a single device. These rules have zero event counts for the time frame you specified for the report and are identified with an icon in the Status column.*

Table 9-19 Device Rules Chart Parameters (continued)

Parameter	Description
Date/Time Range	Select the time frame for your report. The options include: • **Current Configuration** - The results of the Device Rules report is based on the rules that exist in the current device configuration. This report displays rules and event counts for the existing device configuration. The current configuration for a device is based on the last time Configuration Source Management backed up your network device. • **Interval** - The results of the Device Rules report is based on the rules that existed during the time frame of the interval. This report displays rules and event counts for the specified interval from the last hour to 30 days. • **Specific Range** - The results of the Device Rules report is based on the rules that existed between the start time and end time of the time range. This report displays rules and event counts for the specified time frame.
Timezone	Select the timezone you want to use as a basis for your report. The default timezone is based on the configuration of your QRadar SIEM Console. When configuring the Timezone parameter for your report, consider the location of the devices associated with the reported data. If the report uses data spanning multiple time zones, the data used for the report is based on the specific time range of the time zone. For example, if your QRadar SIEM Console is configured for Eastern Standard Time (EST) and you schedule a daily report between 1pm and 3pm and set the timezone as Central Standard Time (CST), the results in the report contains information from 2pm and 4pm EST.
Targeted Data Selection	Targeted Data Selection is used to filter the Date/Time Range to more specific value. Using the Targeted Data Selection options, you can create a report to view your device rules over a custom defined period of time, with the option to only include data from the hours and days that you select. For example, you can schedule a report to run from October 1 to October 31 and view your most active, least active or unused rules and their rule counts that occur during your business hours, such as Monday to Friday, 8 AM to 9 PM. ***Note:*** *The filter details only display when you select the* ***Targeted Data Selection*** *check box in the Report Wizard.*

Table 9-19 Device Rules Chart Parameters (continued)

Parameter	Description
Format	Select the format for your device rules report. The options include: • **One aggregate report for specified devices** - This report format aggregates the report data across multiple devices. For example, if you create a report to display the top ten most denied rules, then an aggregate report displays the top ten most denied rules across all of the devices you have selected for the report. This report returns 10 results in total for the report. • **One report per device** - This report format displays the report data for one device. For example, if you create a report to display the top ten most denied rules, then an aggregate report displays the top ten most denied rules for each device you have selected for the report. This report returns the top 10 results for every device selected for the report. If you selected 5 devices, the report returns 50 results. ***Note:*** *Shadowed rule reports are only capable of displaying one report per device.*

Table 9-19 Device Rules Chart Parameters (continued)

Parameter	Description
Devices	Select the devices included in the report. The options include: • **All Devices** - Select this option to include all devices in QRadar Risk Manager in your report. • **Adapter** - From the list box, select an adapter type to include in your report. Only one adapter type can be selected from the list box for a report. • **Specific Devices** - Select this option to only include specific devices in your report. The Device Selection window allows you to select and add devices to your report. To add individual devices to your report: **1** Click **Browse** to display the Device Selection window. **2** Select any devices and click **Add Selected**. To add all devices to your report: **1** Click **Browse** to display the Device Selection window. **2** Click **Add All**. To search for devices to include in your report: **1** Click **Browse** to display the Device Selection window. **2** Click **Search**. **3** Select the search options to filter the full device list by configuration obtained, IP or CIDR address, hostname, type, adapter, vendor, or model. **4** Click **Search**. **5** Select any devices and click **Add Selected**.

Device Unused Objects

A device unused objects report displays object reference groups that are not being used by your network device. This report displays object references, such as a collection of IP address, CIDR address ranges, or host names that are unused by your network device.

▶ To configure a device unused objects container, configure values for the following parameters:

Table 9-20 Device Unused Objects Report Parameters

Parameter	Description
Container Details - Device Unused Objects	
Limit Objects to Top	From the list box, select the number of rules to be displayed in the generated report.

Table 9-20 Device Unused Objects Report Parameters (continued)

Parameter	Description
Devices	Select the devices included in the report. The options include: • **All Devices** - Select this option to include all devices in QRadar Risk Manager in your report. • **Adapter** - From the list box, select an adapter type to include in your report. Only one adapter type can be selected from the list box for a report. • **Specific Devices** - Select this option to only include specific devices in your report. The Device Selection window allows you to select and add devices to your report. To add individual devices to your report: **1** Click **Browse** to display the Device Selection window. **2** Select any devices and click **Add Selected**. To add all devices to your report: **1** Click **Browse** to display the Device Selection window. **2** Click **Add All**. To search for devices to include in your report: **1** Click **Browse** to display the Device Selection window. **2** Click **Search**. **3** Select the search options to filter the full device list by configuration obtained, IP or CIDR address, hostname, type, adapter, vendor, or model. **4** Click **Search**. **5** Select any devices and click **Add Selected**.

Manually generating a report

Reports can be started manually instead of waiting for QRadar Risk Manager to start a report based on a schedule. If you start multiple reports manually, the reports are added to a queue and labeled with their queue position. Manually generating a report does not reset the existing report schedule. For example, if you generate a weekly report for most active firewall denies, then manually generate the report, the weekly report still generates on the schedule you initially configured.

To manually generate a report:

Step 1 Click the **Reports** tab.

Step 2 Select the report that you want to generate.

Step 3 Click **Run Report**.

The report generates. While the report generates, the **Next Run Time** column displays one of the three following messages:

- **Generating** - The report is generating.
- **Queued (*position in the queue*)** - The report is queued for generation. The message indicates the position the report is in the queue. For example, 1 of 3.
- **(*x* hour(s) *x* min(s) *y* sec(s))** - The report is scheduled to run. The message is a count-down timer that specifies when the report will run next.

NOTE

You can select the **Refresh** icon to refresh the view, including the information in the **Next Run Time** column.

After the report generates, you can view the generated report from the **Generated Reports** column.

Editing a report

You can edit a report allows you to adjust a report’s schedule, layout, configuration, title, format, and delivery method. You can either edit existing reports or edit a default report.

To edit an existing report:

Step 1 Click the **Reports** tab.

Step 2 Select the report that you want to edit.

Step 3 From the **Actions** list box, select **Edit**.

NOTE

Double-clicking on a report also opens the Report Wizard, which allows you to edit an existing report.

Step 4 Select the frequency for the new reporting schedule.

- **Manually** - Generates a report one time without a reoccurring schedule.
- **Hourly** - Schedules the report to generate at the end of each hour using the data from the previous hour.
- **Daily** - Schedules the report to generate daily using the data from the previous day. For each chart on a report, you can select the previous 24 hours of the day, or select a specific time frame from the previous day.
- **Weekly** - Schedules the report to generate weekly using the data from the previous week.
- **Monthly** - Schedules the report to generate monthly using the data from the previous month.

Step 5 In the Allow this report to generate manually pane, select one of the following options:

- **Yes** - Enables manual generation of this report.
- **No** - Disables manual generation of this report.

Step 6 Click **Next** to move to the next page of the Report Wizard.

Step 7 Configure the layout of your report:

a From the **Orientation** list box, select the page orientation.

b Select a layout option for your QRadar Risk Manager report.

c Click **Next**.

Step 8 Specify values for the following parameters:

- **Report Title** - Type a report title. The title can be up to 100 characters in length. Do not use special characters.
- **Logo** - From the list box, select a logo. The QRadar logo is the default logo. For more information about branding your report, see the *IBM Security QRadar SIEM Administrator Guide*.

Step 9 Configure the container for your report data:

a Click **Define**.

b Configure the report data for your chart.

For detailed information about configuring your chart container, see **Configuring charts**.

c Click **Save Container Details**.

The Wizard returns to the previous page, enabling you to specify more contents for your report.

d If required, repeat steps **a** to **c** to edit any additional containers.

e Click **Next** to move to the next page of the Report Wizard.

Step 10 Click **Next** to move to the next step of the Report Wizard.

Step 11 Select the check boxes for the report formats. You can select more than one option. The options include:

- Portable Document Format (PDF) - This is the default report format.
- Hypertext Markup Language (HTML)
- Rich Text Format (RTF)
- Extended Markup Language (XML)
- Excel Spreadsheet (XLS)

NOTE

QRadar Risk Manager specific reports, such as Device Rule and Device Unused Object reports only support PDF, HTML, and RTF formats.

Step 12 Click **Next** to move to the next page of the Report Wizard.

Step 13 Select the distribution channels for your report.

Step 14 Click **Next** to go to the final step of the Report Wizard.

Step 15 Configure values for the following parameters:

Table 9-21 Finishing Up Parameters

Parameter	Description
Report Description	Type a description for this report. This description is displayed on the Report Summary page and in the generated report distribution e-mail.
Groups	Select the groups to which you want to assign this report. For more information about groups, see Managing Reports in the *IBM Security QRadar SIEM Administration Guide*.
Would you like to run the report now?	Select this check box if you want to generate the report when the wizard is complete. By default, the check box is selected.

Step 16 Click **Next** to view the report summary.

The Report Summary page is displayed, providing the details for the report. You can select the tabs available on the summary report to preview the report selections.

Step 17 Click **Finish**.

The report is updated with your changes.

Duplicating a report

To duplicate a report:

Step 1 Click the **Reports** tab.

Step 2 Select the report you want to duplicate.

Step 3 From the **Actions** list box, click **Duplicate**.

Step 4 Type a new name, without spaces, for the report.

Sharing a report

You can share reports with other users. When you share a report, you provide a copy of the selected report to another user to edit or schedule. Any updates that the user makes to a shared report does not affect the original version of the report.

NOTE

You must have administrative privileges to share reports. Also, for a new user to view and access reports, an administrative user must share all the necessary reports with the new user.

To share a report:

Step 1 Click the **Reports** tab.

Step 2 Select the reports you want to share.

Step 3 From the **Actions** list box, click **Share**.

Step 4 From the list of users, select the users with whom you want to share this report.

If no users with appropriate access are available, a message is displayed.

Step 5 Click **Share**.

For more information on reports, see the *IBM Security QRadar SIEM Users Guide*.

10 USING SIMULATIONS

Simulations allow you to define, schedule, and run exploit simulations on your network. You can create simulations based on a series of rules that can be combined and configured. The simulation can be scheduled to run on a periodic basis or run manually. After a simulation is complete, you can review the results of the simulation and approve any acceptable or low risk result based on your network policy. This allows you to approve acceptable actions or traffic from your results. After you've tuned your simulation, you can then configure the simulation to monitor the results. Monitoring a simulation enables you to define how you want the system to respond when unapproved results are returned. This response could be an email, the creation of an event, or to send the response to syslog.

Using simulations

From the main toolbar on the Simulations page, you can access the following options:

Table 10-1 Toolbar Options

Option	Description
Group	Allows you to view simulations based on a group. Using the **Group** drop-down list box, select the group for the simulations you want to view.
Groups	Allows you to configure groups for simulations. See **Grouping simulations**.
Monitor	Allows you to monitor a simulation, which ensures that an event is generated when new results occur. See **Monitoring simulations**.

Table 10-1 Toolbar Options (continued)

Option	Description
Actions	The **Actions** drop-down list box allows you to perform the following actions: • **New** - Allows you to create a new simulation. See **Creating a simulation**. • **Edit** - Allows you to view or edit the configuration for an existing simulation. See **Editing a simulation**. • **Duplicate** - Allows you to copy a simulation. See **Duplicating a simulation**. • **Delete** - Allows you to delete a simulation. See **Deleting a simulation**. • **Assign Groups** - Allows you to assign a simulation to a group. See **Assigning an item to a group**. • **Toggle Scheduling** - Toggles active/inactive for the selected simulation. • **Run Simulation** - Allows you to manually run a simulation. See **Manually running a simulation**.
Print	Allows you to print the current display.

Viewing simulations

Simulations created by users and the simulation results can be viewed from the Simulations page.

To view existing simulations:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

The Simulations window provides the following information:

Table 10-2 Simulation Definitions Parameters

Parameter	Description
Simulation Name	The name of the simulation, as defined by the creator of the simulation.
Model	The model type. Simulations can be modeled off of your Current Topology or a Topology model. The options are: • Current Topology • The name of the topology model. For more information on Topology Models, see **Chapter 11** Using topology models.
Groups	The groups the simulation is associated with.
Created By	The user who created the simulation.
Creation Date	The date and time that the simulation was created.

Table 10-2 Simulation Definitions Parameters (continued)

Parameter	Description
Last Modified	The date and time that the simulation was last modified.
Schedule	The frequency the simulation is scheduled to run. The options include: • **Manual** - The simulation runs when manually executed. • **Once** - Specify the date and time the simulation is scheduled to run. • **Daily** - Specify the time of day the simulation is scheduled to run. • **Weekly** - Specify the day of the week and the time the simulation is scheduled to run. • **Monthly** - Specify the day of the month and time the simulation is scheduled to run.
Last Run	The last date and time that the simulation was run.
Next Run	The date and time that the next simulation will be run.
Results	If the simulation has been run, this parameter includes a drop-down list box that contains a list of the dates containing the results of your simulation. If the simulation has not been run, the Results column displays No Results. For more information, see **Viewing simulation results**.

Managing simulations

You can create, view, edit, duplicate and delete simulations. T

Creating a simulation

You can create simulations on the **Risks** tab.

To create a simulation:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

Step 3 From the **Actions** drop-down list box, select **New**.

Step 4 Type a name for the simulation in the **What do you want to name this simulation?** parameter.

This name is displayed in the main Simulation window.

Step 5 Using the **Which model do you want to base this on?** drop-down list box, select the type of data you want to return. The options are:

- **Current Topology** - Allows you to run a simulation against the current topology model.
- **<Topology Model>** - Allows you to view existing topology models. If no topology models have been created, only the Current Topology option is displayed.

Step 6 Choose one of the following options:

- **a** If you want to base the simulation on connection and topology data, select the **Use Connection Data** check box.
- **b** If you want to base the simulation only on topology data, clear the **Use Connection Data** check box.

If your Topology Model does not include any data and you clear the **Use Connection Data** check box, the simulation does not return any results.

Step 7 Using the **Importance Factor** drop-down list box, select the level of importance you want to associate with this simulation.

The Importance Factor is used to calculate the Risk Score. The range is 1 (low importance) to 10 (high importance). The default is 5.

Step 8 From the **Where do you want the simulation to begin?** drop-down list box, select an origin for the simulation.

The chosen value determines the start point of the simulation. For example, the attack originates at a specific network.

The selected simulation parameters are displayed in the **Generate a simulation where** window.

Step 9 Add simulation attack targets to the simulation test.

When the test targets are added to the **Generate a simulation where** window, the configurable parameters are displayed with an underlined.

Table 10-3 Simulation Tests

Test Name	Description	Parameters
Attack originates from one of the following **IP addresses**	Allows you to simulate attacks originating from specific IP addresses or CIDR ranges.	Configure the **IP addresses** parameter to specify the IP address(es) or CIDR ranges to which you want this simulation to originate.
Attack originates from one of the following **networks**	Allows you to simulate attacks originating from assets that are a member of one or more defined network locations.	Configure the **networks** parameter to specify the networks to which you want this simulation to originate.
Attack originates from the Internet	Allows you to simulate attacks originating from the Internet.	None.
Attack originates from one of the following **asset building blocks**	Allows you to simulate attacks originating from one or more groups of defined asset building blocks.	Configure the **asset building blocks** parameter to specify the asset building blocks to which you want this simulation to originate.
Attack originates from one of the following **geographic network locations**	Allows you to simulate attacks originating from one or more hostile geographic network location.	Configure the **geographic network locations** parameter to specify the location to which you want this simulation to originate.

Table 10-3 Simulation Tests (continued)

Test Name	Description	Parameters
Attack originates from somebody that has visited one of the following **geographic network locations** over the last **1** days	Allows you to simulate an asset that may have visited a server hosted in one or more hostile geographic locations within a recent time frame, which may indicate client-side vulnerabilities.	Configure the following parameters: • **geographic network locations -** Specify the location to which you want this simulation to originate. • **1** - Specify the number of days to which you want this simulation to consider. The default is 1.
Attack originates from one of the following **remote network locations**	Allows you to simulate an attack originating from one or more hostile remote network.	Configure the **remote network locations** parameter to specify the remote location to which you want this simulation to originate.
Attack originates from somebody that has visited one of the following **remote network locations** over the last **1** days.	Allows you to simulate an asset that may have visited one or more hostile remote network within a recent time frame, which may indicate client-side vulnerabilities.	Configure the following parameters: • **remote network locations -** Specify the location to which you want this simulation to originate. • **1** - Specify the number of days to which you want this simulation to consider. The default is 1.

Step 10 Using the **Which simulations do you want to include in the attack?** field, select the **+** sign beside the simulation you want to include.

The simulation options are displayed in the **Generate a simulation where** window.

Step 11 From the **Generate a simulation where** window, click any underlined parameters to further configure simulation parameters.

Table 10-4 Simulation Tests

Test Name	Description	Parameters
Attack targets one of the following IP addresses	Allows you to simulate attacks against specific IP addresses or CIDR ranges.	Configure the **IP addresses** parameter to specify the IP address(es) or CIDR ranges to which you want this simulation to apply.
Attack targets one of the following networks	Allows you to simulate attacks targeting networks that are a member of one or more defined network locations.	Configure the **networks** parameter to specify the networks to which you want this simulation to apply.
Attack targets one of the following **asset building blocks**	Allows you to simulate attacks targeting one or more defined asset building blocks.	Configure the **asset building blocks** parameters to specify the asset building blocks to which you want this simulation to apply.
Attack targets a vulnerability on one of the following ports using protocols	Allows you to simulate attacks targeting a vulnerability on one or more defined ports.	Configure the following parameters: • **Ports** - Specify the ports you want this simulation to consider. • **Protocols** - Specify the protocol you want this simulation to consider.

Table 10-4 Simulation Tests (continued)

<table>
<tr><th>Test Name</th><th>Description</th><th>Parameters</th></tr>
<tr><td>Attack targets a vulnerability on one of the following <b>operating systems</b></td><td>Allows you to simulate attacks targeting a vulnerability on one or more defined operating systems.</td><td>Configure the operating systems parameter to identify <b>operating systems</b> you want this simulation to consider. Only known operating systems for assets in your deployment appear in the list.</td></tr>
<tr><td colspan="3"><i><b>Note:</b> The simulation test for <b>attack targets a vulnerability on one of the following operating systems</b> has been hidden in the Simulation Editor. If you currently use this simulation the option is still visible, but has been replaced by a simulation test that searches assets for vulnerabilities by text entries or regular expressions.</i></td></tr>
<tr><td><b>Attack targets assets susceptible to one of the following vulnerabilities</b></td><td>Allows you to simulate attacks targeting assets that are susceptible to one or more defined vulnerabilities.</td><td>Configure the <b>vulnerabilities</b> parameter to identify the vulnerabilities that want this test to apply. You can search for vulnerabilities using OSVDB ID, Bugtraq ID, CVE ID, or title.</td></tr>
<tr><td>Attack targets assets susceptible to vulnerabilities with one of the following <b>classifications</b></td><td>Allows you to simulate attacks targeting an asset that is susceptible to vulnerabilities for one or more defined classifications.</td><td>Configure the <b>classifications</b> parameter to identify the vulnerability classifications. For example, a vulnerability classification may be Input Manipulation or Denial of Service.</td></tr>
<tr><td><b>Attack targets assets susceptible to vulnerabilities with CVSS score greater than 5</b></td><td>A Common Vulnerability Scoring System (CVSS) value is an industry standard for assessing the severity of vulnerabilities. This simulation filters assets in your network that include the configured CVSS value.
Allows you to simulate attacks targeting an asset that is susceptible to vulnerabilities with a CVSS score greater than 5.</td><td>Configure the following parameters:
• <b>greater than</b> - Specify whether the Common Vulnerability Scoring System (CVSS) score to be greater than, greater than or equal to, less than, less than or equal to, equal to, or not equal to the configured value. The default is greater than.
• <b>5</b> - Specify the CVSS score you want this test to consider. The default is 5.</td></tr>
<tr><td>Attack targets assets susceptible to vulnerabilities from one of the following <b>vendors</b></td><td>Allows you to simulate attacks targeting an asset that is susceptible to vulnerabilities from the specified vendors.</td><td>Configure the <b>vendor</b> parameter to identify vulnerability vendors you want this simulation to consider.</td></tr>
<tr><td colspan="3"><i><b>Note:</b> The simulation test for </i><b>attack targets assets susceptible to vulnerabilities from one of the following vendors</b><i> has been hidden in the Simulation Editor. If you currently use this simulation test the option is still visible, but the functionality has been replaced by a simulation test that searches assets for vulnerabilities by text entries or regular expressions.</i></td></tr>
<tr><td>Attack targets assets susceptible to vulnerabilities from one of the following <b>products</b></td><td>Allows you to simulate attacks targeting an asset that is susceptible to vulnerabilities from the specified products.</td><td>Configure the <b>products</b> parameter to identify vulnerability products you want this simulation to consider.</td></tr>
<tr><td colspan="3"><i><b>Note:</b> The simulation test for </i><b>attack targets assets susceptible to vulnerabilities from one of the following products</b><i> has been hidden in the Simulation Editor. If you currently use this simulation test the option is still visible, but the functionality has been replaced by a simulation test that searches assets for vulnerabilities by text entries or regular expressions.</i></td></tr>
</table>

Table 10-4 Simulation Tests (continued)

Test Name	Description	Parameters
Attack targets assets susceptible to vulnerabilities disclosed after this date	Allows you to simulate attacks targeting an asset that is susceptible to vulnerabilities discovered before, after, or on the configured date.	Configure the following parameters: • **before | after | on** - Specify whether you want the simulation to consider the disclosed vulnerabilities to be after, before, or on the configured date on assets. The default is before. • **this date** - Specify the date that you want this simulation to consider.
Attack targets assets susceptible to vulnerabilities where the name, vendor, version or service contains one of the following **text entries**	Allows you to simulate attacks targeting an asset that is susceptible to vulnerabilities matching the asset name, vendor, version or service based one or more text entry.	Configure the **text entries** parameter to identify the asset name, vendor, version or service you want this simulation to consider.
Attack targets assets susceptible to vulnerabilities where the name, vendor, version or service contains one of the following **regular expressions**	Allows you to simulate attacks targeting an asset that is susceptible to vulnerabilities matching the asset name, vendor, version or service based one or more regular expression.	Configure the **regular expressions** parameter to identify the asset name, vendor, version or service you want this simulation to consider.

Step 12 In the **Run this simulation for** drop-down list box, select the number of steps you want to run this simulation (1 to 5) and the schedule for running the simulation. The options are:

- **Manual** - The simulation runs when manually executed.
- **Once** - Specify the date and time the simulation is scheduled to run.
- **Daily** - Specify the time of day the simulation is scheduled to run.
- **Weekly** - Specify the day of the week and the time the simulation is scheduled to run.
- **Monthly** - Specify the day of the month and time the simulation is scheduled to run.

Step 13 In the groups area, select a checkbox for any group you want to assign this simulation. For more information on grouping simulations, see **Grouping simulations**.

Step 14 Click **Save Simulation**.

Editing a simulation

You can edit simulations on the **Risks** tab.

To edit a simulation:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

Step 3 Select the simulation definition you want to edit.

Step 4 From the **Actions** drop-down list box, select **Edit**.

Step 5 Update parameters, as necessary.

For more information on the Simulation parameters, see **Creating a simulation**.

Step 6 Click **Save Simulation**.

Duplicating a simulation

You can duplicate simulations **Risks** tab.

To duplicate a simulation:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

Step 3 Select the simulation you want to duplicate.

Step 4 From the **Actions** drop-down list box, select **Duplicate**.

Step 5 Type the name for the simulation.

Step 6 Click **OK**.

Deleting a simulation

You can delete simulations **Risks** tab.

To delete a simulation:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

Step 3 Select the simulation you want to delete.

Step 4 From the **Actions** drop-down list box, select **Delete**.

Step 5 Click **OK**.

Manually running a simulation

Using the Simulation Editor, you can schedule a simulation to run. You can also manually run a simulation using the below process. For more information on scheduling a simulation, see **Creating a simulation**.

To manually run a simulation:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

Step 3 From the **Actions** drop-down list box, select **Run Simulation**.

Step 4 Click **OK**.

The simulation process can take an extended period of time. While the simulation is running, the Next Run column indicates the percentage complete. When complete, the Results column displays the simulation date and time. To view results, see **Viewing simulation results**.

If you run a simulation and then perform changes that affect the tests associated with the simulation, these changes may take up to an hour to appear.

Managing simulation results

After a simulation runs, the Results column displays a drop-down list box containing a list of the dates when the simulation was generated. All simulation results are retained for 30 days.

Viewing simulation results

To view simulation results:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

Step 3 In the Results column, select the date and time of the simulation you want to view using the drop-down list box.

NOTE

The drop-down list box is only displayed in the Results column if the simulation has been run. If no simulation runs, this field indicates No Results.

Step 4 Click **View Result**.

Simulation results appear providing information on each step of the simulation.

For example, the first step provides a list of the directly connected assets affected by the simulation. The second step lists assets in your network that can communicate to first level assets in your simulation.

The Simulation Results window provides the following information:

Table 10-5 Simulation Results Parameters

Parameter	Description
Simulation Definition	The description of the simulation.
Using Model	The name of the model against which the simulation was run.
Simulation Result	The date on which the simulation was run.
Step Results	The number of steps for the result including the step that is currently being displayed.
Assets Compromised	The number of total assets compromised in this step and across all simulation steps. If the Topology Model includes data from an IP range of /32 defined as reachable, then QRadar Risk Manager does not validate those assets against the database. Therefore, those assets are not considered in the Asset Compromised total. QRadar Risk Manager only validates assets in broader IP ranges, such as /24 to determine which assets exist.

Table 10-5 Simulation Results Parameters (continued)

Parameter	Description
Risk Score	Risk score is a calculated value based on the number of results, steps, the number of compromised assets, and the importance factor assigned to the simulation. This value indicates the severity level associated with the simulation for the displayed step.

Step 5 View the progression information to view the progression of the simulation:

a Move your mouse pointer over a connection to determine the list of assets affected by this simulation.

The top 10 assets display when you move your mouse over the connection. The table below the graph displays the full list of assets.

b Move your mouse pointer over the connection to highlight the path through the network, as defined by the subnet.

Step 6 View the Results for this Step table to determine the assets affected:

The Results for this step table provides the following information:

Table 10-6 Results Parameters

Parameter	Description
Approve	Allows you to approve simulation results. See **Approving simulation results**.
Parent	The originating IP address for the displayed step of the simulation.
IP	The IP address of the affected asset.
Network	The network of the target IP addresses, as defined in the network hierarchy.
Asset Name	The name of the affected asset, as defined by the asset profile.
Asset Weight	The weight of the affected asset, as defined in the asset profile.

Step 7 To view the next step of the simulation results, click **Next Step**.

Approving simulation results

Simulation results allow you to approve network traffic that are deemed low risk or normal communication on the asset. Approving results allows you to filter the result list so future simulations ignore normal or approved communications.

To approve simulation results, perform the following steps:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

Step 3 In the Results column, select the date and time of the simulation you want to view using the drop-down list box.

The drop-down list box only displays in the Results column if the simulation runs. If no simulation has run, this field indicates No Results.

Step 4 Click **View Result**.

Step 5 In the Results for this step table, use one of the following methods to approve assets:

a Select a check box for each asset you want to approve, then click **Approve Selected**.

b Click **Approve All**.

Step 6 Click **View Approved** to view all approved assets.

Revoking simulation approval

Revoking approvals allows you to take an approved connection or communication off of the approved list. After an approved simulation result is removed, future simulations display non-approved communications in the simulation results.

To revoke approval for simulation results, perform the following steps:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

Step 3 In the Results column, select the date and time of the simulation you want to view using the drop-down list box.

The drop-down list box only displayed in the Results column if the simulation has been run. If no simulation has been run, this field indicates No Results.

Step 4 Click **View Result**.

Step 5 Click **View Approved** to view all approved assets.

Step 6 Choose one of the following options:

a Select the check box for each result for which you want to revoke the approval, and click **Revoke Selected**.

b To revoke all approvals for results, click **Revoke All**.

Monitoring simulations

If you want to generate an event when new simulation results occur, you can configure the simulation to be monitored. When you configure a simulation to be monitored, QRadar Risk Manager analyzes the simulation to determine if the results of the simulation have changed. You can configure a maximum of 10 simulations in monitor mode.

NOTE

A simulation in monitor mode defaults to a time range of 1 hour. This value overrides the configured time value when the simulation was created. For more information on creating a simulation, see **Creating a simulation**.

To configure a simulation to be monitored:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

Step 3 Select the Simulation you want to monitor.

Step 4 Click **Monitor**.

Step 5 Type values for the parameters:

Table 10-7 Monitor Simulation Results Parameters

Parameter	Description
Event Name	Type the name of the event you want to display in the **Log Activity** and **Offenses** tab.
Event Description	Type a description for the event. The description is displayed in the Annotations of the event details.
Event Details	Select from the following options: • **High-Level Category** - Using this drop-down list box, select the high-level event category you want this simulation to use when processing events. By default, the category is Risk. • **Low-Level Category** - Using this drop-down list box, select the low-level event category you want this simulation to use when processing events. By default, the category is Compliance Violation. • **Ensure the dispatched event is part of an offense (Correlate By:)** - Select the check box if you want, as a result of this monitored simulation, the events forwarded to the Magistrate component. If no offense has been generated in the **Offenses** tab, a new offense is created. If an offense exists, this event is added to the existing offense. If you select the check box, the following option becomes available: • **Question/Simulation** - All events from a question are associated with a single offense. • **Asset** - A unique offense is created (or updated) for each unique asset. ***Note:*** *For more information on event categories, see the QRadar Users Guide.*

Table 10-7 Monitor Simulation Results Parameters (continued)

Parameter	Description
Additional Actions	Select the check box(es) to indicate the additional methods to be taken on an event. The options include: • **Email** - Select this check box and specify the email address(es) to send notifications if the event is generated. Separate multiple email addresses using a comma. • **Send to Syslog** - Select this check box if you want to log the event. By default, the check box is clear. For example, the syslog output may resemble: `Sep 28 12:39:01 localhost.localdomain ECS: Rule 'Name of Rule' Fired: 172.16.60.219:12642 -> 172.16.210.126:66666, Event Name: SCAN SYN FIN, QID: 1000398, Category: 1011, Notes: Event description` • **Notify** - Select this check box if you want events that generate as a result of this monitored question to appear in the System Notifications item in the Dashboard. For more information on the **Log Activity** tab and the QRadar SIEM Dashboard, see the *IBM Security QRadar SIEM Users Guide.*
Enable Monitor	Select this check box if you want to monitor the simulation.

Step 6 Click **Save Monitor**.

Grouping simulations

You can group and view your simulations based on your chosen criteria. Categorizing your simulations allows you to efficiently view and track your simulation. For example, you can view all simulations related to compliance.

As you create new simulations, you can assign the simulations to an existing group. For information on assigning a group, see **Managing simulations**.

Viewing groups

To view simulations using groups:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

The Simulations window is displayed.

Step 3 Using the **Group** drop-down list box, select the group you want to view.

The list of items assigned to that group appear.

Creating a group

To create a group:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

Step 3 Click **Groups**.

Step 4 From the menu tree, select the group under which you want to create a new group.

NOTE

After you create a group, you can drag and drop groups in the menu tree to change the organization.

Step 5 Click **New**.

Step 6 Type values for the parameters:

- **Name** - Type the name you want to assign to the new group. The name can be up to 255 characters in length.
- **Description** - Type a description you want to assign to this group. The description can be up to 255 characters in length.

Step 7 Click **OK**.

Step 8 If you want to change the location of the new group, click the new group and drag the folder to the preferred location in your menu tree.

Step 9 Close the Groups window.

Editing a group

To edit a group:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

Step 3 Click **Groups**.

Step 4 From the menu tree, select the group you want to edit.

Step 5 Click **Edit**.

Step 6 Update values for the parameters, as necessary:

- **Name** - Type the name you want to assign to the new group. The name can be up to 255 characters in length.
- **Description** - Type a description you want to assign to this group. The description can be up to 255 characters in length.

Step 7 Click **OK**.

Step 8 If you want to change the location of the group, select a group and drag the folder to the preferred location in your menu tree.

Step 9 Close the Groups window.

Copying an item to another group

Using the groups functionality, you can copy a simulation to one or many groups. To copy a simulation:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

Step 3 Click **Groups**.

Step 4 From the menu tree, select the question you want to copy to another group.

Step 5 Click **Copy**.

Step 6 Select the check box for the group to which you want to copy the simulation.

Step 7 Click **Copy**.

Step 8 Close the Groups window.

Deleting an item from a group

To delete a question from a group:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

Step 3 Click **Groups**.

Step 4 From the menu tree, select the top level group.

Step 5 From the list of groups, select the item or group you want to delete.

Step 6 Click **Remove**.

Step 7 Click **OK**.

Step 8 Close the Groups window.

Assigning an item to a group

To assign a simulation to a group:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulation > Simulations**.

The Simulations window is displayed.

Step 3 Select the simulation you want to assign to a group.

Step 4 Using the **Actions** drop-down list box, select **Assign Groups**.

The Choose Group window is displayed.

Step 5 Select the group to which you want the question assigned.

Step 6 Click **Assign Groups**.

11 USING TOPOLOGY MODELS

The Topology Model from the Simulation navigation menu enables you to define virtual network models based on your existing network. You can create a network model based on a series of modifications that can be combined and configured. This allows you to determine the effect of configuration changes on your network using the Simulation functionality. For more information about simulations, see **Using simulations**.

Viewing topology models

To view topology models:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulations > Topology Models**.

Topology Models provides the following information:

Table 11-1 Model Definitions Parameters

Parameter	Description
Model Name	The name of the topology model, as defined by the user when created.
Group(s)	The groups to which this topology is associated.
Created By	The user who created the model definition.
Created On	The date and time that the model definition was created.
Last Modified	The number of days since the model definition was created.

Creating a topology model

To create a topology model:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulations > Topology Models**.

The Topology Models window is displayed.

Step 3 From the **Actions** drop-down menu, select **New**.

The Model Editor window is displayed.

Step 4 In the **What do you want to name is model?** field, type a name for the model definition.

Step 5 In the **Which modifications do you want to apply to your model?** pane, select the modifications that you want to apply to the Topology to create your model.

The selected tests are displayed in the Configure model as follows pane.

Step 6 Configure the tests added to the **Configure model as follows** pane.

When the test is displayed in the pane, the configurable parameters appear underlined. Click each parameter to further configure this modification for your model.

Table 11-2 Topology Tests

Test Name	Parameters
A rule is added to the selected devices that allows connections from source CIDRs to destination CIDRs on protocols, ports	Configure the following parameters: • **devices** - Specify the devices to which you want to add to this rule. In the Customize Parameter window, select the **All** check box to include all devices or you can search devices using one of the following search criteria: **IP/CIDR** - Select the IP/CIDR option and specify the IP address or CIDR to which you want to add to this rule. **Hostname** - Select the Hostname option and specify the hostname you want to filter. To search for multiple hostnames, use a wildcard character (*) at the beginning or end of the string. **Adapter** - Select the Adapter option and use the drop-down list box to filter the device list by adapter. **Vendor** - Select the Vendor option and use the drop-down list box to filter the device list by vendor. You can also specify a model for the vendor. To search for multiple models, use a wildcard character (*) at the beginning or end of the string. • **allows | denies** - Select the condition (accept or denied) for connections that you want this test to apply. • **CIDRs** - Select any source IP addresses or CIDR ranges to which you want to add to this rule. • **CIDRs** - Select any destination IP addresses or CIDR ranges to which you want to add to this rule. • **protocols** - Specify the protocols to which you want to add to this rule. To include all protocols, select the **All** check box. • **ports** - Specify the ports to which you want to add to this rule. To include all ports, select the **All** check box.

Table 11-2 Topology Tests (continued)

Test Name	Parameters
A rule is added to the selected IPS devices that allows connections from source CIDRs to destination CIDRs with vulnerabilities	Configure the following parameters: • **IPS devices** - Specify the IPS devices that you want this topology model to include. To include all IPS devices, select the **All** check box. • **allows | denies** - Specify the condition (accept or denied) for connections that you want this test to apply. • **CIDRs** - Specify any source IP addresses or CIDR ranges you want this topology model to include. • **CIDRs** - Specify any destination IP addresses or CIDR ranges you want this topology model to include. • **vulnerabilities** - Specify the vulnerabilities that you want to apply to the topology model. You can search for vulnerabilities using the Bugtraq ID, OSVDB ID, CVE ID, or title.
The following assets allow connections to the selected ports	Configure the following parameters: • **assets** - Specify the assets that you want this topology model to include. • **allow | deny** - Specify the condition (allow or deny) for connections that you want this topology model to apply. The default is allow. • **ports** - Specify the ports that you want this topology model to include. To include all ports, select the **All** check box.
Assets in the following **asset building blocks allow** connections to **ports**	Configure the following parameters: • **assets building blocks** - Specify the building blocks that you want this topology model to include. • **allow | deny** - Specify the condition (allow or deny) that you want this topology model to apply. The default is allow. • **ports** - Specify the ports that you want this topology model to include. To include all ports, select the **All** check box.

Step 7 In the groups area, select the check box to assign groups to this question. For more information on grouping questions, see Grouping topology models.

Step 8 Click **Save Model**.

Editing a topology model

To edit a topology model:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulations > Topology Models**.

The Topology Models window is displayed.

Step 3 Select the model definition you want to edit.

Step 4 From the **Actions** drop-down menu, select **Edit**.

The Model Editor window is displayed.

Step 5 Update parameters, as necessary.

For more information on the Model Editor parameters, see Creating a topology model.

Step 6 Click **Save Model**.

Duplicating a topology model

To duplicate a topology model:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulations > Topology Models**.

The Topology Models window is displayed.

Step 3 Select the model definition you want to duplicate.

Step 4 From the **Actions** drop-down menu, select **Duplicate**.

The name window is displayed.

Step 5 Type a name that you want to assign to the copied topology model.

Step 6 Click **OK**.

Step 7 Edit the model, as desired.

For information on editing a question, see Editing a topology model.

Deleting a topology model

To delete a topology model:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulations > Topology Models**.

The Topology Models window is displayed.

Step 3 Select the model definition you want to delete.

Step 4 From the **Actions** drop-down menu, select **Delete**.

A confirmation window is displayed.

Step 5 Click **OK**.

Grouping topology models

You can group and view your topology models based on your chosen criteria. Categorizing your topology model allows you to efficiently view and track your models. For example, you can view all topology models related to compliance.

As you create new topology models, you can assign the topology models to an existing group. For information on assigning a group, see Creating a topology model.

Viewing groups

To view topology models using groups:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulations > Topology Models**.

The Topology Models window is displayed.

Step 3 Using the **Group** drop-down list box, select the group you want to view.

The list of Topology Models assigned to that group displays.

Creating a group

To create a group:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulations > Topology Models**.

The Topology Model window is displayed.

Step 3 Click **Groups**.

The Group window is displayed.

Step 4 From the menu tree, select the group under which you want to create a new group.

After you create the group, you can drag and drop groups in the menu tree items to change the organization.

Step 5 Click **New**.

The Group Properties window is displayed.

Step 6 Type values for the parameters:

- **Name** - Specify the name you want to assign to the new group. The name can be up to 255 characters in length.
- **Description** - Specify a description you want to assign to this group. The description can be up to 255 characters in length.

Step 7 Click **OK**.

Step 8 If you want to change the location of the new group, click the new group and drag the folder to location in your menu tree.

Step 9 Close the Groups window.

Editing a group

To edit a group:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulations > Topology Models**.

The Topology Models window is displayed.

Step 3 Click **Groups**.

The Group window is displayed.

Step 4 From the menu tree, select the group you want to edit.

Step 5 Click **Edit**.

The Group Properties window is displayed.

Step 6 Update values for the parameters, as necessary:

- **Name** - Specify the name you want to assign to the new group. The name can be up to 255 characters in length.
- **Description** - Specify a description you want to assign to this group. The description can be up to 255 characters in length.

Step 7 Click **OK**.

Step 8 If you want to change the location of the group, click the new group and drag the folder to location in your menu tree.

Step 9 Close the Groups window.

Copying an item to another group

Using the groups functionality, you can copy a topology model to one or many groups.

To copy a topology model:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulations > Topology Models**.

The Topology Models window is displayed.

Step 3 Click **Groups**.

The Group window is displayed.

Step 4 From the menu tree, select the question you want to copy to another group.

Step 5 Click **Copy**.

The Choose Group window is displayed.

Step 6 Select the check box for the group to which you want to copy the simulation.

Step 7 Click **Copy**.

Step 8 Close the Groups window.

Deleting an item from a group

To delete a topology model from a group:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulations > Topology Models**.

Step 3 Click **Groups**.

Step 4 From the menu tree, select the top level group.

Step 5 From the list of groups, select the group you want to delete.

Step 6 Click **Remove**.

Step 7 Click **OK**.

Step 8 If you want to change the location of the new group, click the new group and drag the folder to location in your menu tree.

Step 9 Close the Groups window.

Assign a topology to a group

To assign a topology model to a group:

Step 1 Click the **Risks** tab.

Step 2 On the navigation menu, select **Simulations > Topology Models**.

Step 3 Select the topology model you want to assign to a group.

Step 4 From the **Actions** drop-down menu, select **Assign Group**.

Step 5 Select the group to which you want the question assigned.

Step 6 Click **Assign Groups**.

A POLICY MONITOR QUESTIONS

The Policy Monitor allows users to define test questions to identify risk in network devices or rules on network devices. This appendix includes the detailed question parameters for Policy Monitor tests.

This section provides information on the following:

- **Asset Questions** - Identify assets on the network that violate a defined policy or which introduced risk into the environment. For a detailed list of asset questions, see **Asset test questions**.
- **Devices/Rules** - Identify rules in a device that violate a defined policy that can introduced risk into the environment. For a detailed list of device rule questions, see **Device/Rules tests**.

Asset test questions

Asset test questions are categorized by communication type: actual or possible.

- **Actual Communication** - Includes any assets on which communications have been detected using connections.
  - **Contributing Test** - A contributing test question is the base test question that defines what type actual communication you are trying to test. For more information, see **Asset tests - Actual communication (contributing)**.
  - **Restrictive Test** - A restrictive test question restricts the test results from the contributing test to further filter the actual communication for specific violations. For more information, see **Asset tests - Actual communication (restrictive)**.
- **Possible Communication** - Possible communication questions allow you to review if specific communications are possible on assets, regardless of whether or not a communication has been detected.
  - **Contributing Test** - A contributing test question is the base test question that defines what type of possible communication you are attempting to test. For more information, see **Asset tests - Possible communication (contributing)**.
  - **Restrictive Test** - A restrictive test question restricts the test results from the contributing test to further filter the possible communication for specific violations. For more information, see **Asset tests - Possible**

communication (restrictive).The actual communication tests for assets include the following restrictive question parameters:

Asset tests - Actual communication (contributing)

The actual communication tests for assets include the following contributing question parameters:

Table A-1 Actual Communication - Contributing Tests

Test Name	Description	Parameters
have accepted communication **to any destination**	Detects assets that have communications to any or from any configured network. This test allows you to define a start or end point to your question. For example, to identify the assets that have accepted communication from the DMZ, configure the test as follows: have accepted communication from any source <networks> You can use this test to detect out-of-policy communications.	Configure the following parameters: • **accepted | rejected** - Specify if you want this test to consider accepted or rejected communications. The default is accepted. • **to any destination | from any source** - Specify if you want this test to consider the source or destination network. The default is to destination.
have accepted communication **to destination networks**	Detects assets that have communications to or from the configured network. This test allows you to define a start or end point to your question. For example, to identify the assets that communicated to the DMZ, configure the test as follows: have accepted communication from source <networks> You can use this test to detect out-of-policy communications.	Configure the following parameters: • **have | have not** - Specify the condition that you want this test to apply. The options are have or have not. The default is have. When you apply the have not condition to this test, the not condition applies to the networks parameter. For example, if you configure this test as **have not accepted communication to destination networks**, the test detects assets that have accepted communications to networks other than the configured network. • **accepted | rejected** - Specify if you want this test to consider accepted or rejected communications. The default is accepted. • **to destination | from source** - Specify if you want this test to consider the source or destination network. The default is to destination. • **networks** - Specify the area of the networks to which you want this test to apply.

Table A-1 Actual Communication - Contributing Tests (continued)

Test Name	Description	Parameters
have accepted communication **to destination IP addresses**	Detects assets that have communications to or from the configured IP address. This test allows you to specify IP or CIDR address. For example, if you want to identify all assets that communicated to a specific compliance server, configure the test as follows: have accepted communications to destination <compliance server IP address>	Configure the following parameters: • **have | have not** - Specify the condition that you want this test to apply. The options are have or have not. The default is have. When you apply the have not condition to this test, the not condition applies to the IP addresses parameter. For example, if you configure this test as **have not accepted communication to destination IP addresses**, the test detects assets that have accepted communications to IP addresses other than the configured IP addresses. • **accepted | rejected** - Specify if you want this test to consider accepted or rejected communications. The default is accepted. • **to destination | from source** - Specify if you want this test to consider the source or destination IP addresses. The default is to destination. • **IP addresses** - Specify the list of IP address(es) to which you want this test to apply.
have accepted communication **to destination asset building blocks**	Detects assets that have communications to or from the configured asset building blocks. This test allows you to re-use building blocks defined in the QRadar Rules Wizard in your query. For more information about rules, assets, and building blocks, see the *QRadar Administration Guide*.	Configure the following parameters: • **have | have not** - Specify the condition that you want this test to apply. The options are have or have not. The default is have. When you apply the have not condition to this test, the not condition applies to the asset building blocks parameter. For example, if you configure this test as **have not accepted communication to destination asset building blocks**, the test detects assets that have accepted communications to asset building blocks other than the configured asset building blocks. • **accepted | rejected** - Specify if you want this test to consider accepted or rejected communications. The default is accepted. • **to destination | from source** - Specify if you want this test to consider the source or destination asset building blocks. The default is to destination. • **asset building blocks** - Specify the asset building blocks to which you want this test to apply.

Table A-1 Actual Communication - Contributing Tests (continued)

Test Name	Description	Parameters
have accepted communication **to destination remote network locations**	Detects assets that have communicated with networks defined as a remote network. For example, this test can identify hosts that have communicated to botnets or other suspicious Internet address space.	Configure the following parameters: • **have | have not** - Specify the condition that you want this test to apply. The options are have or have not. The default is have. When you apply the have not condition to this test, the not condition applies to the remote network locations parameter. For example, if you configure this test as **have not accepted communication to destination remote network locations**, the test detects assets that have accepted communications to remote network locations other than the configured remote network locations. • **accepted | rejected** - Specify if you want this test to consider accepted or rejected communications. The default is accepted. • **to destination | from source** - Specify if you want this test to consider the source or destination network locations. The default is to destination. • **remote network locations** - Specify the remote networks to which you want this test to apply.
have accepted communication **to destination geographic network locations**	Detects assets that have communicated with networks defined as geographic networks. For example, this test can detect assets that have attempted communications with countries in which you do not have business operations.	Configure the following parameters: • **have | have not** - Specify the condition that you want this test to apply. The options are have or have not. The default is have. When you apply the have not condition to this test, the not condition applies to the geographic network locations parameter. For example, if you configure this test as **have not accepted communication to destination geographic network locations**, the test detects assets that have accepted communications to geographic network locations other than the configured geographic network locations. • **accepted | rejected** - Specify if you want this test to consider accepted or rejected communications. The default is accepted. • **to destination | from source** - Specify if you want this test to consider the source or destination network locations. The default is to destination. • **geographic network locations** - Specify the geographic networks to which you want this test to apply.

Table A-1 Actual Communication - Contributing Tests (continued)

Test Name	Description	Parameters
have accepted communication **to** the Internet	Detects source or destination communications to or from the Internet.	Configure the following parameters: • **have | have not** - Specify the condition that you want this test to apply. The options are have or have not. The default is have. When you apply the have not condition to this test, the not condition applies to the Internet portion of the test. For example, if you configure this test as **have not accepted communication to the Internet**, the test detects assets that have accepted communications from or to areas other than the Internet. • **accepted | rejected** - Specify if you want this test to consider accepted or rejected communications. The default is accepted. • **to | from -** Specify if you want this test to consider communication traffic to or from the Internet. The default is to.
are susceptible to one of the following **vulnerabilities**	Detects specific vulnerabilities. If you want to detect vulnerabilities of a particular type, use the “are susceptible to vulnerabilities with one of the following classifications” test.	Configure the following parameters: • **are | are not** - Specify the condition (are or are not) that you want this test to apply. The default is are. • **vulnerabilities** - Specify the vulnerabilities to which you want this test to apply. You can search for vulnerabilities using the OSVDB ID, CVE ID, Bugtraq ID, or title. For more information about OSVDB, see http://osvdb.org.
are susceptible to vulnerabilities with one of the following **classifications**	A vulnerability can be associated with one or more vulnerability classifications. This test filters all assets that include vulnerabilities with the specified classifications.	Configure the **classifications** parameter to identify the vulnerability classifications that you want this test to apply. For example, a vulnerability classification may be Input Manipulation or Denial of Service.

Table A-1 Actual Communication - Contributing Tests (continued)

Test Name	Description	Parameters
are susceptible to vulnerabilities with CVSS score **greater than 5**	A Common Vulnerability Scoring System (CVSS) value is an industry standard for assessing the severity of vulnerabilities. CVSS is composed of three metric groups: Base, Temporal, and Environmental. These metrics allow CVSS to define and communicate the fundamental characteristics of a vulnerability. This test filters assets in your network that include vulnerabilities with a CVSS score, as specified.	Configure the following parameters: • **greater than | less than | equal to** - Specify whether the Common Vulnerability Scoring System (CVSS) score should be greater than, less than, or equal to the configured value. The default is greater than. • **5** - Specify the CVSS score you want this test to consider. The default is 5.
are susceptible to vulnerabilities from the following **vendors**		Configure the **vendors** parameter to identify possible vulnerabilities that have been introduced on assets from specific vendors.
Note: *The contributing test for assets that are susceptible to vulnerabilities from the following vendors has been hidden in the Policy Monitor. If you currently use this contributing test it is still visible in the test, but has been replaced by a contributing test that searches assets for vulnerabilities by text entries or regular expressions.*		
are susceptible to vulnerabilities with the following **services**		Configure the **services** parameter to identify possible vulnerabilities that have been introduced on assets from specific services.
Note: *The contributing test for assets that are susceptible to vulnerabilities from the following services has been hidden in the Policy Monitor. If you currently use this contributing test it is still visible in the test, but has been replaced by a contributing test that searches assets for vulnerabilities by text entries or regular expressions.*		
are susceptible to vulnerabilities disclosed **after specified date**	Detects assets in your network with a vulnerability that is disclosed after, before, or on the configured date.	Configure the following parameters: • **after | on | before** - Specify whether you want the test to consider the disclosed vulnerabilities to be after, before, or on the configured date. The default is after. • **specified date** - Specify the date that you want this test to consider.
are susceptible to vulnerabilities on one of the following **ports**	Detects assets in your network with a vulnerability that is associated with the configured ports.	Configure the **ports** parameter to identify ports you want this test to consider.
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following **text entries**	Detects assets in your network with a vulnerability that matches the asset name, vendor, version or service based one or more text entry.	Configure the **text entries** parameter to identify the asset name, vendor, version or service you want this test to consider.

Table A-1 Actual Communication - Contributing Tests (continued)

Test Name	Description	Parameters
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following **regular expressions**	Detects assets in your network with a vulnerability that matches the asset name, vendor, version or service based one or more regular expression.	Configure the **regular expressions** parameter to identify the asset name, vendor, version or service you want this test to consider.

Asset tests - Actual communication (restrictive)

The actual communication tests for assets include the following restrictive question parameters:

Table A-2 Actual Communication - Restrictive Tests

Test Name	Description	Parameters
include only the following **protocols**	Filters assets from the contributing test that include or exclude the specified protocols. This test is only selectable when a contributing asset test is added to this question.	Configure the following parameters: • **include only | exclude** - Specify the condition (include only or exclude) that you want this test to apply. When you apply the exclude condition to this test, the not condition applies to the protocols parameter. For example, if you configure this test as **exclude the following protocols**, the test excludes all returned asset results that exclude the specified protocols other than the configured protocols. • **protocols** - Specify the list of protocols to which you want this test to apply.
include only the following **inbound ports**	Filters assets from the contributing test that include only or exclude the specified ports. This test is only selectable when a contributing asset test is added to this question.	Configure the following parameters: • **include only | exclude** - Specify the condition (include only or exclude) that you want this test to apply. When you apply the exclude condition to this test, the not condition applies to the ports parameter. For example, if you configure this test as **exclude the following inbound ports**, the test excludes all returned asset results that exclude the specified ports coming to the asset other than the configured port. • **inbound | outbound** - Specify if you want this test to consider inbound or outbound communications. The default is inbound. • **ports** - Specify the ports to which you want this test to apply.

Table A-2 Actual Communication - Restrictive Tests (continued)

Test Name	Description	Parameters
	Note: *Inbound refers to a test that is filtering the connections for which the asset in question is a destination. Outbound refers to a test that is filtering connections for which the asset in question is a source.* ***Note:*** *We recommend when using restrictive tests that the direction of the restrictive test follows the same direction as the contributing test. Restrictive tests using a mix of inbound and outbound directions can be used in situations where you are trying to locate assets in between two points, such as two networks or IP addresses.*	
include only the following **inbound applications**	Filters assets from the contributing test question that include only or exclude any inbound or outbound applications. This test only filters connections that include flow data.	Configure the following parameters: • **include only | exclude** - Specify the condition (include only or exclude) that you want this test to apply. When you apply the exclude condition to this test, the not condition applies to the application parameter. For example, if you configure this test as **exclude the following inbound applications**, the test excludes all returned asset results that exclude the specified applications inbound to the asset. • **inbound | outbound** - Specify if you want this test to consider inbound or outbound communications. The default is inbound. • **applications** - Specify any applications to which you want this test to apply. This information is only available when the application level flows are provided.

Note: *Inbound refers to a test that is filtering the connections for which the asset in question is a destination. Outbound refers to a test that is filtering connections for which the asset in question is a source.*

Note: *We recommend when using restrictive tests that the direction of the restrictive test follows the same direction as the contributing test. Restrictive tests using a mix of inbound and outbound directions can be used in situations where you are trying to locate assets in between two points, such as two networks or IP addresses.*

Table A-2 Actual Communication - Restrictive Tests (continued)

Test Name	Description	Parameters
include only if the **source inbound** and **destination outbound** bytes have a percentage difference **less than 10**	Filters assets from the contributing test question based on communications with a specific ratio of inbound to outbound (or outbound to inbound) bytes. This test is useful for detecting hosts that may be exhibiting proxy type behavior (inbound equals outbound).	Configure the following parameters: • **source | destination** - Specify if you want this test to consider source or destination communications. The default is source. • **inbound | outbound** - Specify if you want this test to consider inbound or outbound communications. The default is inbound. • **destination | source** - Specify if you want this test to consider source or destination communications. The default is destination. • **outbound | inbound** - Specify if you want this test to consider inbound or outbound communications. The default is outbound. • **less than | greater than | equal to** - Specify if you want this test to consider greater than, less than, or equal to the configured value. The default is less than. • **10** - Specify the number you want this test to consider.
include only if the inbound and outbound **flow count** has a percentage difference **less than 10**	Filters assets from the contributing test question based on communications with a specific ratio of inbound to outbound (or outbound to inbound) flows. This test only filters connections that include flow data when flow count is selected.	Configure the following parameters: • **flow count | host count -** Specify whether you want this test to consider flow count or host count. The default is host count. • **less than | greater than | equal to** - Specify if you want this test to consider greater than, less than, or equal to the configured value. The default is less than. • **10** - Specify the number you want this test to consider.

***Note:** This restrictive test requires two contributing tests that specify a source and destination. The following test outlines a set of questions trying to determine what assets between two points have an inbound and outbound percentage difference greater than 40%. For example,*

- **Contributing test** - have accepted communication to the internet.
- **Contributing test** - and have accepted communication from the internet.
- **Restrictive test** - and include only if the inbound and outbound flow count has a percentage difference greater than 40.

Table A-2 Actual Communication - Restrictive Tests (continued)

Test Name	Description	Parameters
include only if the time is between **start time** and **end time** inclusive	Filters communications within your network that occurred within a specific time range. This allows you to detect out-of-policy communications. For example, if your corporate policy allows FTP communications between 1 and 3 am, this tests can detect any attempts to use FTP to communicate outside of that time range.	Configure the following parameters: • **include only | exclude** - Specify the condition (include only or exclude) that you want this test to apply. When you apply the exclude condition to this test, the not condition applies to the time window specified. For example, if you configure this test as **exclude if the time is between start time and end time inclusive**, the test excludes all returned asset results that fall between the specified start and end time. • **start time** - Specify a start time that you want this test to consider. • **end time** - Specify an end time that you want this test to consider.
include only if the day of week is between **start day** and **end day** inclusive	Filters assets from the contributing test question based on network communications that occurred within a specific time range. This allows you to detect out-of-policy communications.	Configure the following parameters: • **include only | exclude** - Specify the condition (include only or exclude) that you want this test to apply. When you apply the exclude condition to this test, the not condition applies to the time window specified. For example, if you configure this test as **exclude if the day of the week is between start day and end day inclusive**, the test excludes all returned asset results that fall between the specified start and end time. • **start day** - Specify the day of the week you want this test to consider. • **end day** - Specify the day of the week you want this test to consider.
include only if susceptible to vulnerabilities that are exploitable.	Filters assets from a contributing test question searching for specific vulnerabilities and restricts results to exploitable assets.	This restrictive test does not contain configurable parameters, but is used in conjunction with the contributing test, **are susceptible to one of the following vulnerabilities.** This contributing rule containing a vulnerabilities parameter is required.

Table A-2 Actual Communication - Restrictive Tests (continued)

Test Name	Description	Parameters
include only the following **networks**	Filters assets from a contributing test question that includes or excludes the configured networks.	Configure the following parameters: • **include only | exclude** - Specify the condition (include only or exclude) that you want this test to apply. When you apply the exclude condition to this test, the not condition applies to the network specified. For example, if you configure this test as **exclude the following network**, the test excludes all returned asset results that do not include the specified network. • **networks** - Specify the area of networks to which you want this test to apply.
include only the following **asset building blocks**	Filters assets from a contributing test question that are or are not associated with the configured asset building blocks.	Configure the following parameters: • **include only | exclude** - Specify the condition (include only or exclude) that you want this test to apply. When you apply the exclude condition to this test, the not condition applies to the network specified. For example, if you configure this test as **exclude the following asset building blocks**, the test excludes all returned asset results that do not contain the specified building blocks. • **asset building blocks** - Specify the assets to which you want this test to apply.
include only the following **IP addresses**	Filters assets that are or are not associated with the configured IP addresses.	Configure the following parameters: • **include only | exclude** - Specify the condition (include only or exclude) that you want this test to apply. When you apply the exclude condition to this test, the not condition applies to the network specified. For example, if you configure this test as **exclude the following IP addresses**, the test excludes all returned asset results that do not include the specified IP addresses. • **IP addresses** - Specify the IP address(es) to which you want this test to apply.

Asset tests - Possible communication (contributing)

The possible communication tests for assets include the following contributing question parameters:

Table A-3 Possible Communication - Contributing Tests

Test Name	Description	Parameters
have accepted communication **to any destination**	Detects assets that have possible communications to or from any specified source or destination. For example, to determine if a critical server can possibly receive communications from any source, configure the test as follows: have accepted communication from any source. You can then apply a restrictive test to return if that critical server has received any communications on port 21. This allows you to detect out-of-policy communications for that critical server.	Configure the following parameters: • **to any destination | from any source** - Specify if you want this test to consider the source or destination network. The default is to any destination. • **networks** - Specify the area of the networks to which you want this test to apply.
have accepted communication **to destination networks**	Detects assets that have possible communications to or from the configured network. This test allows you to define a start or end point to your question. For example, to identify the assets that have the possibility of communicating to the DMZ, configure the test as follows: have accepted communication from source <networks> You can use this test to detect out-of-policy communications.	Configure the following parameters: • **to destination | from source** - Specify if you want this test to consider the source or destination network. The default is to destination. • **networks** - Specify the area of the networks to which you want this test to apply.

Table A-3 Possible Communication - Contributing Tests (continued)

Test Name	Description	Parameters
have accepted communication **to destination IP addresses**	Detects assets that have possible communications to or from the configured IP address. This test allows you to specify a single IP address as a focus for possible communications. For example, if you want to identify all assets that can communicate to a specific compliance server, configure the test as follows: have accepted communications to destination <compliance server IP address>	Configure the following parameters: • **to destination | from source** - Specify if you want this test to consider the source or destination IP addresses. The default is to destination. • **IP addresses** - Specify the list of IP address(es) to which you want this test to apply.
have accepted communication **to destination asset building blocks**	Detects assets that have possible communications to or from the configured asset using building blocks. This test allows you to re-use building blocks defined in the QRadar Rules Wizard in your query. For example, if you want to identify all assets that can communicate to a Protected Assets, configure the test as follows: have accepted communications to destination <BB:HostDefinition:Protected Assets> For more information about rules and building blocks, see the *QRadar Administration Guide*.	Configure the following parameters: • **to destination | from source** - Specify if you want this test to consider the source or destination asset building blocks. The default is to destination. • **asset building blocks** - Specify the assets to which you want this test to apply.
have accepted communication **to** the Internet	Detects if source or destination communications are possible to or from the Internet.	Configure the **to | from** parameter, which allows you to specify if you want this test to consider communication traffic to the Internet or from the Internet. The default is to.

Table A-3 Possible Communication - Contributing Tests (continued)

Test Name	Description	Parameters
are susceptible to one of the following **vulnerabilities**	Detects possible specific vulnerabilities. If you want to detect vulnerabilities of a particular type, use the “are susceptible to vulnerabilities with one of the following classifications” test.	Configure the **vulnerabilities** parameter, which allows you to specify the vulnerabilities to which you want this test to apply. You can search for vulnerabilities using the OSVDB ID, CVE ID, Bugtraq ID, or title. For more information about OSVDB, see http://osvdb.org.
are susceptible to vulnerabilities with one of the following **classifications**	A vulnerability can be associated with one or more vulnerability classification. This test filters all assets that have possible vulnerabilities with a Common Vulnerability Scoring System (CVSS) score, as specified.	Configure the **classifications** parameter to identify the vulnerability classifications that you want this test to apply.
are susceptible to vulnerabilities with CVSS score **greater than 5**	A Common Vulnerability Scoring System (CVSS) value is an industry standard for assessing the severity of possible vulnerabilities. CVSS is composed of three metric groups: Base, Temporal, and Environmental. These metrics allow CVSS to define and communicate the fundamental characteristics of a vulnerability. This test filters assets in your network that include the configured CVSS value.	Configure the following parameters: • **greater than | less than | equal to** - Specify whether the Common Vulnerability Scoring System (CVSS) score should be greater than, less than, or equal to the configured value. The default is greater than. • **5** - Specify the CVSS score you want this test to consider. The default is 5.
are susceptible to vulnerabilities from the following **vendors**		Configure the **vendors** parameter to identify possible vulnerabilities that have been introduced on assets from a specific vendors.
Note: *The contributing test for assets that are susceptible to vulnerabilities from the following vendors has been hidden in the Policy Monitor. If you currently use this contributing test it is still visible in the test, but has been replaced by a contributing test that searches assets for vulnerabilities by text entries or regular expressions.*		
are susceptible to vulnerabilities with the following **services**		Configure the **services** parameter to identify possible vulnerabilities that have been introduced on assets from a specific services.
Note: *The contributing test for assets that are susceptible to vulnerabilities from the following services has been hidden in the Policy Monitor. If you currently use this contributing test it is still visible in the test, but has been replaced by a contributing test that searches assets for vulnerabilities by text entries or regular expressions.*		

Table A-3 Possible Communication - Contributing Tests (continued)

Test Name	Description	Parameters
are susceptible to vulnerabilities disclosed **after specified date**	Filters assets in your network with a possible vulnerability that is disclosed after, before, or on the configured date.	Configure the following parameters: • **after | on | before** - Specify whether you want the test to consider the disclosed vulnerabilities to be after, before, or on the configured date. The default is after. • **specified date** - Specify the date that you want this test to consider.
Are susceptible to vulnerabilities on one of the following **ports**	Filters assets in your network with a possible vulnerability that is associated with the configured ports.	Configure the **ports** parameter to identify assets that have possible vulnerabilities based on the specified port number.
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following **text entries**	Detects assets in your network with a vulnerability that matches the asset name, vendor, version or service based one or more text entry.	Configure the **text entries** parameter to identify the asset name, vendor, version or service you want this test to consider.
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following **regular expressions**	Detects assets in your network with a vulnerability that matches the asset name, vendor, version or service based one or more regular expression.	Configure the **regular expressions** parameter to identify the asset name, vendor, version or service you want this test to consider.

Asset tests - Possible communication (restrictive)

The possible communication tests for assets include the following restrictive question parameters:

Table A-4 Possible Communication - Restrictive Tests

Test Name	Description	Parameters
include only the following **protocols**	Filters assets that have or have not possibly communicated with the configured protocols, in conjunction with the other tests added to this question.	Configure the **protocols** parameter, which allows you to specify the list of protocols to which you want this test to apply.
include only the following inbound **ports**	Filters assets that have or have not possibly communicated with the configured ports, in conjunction with the other tests added to this question.	Configure the **ports** parameter, which allows you to specify the ports to which you want this test to apply.
include only ports other than the following **inbound ports**	Filters assets from a contributing test question that have or have not possibly communicated with ports other than the configured ports, in conjunction with the other tests added to this question.	Configure the following parameters: • **inbound | outbound** - Specify if you want this test to consider inbound or outbound communications. The default is inbound. • **ports** - Specify the ports to which you want this test to apply.

Note: *Inbound refers to a test that is filtering the connections for which the asset in question is a destination. Outbound refers to a test that is filtering connections for which the asset in question is a source.*

Note: *We recommend when using restrictive tests that the direction of the restrictive test follows the same direction as the contributing test. Restrictive tests using a mix of inbound and outbound directions can be used in situations where you are trying to locate assets in between two points, such as two networks or IP addresses.*

include only if susceptible to vulnerabilities that are exploitable.	Filters assets from a contributing test question searching for possible specific vulnerabilities and restricts results to exploitable assets.	This restrictive test does not contain configurable parameters, but is used in conjunction with the contributing test, **are susceptible to one of the following vulnerabilities**. This contributing rule containing a vulnerabilities parameter is required.
include only the following **networks**	Filters assets from a contributing test question that include only or exclude the configured networks.	Configure the following parameters: • **include only | exclude** - Specify the condition (include only or exclude) that you want this test to apply. • **networks** - Specify the area of networks to which you want this test to apply.
include only the following **asset building blocks**	Filters assets from a contributing test question that include only or exclude the configured asset building blocks.	Configure the following parameters: • **include only | exclude** - Specify the condition (include only or exclude) that you want this test to apply. • **asset building blocks** - Specify the assets to which you want this test to apply.

Table A-4 Possible Communication - Restrictive Tests (continued)

Test Name	Description	Parameters
include only the following **IP addresses**	Filters assets Filters assets from a contributing test question include only or exclude the configured IP addresses.	Configure the following parameters: • **include only | exclude** - Specify the condition (include only or exclude) that you want this test to apply. • **IP addresses** - Specify the IP address(es) to which you want this test to apply.

Device/Rules tests

The Device/Rules tests include:

Table A-5 Device/Rules Tests

Test Name	Description	Parameters
allow connections **to** the following **networks**	Filters device rules and connections to or from the configured networks. For example, if you configure the test to allow communications to a network, the test filters all rules and connections that allow connections to the configured network.	Configure the following parameters: • **allow | deny** - Specify the condition (allow or do not allow) that you want this test to apply. The default is allow. • **to| from** - Specify if you want this test to consider communication traffic to or from the specified networks. The default is to. • **networks** - Specify the area of networks to which you want this test to apply.
allow connections **to** the following **IP addresses**	Filters device rules and connections to or from the configured IP addresses. For example, if you configure the test to allow communications to an IP address, the test filters all rules and connections that allow connections to the configured IP address.	Configure the following parameters: • **allow | deny** - Specify the condition (allow or do not allow) that you want this test to apply. The default is allow. • **to| from** - Specify if you want this test to consider communication traffic to or from the specified IP addresses. The default is to. • **IP addresses**- Specify the IP address(es) to which you want this test to apply.
allow connections **to** the following **asset building blocks**	Filters device rules and connections to or from the configured asset building block.	Configure the following parameters: • **allow | deny** - Specify the condition (allow or do not allow) that you want this test to apply. The default is allow. • **to| from** - Specify if you want this test to consider communication traffic to or from the defined asset building blocks. The default is to. • **asset building blocks** - Specify the assets to which you want this test to apply.

Table A-5 Device/Rules Tests (continued)

Test Name	**Description**	**Parameters**
allow connections using the following **destination ports and protocols**	Filters device rules and connections to or from the configured ports and protocols	Configure the following parameters: • **allow | deny** - Specify the condition (allow or do not allow) that you want this test to apply. The default is allow. • **destination | source** - Specify if you want this test to consider the source or destination port. The default is to destination. • **ports** - Specify the destination ports to which you want this test to apply. • **protocols** - Specify the list of protocols to which you want this test to apply.
allow connections using the following **protocols**	Filters device rules and connections to or from the configured protocols.	Configure the following parameters: • **allow | deny** - Specify the condition (allow or do not allow) that you want this test to apply. The default is allow. • **protocols** - Specify the list of protocols to which you want this test to apply.
allow connections **to** the Internet	Filters device rules and connections to and from the Internet.	**Configure the following parameters:** • **allow | deny** - Specify the condition (allow or do not allow) that you want this test to apply. The default is allow. • **to| from** - Specify if you want this test to consider communication traffic to or from the Internet. The default is to.
are one of the following **devices**	Filters all network devices to the configured devices. This test can filter based on devices that are or are not in the configured list.	Configure the following parameters: • **are | are not** - Specify the condition (are or are not) that you want this test to apply. The default is are. • **devices** - Specify the devices that you want this test to consider.

B VIEWING AUDIT LOGS

Changes made by IBM Security QRadar Risk Manager users are recorded in the **Log Activity** tab of IBM Security QRadar SIEM. All logs appear in the Risk Manager Audit category. For more information on using the **Log Activity** tab in QRadar SIEM, see the *IBM Security QRadar SIEM Users Guide.*

Logged actions

QRadar Risk Manager logs the following categories of actions:

Table B-1 Logged Actions

Category	Action
Policy Monitor	Create a question.
	Edit a question.
	Delete a question.
	Submit a question manually.
	Submit a question automatically.
	Approve results.
	Revoke results approval.
Topology Model	Create a topology model.
	Edit a topology model.
	Delete a topology model.
Topology	Save layout.
	Create a Topology saved search.
	Edit a Topology saved search
	Delete a Topology saved search
	Placing an IPS.
Configuration Monitor	Create a log source mapping
	Edit a log source mapping
	Delete a log source mapping

Table B-1 Logged Actions (continued)

Category	Action
Simulations	Create a simulation.
	Edit a simulation.
	Delete a simulation.
	Manually run a simulation.
	Automatically run a simulation.
	Approve simulation results.
	Revoke simulation results.
Configuration Source Management	Successfully authenticate for the first time on a session.
	Add a device.
	Remove a device.
	Edit the IP address or adapter for a device.
	Save a credential configuration.
	Delete a credential configuration.
	Save a protocol configuration.
	Remove a protocol configuration.
	Create a schedule for a backup job.
	Delete a schedule for a backup job.
	Edit a backup job.
	Add a backup job.
	Delete a backup job.
	Run a scheduled backup job.
	Complete a scheduled job whether the job is successful or has failed.
	After a backup job has completed processing and the configuration was persisted, no changes discovered.
	After a backup job has completed processing and the configuration was persisted, changes were discovered.
	After a backup job has completed processing and the configuration was persisted, unpersisted changes were discovered.
	After a backup job has completed processing and the configuration that was previously persisted no longer resides on the device.
	Adapter operation attempt has begun, which includes protocols and credentials.
	Adapter operation attempt has been successful, including the protocols and credentials.

Viewing QRadar Risk Manager user activity in QRadar Risk Manager

To view activity for QRadar Risk Manager users in QRadar SIEM:

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

The Log Activity page is displayed. If you previously saved a search as the default, the results for that saved search is displayed.

Step 2 Click **Search** > **New Search** to create a search.

Step 3 In the **Time Range** pane, select an option for the time range you want to capture for this search.

Step 4 In the **Search Parameters** pane, define your search criteria:

a From the first drop-down list box, select **Category**.

b From the **High Level Category** drop-down list box, select **Risk Manager Audit**.

c Optional. From the **Low Level Category** drop-down list box, select a category to refine your search.

Step 5 Click **Add Filter**.

The Current Filters updates with your search filter.

Step 6 Click **Filter** to search for QRadar Risk Manager events.

Viewing the log File

All audit logs are stored in plain text and are archived and compressed when the audit log file reaches a size of 200 MB. The current log file is named **`audit.log`**. If the audit log file reaches a size of 200 MB a second time, the file is compressed and the old audit log is renamed as follows: **`audit.1.gz, audit.2.gz`**, etc with the file number increments each time a log file is archived. QRadar Risk Manager can store up to 50 archived log files.

To view an audit logs in QRadar Risk Manager:

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

Username: **`root`**

Password: **`<Password>`**

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

Username: **`root`**

Password: **`<Password>`**

Step 3 Go to the following directory:

```
/var/log/audit
```

Step 4 Open your audit log file.

Each entry in the log file displays using the following format:

NOTE

The maximum size of any audit message (not including date, time, and host name) is 1024 characters.

```
<date_time> <host name> <user>@<IP address> (thread ID)
[<category>] [<sub-category>] [<action>] <payload>
```

Where:

`<date_time>` is the date and time of the activity in the format: Month Date HH:MM:SS.

`<host name>` is the host name of the Console where this activity was logged.

`<user>` is the name of the user that performed the action.

`<IP address>` is the IP address of the user that performed the action.

`(thread ID)` is the identifier of the JavaTM thread that logged this activity.

`<category>` is the high-level category of this activity.

`<sub-category>` is the low-level category of this activity.

`<action>` is the activity that occurred.

`<payload>` is the complete record that has changed, if any.

C 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 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*.

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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

INDEX