JUNIPER NETWORKS | Engineering Simplicity

Juniper Secure Analytics Risk Manager User Guide

Published
2023-07-25

RELEASE
7.5.0

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Secure Analytics Risk Manager User Guide
7.5.0

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

Use this guide to configure and use Risk Manager on a JSA console.

1
CHAPTER

JSA Risk Manager

JSA Risk Manager Overview

SUMMARY

JSA 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.

IN THIS SECTION

JSA Risk Manager uses data that is collected by JSA. For example, configuration data from firewalls, routers, switches, or intrusion prevention systems (IPSs), vulnerability feeds, and third-party security sources. Data sources enable JSA Risk Manager to identify security, policy, and compliance risks in your network and estimate the probability of risk exploitation.

JSA Risk Manager alerts you to discovered risks by displaying offenses on the **Offenses** tab. Risk data is analyzed and reported in the context of all other data that JSA processes. In JSA Risk Manager, you can evaluate and manage risk at an acceptable level that is based on the risk tolerance in your company.

You can also use JSA Risk Manager to query all network connections, compare device configurations, filter your network topology, and simulate the possible effects of updating device configurations.

You can use JSA Risk Manager to define a set of policies (or questions) about your network and monitor the policies for changes. For example, if you want to deny unencrypted protocols in your DMZ from the Internet, you can define a policy monitor question to detect unencrypted protocols. Submitting the question returns a list of unencrypted protocols that are communicating from the Internet to your DMZ and you can determine which unencrypted protocols are security risks.

What's New for Users in JSA Risk Manager 7.4.0

SUMMARY

JSA Risk Manager 7.4.0 introduces improved support for Juniper Networks JUNOS OS Network Address Translation.

JSA Risk Manager 7.4.0 introduces improved support for Network Address Translation (NAT) functionality in Juniper Networks JUNOS OS devices to cater to service sets. NAT provides increased security for your JSA deployment because requests are managed through the conversion process and internal IP addresses are hidden. Unlike other devices that perform NAT, JUNOS OS NAT functions use expansion cards to perform the NAT process.

For more information about the Juniper Networks JUNOS OS adapter, see the *Supported adapters* section of the *Juniper Secure Analytics Risk Manager Adapter Configuration Guide*.

Supported Web Browsers

SUMMARY

For the features in JSA products to work properly, you must use a supported web browser.

IN THIS SECTION

The following table lists the supported versions of web browsers.

Table 1: Supported Web Browsers for JSA Products

Web browser	Supported versions
64-bit Mozilla Firefox	60 Extended Support Release and later
64-bit Microsoft Edge	38.14393 and later
64-bit Google Chrome	Latest

The Microsoft Internet Explorer web browser is no longer supported on JSA 7.4.0 or later.

Security Exceptions and Certificates

If you are using the Mozilla Firefox web browser, you must add an exception to Mozilla Firefox to log in to JSA. For more information, see your Mozilla Firefox web browser documentation.

Navigate the Web-Based Application

When you use JSA, use the navigation options available in the JSA Console instead of your web browser **Back** button.

JSA Risk Manager Login Information

SUMMARY

JSA Risk Manager uses default login information for the URL, username, and password.

You access JSA Risk Manager through the JSA Console. Use the information in the following table when you log in to your JSA Console.

Table 2: Default login information for JSA Risk Manager

Login information	Default
URL	**https://<IP address>**, where *<IP address>* is the IP address of the JSA Console.
Username	admin
Password	The password that is assigned to JSA Risk Manager during the installation process. **TIP**: As a good security practice, change the root password on your JSA Risk Manager host at regular intervals.
License key	A default license key provides access to the system for 5 weeks.

JSA Risk Manager Feature Overview

SUMMARY

Use JSA Risk Manager features to manage risk in your network, monitor device configurations, view topologies, simulate changes to your network environment, and prioritize risks and vulnerabilities in your network.

IN THIS SECTION

Connections

Use the **Connections** feature to monitor the network connections of your local hosts. The connection graph provides a visual representation of the connections in your network. Use the time-series charts to access, navigate, and investigate connections from various views and perspectives. Run queries and reports on the network connections of your local hosts that are based on applications, ports, protocols, and websites that the local hosts can communicate with.

Configuration Monitor

Use the configuration monitor to review and compare device configurations, and to manage security policies and to monitor device modifications within your network. Device configurations might 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, which you can use to identify inconsistencies and configuration changes that introduce risk in your network.

Topology

The topology is a graphical representation that depicts the physical infrastructure and connectivity of your layer 3 network topology. The topology is drawn form configuration information that is imported from devices in your network by using configuration source management.

The graph is created from detailed configuration information that is obtained from network devices, such as firewalls, routers, switches, and intrusion prevention systems (IPS).

Use the interactive graph in the topology to view connections between devices. A topology path search can determine how your network devices are communicating and the network path that they use to communicate. Path searching allows JSA Risk Manager to display the path between a source and destination, along with the ports, protocols, and rules.

Policy Monitor

Use the policy monitor to define specific questions about risk in your network and then submit the question to JSA Risk Manager.
JSA Risk Manager evaluates the parameters that you define 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. JSA Risk Manager provides many predefined policy monitor questions, and you can create your own custom questions. Policy monitor questions can be created for the following situations:

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

The policy monitor uses data from configuration data, network activity data, network and security events, and vulnerability scan data to determine the appropriate response. JSA Risk Manager provides policy templates to help you determine 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.

You can actively monitor an unlimited number of questions in policy monitor. When a question is monitored, JSA Risk Manager continuously evaluates the question for unapproved results. When unapproved results are discovered, JSA Risk Manager can be configured to send email notifications, display notifications, generate a syslog event or create an offense in JSA.

Policy Management

You use the JSA Risk Manager policy management pages to view details about policy compliance and policy risk changes for assets, policies, and policy checks.

The JSA Risk Manager policy management pages display data from the last run policy. You can filter the data by asset, by policy, or by policy check.

Simulation

Use simulations to create network simulations.

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.

Simulate an attack by using a topology model where you can make network changes without impacting a live network.

You can simulate how changes to network rules, ports, protocols, or allowed or denied connections can affect your network. Use the simulation feature to determine the risk impact of proposed changes to your network configuration before you implement these changes.

You can review the results when a simulation is complete.

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

Configuration Source Management

Configure **Configuration Source Management** to get device configuration information from the devices in your network, which give JSA Risk Manager the data it needs to manage risk in your network. You use the configuration information that is collected from your network devices to generate the topology for your network configuration.

Reports

Use the **Reports** tab to create specific reports, based on data available in JSA Risk Manager, such as connections, device rules, and device unused objects.
The following detailed reports are also available:

- Connections between devices
- Firewall rules on a device
- Unused objects on a device

Unsupported features in JSA Risk Manager

It is important to be aware of the features that are not supported by JSA Risk Manager but are available in the JSA Console.

The following features are not supported by JSA Risk Manager:

- High availability (HA)
- Dynamic Routing for Border Gateway Protocol (BGP)
- Non-contiguous network masks
- Load-balanced routes

2

CHAPTER

JSA Risk Manager configuration

JSA Risk Manager Configuration

SUMMARY

You can configure access settings for JSA Risk Manager from the **Admin** tab of JSA. When you add JSA Risk Manager to your deployment, you must configure settings, such as the local firewall, network interfaces, email server, and add the appropriate license.

IN THIS SECTION

If you have administrator permissions, you can configure several appliance settings for JSA Risk Manager:

- From the **System and License Management** window, you can manage licenses, configure the local firewall, add an email server, and configure network interfaces for JSA Risk Manager.
- Change the password for a host.
- Update the system time.

Configuring System Settings

SUMMARY

To get your JSA security system up and running or to maintain your system, you must configure your JSA Console and managed hosts system settings from the **System Information** window.

Assign roles for network interfaces, bond interfaces, manage licenses, configure the email server that you want JSA to use, and use the local firewall to manage access from external devices to JSA.

If you need to make network configuration changes, such as an IP address change to your JSA Console and managed host systems after you install your JSA deployment, use the **qchange_netsetup** utility. If you use **qchange_netsetup**, verify all external storage which is not/store/ariel or /store is not mounted. For more information about network settings, see the *Juniper Secure Analytics Risk Manager Installation Guide*.

If you change the External Flow Source Monitoring Port parameter in the Flow Processor configuration, you must also update your firewall access configuration.

1. Click the **Admin** tab.
2. In the **System Configuration** section, click the **System and License Management** icon.
3. From the **Display** menu, select **Systems**.
4. Select the relevant host.
5. From the **Actions** menu, click **View and Manage System**.
   You can right-click the selected host to access this menu option, or you can double-click the host to open the **Systems Information** window.
6. To configure your local firewall to allow access to this host from specified devices outside of your JSA deployment, click the **Firewall** tab.
   a. Configure access for devices that are outside of your deployment and need to connect to this host.
   b. Add this access rule by clicking the arrow.
7. To configure network interfaces on your JSA system, click the **Network Interfaces** tab.
   a. Select a network interface from the **Device** column.
   b. To edit your network interfaces, click **Edit**, and then configure the parameters.
   c. To bond network interfaces, click **Bond**, and then configure the parameters.

   For more information about configuring network interfaces, see the *Juniper Secure Analytics Administration Guide*.

   IMPORTANT: You can't edit a network interface with a management, HA crossover, or secondary role.

8. To configure an email server to distribute alerts, reports, notifications, and event messages, click the **Email Server** tab.
   a. In the **Email Server Address** field, type the hostname or IP address of the email server that you want to use.
   b. If you don't have an email server and you want to use the email server that JSA provides, type **localhost** to provide local email processing.
   c. If you configure the mail server setting as **localhost**, then the mail messages do not leave the JSA box. If you want external mail delivery, use a valid mail relay server.

TIP: It is a good practice to use port 25 for the email server connection.

9. Click **Save**.

Updating the System Time on the JSA Console

SUMMARY

Configure the system time on your JSA Console by setting the time manually, or by using NTP servers. The JSA Console synchronizes JSA Console system time with the managed hosts in your deployment.

1. Click the **Admin** tab.
2. In the **System Configuration** section, click the **System and License Management** icon.
3. From the **Display** menu, select **Systems**.
4. Select the relevant host.
5. From the **Actions** menu, select **View and Manage System**, and then click the **System Time** tab.
6. Select a time zone from the **Time Zone** menu.

   You can configure only the time zone on a managed host. The system time is synchronized with the JSA Console but if the managed host is in a different time zone, then you can change to that time zone.
7. To configure the system time manually, click **Set time manually**, and then set a date and a time.

   EXCEPTIONS:

   If you set the system time to a future date that is affected by Daylight Saving Time (DST) changes, the time you set is adjusted by one hour. For example, on 4 July 2020, in the US, you set the time and date to 20:00, 16 December 2020. The time that you set ignores the DST change and is adjusted to 19:00.

When you set the system time on VMWare systems and then restart the system, the changes might be lost. To prevent the time changes from being lost you can edit the **.vmx** file on the virtual device to disable time synchronization, by adding the following lines to the synchronization properties:

```
tools.syncTime = "FALSE"
time.synchronize.continue = "FALSE"
time.synchronize.restore = "FALSE"
time.synchronize.resume.disk = "FALSE"
time.synchronize.shrink = "FALSE"
time.synchronize.tools.startup = "FALSE"
```

8. To configure time by using NTP servers, click **NTP Time Servers**.
   a. Type an IP address or a host name for the NTP server in the **Server 1 Address** field.
      Host names are resolved by a DNS server.
   b. To add NTP servers, click the plus icon next to **Add More**.
9. Click **Save**.
10. Click **OK** to accept that services are restarted, or **Cancel** to cancel the changes.
    The services that are restarted include host context and tomcat.

3

CHAPTER

Network Device Management

Network Device Management

SUMMARY

You use Configuration Source Management to configure credentials, add or discover devices, view device configurations, and back up device configurations in JSA Risk Manager.

IN THIS SECTION

Configuration Source Management will no longer work after the end of 2020, when browsers discontinue support for Adobe Flash. You can configure credentials, protocols, and schedules in the "Configuration monitor" on page 45 on JSA 7.4.1, patch 1 and later. For more information about this change, see *Juniper Secure Analytics Risk Manager: Adobe Flash End of Life and Changes to Configuration Source Management (CSM)*.

The data that is 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 JSA.

To set up your configuration sources, you must perform the following actions:

1. Configure your "device credentials" on page 51.

2. Discover or import devices. You can add network devices to JSA Risk Manager in two ways; "discover devices using Configuration Source Management" on page 19 or "import a list of devices" on page 21 from a CSV file in **Device Import**.
3. "Obtain device configuration" on page 25 from each of your devices.
4. "Manage backup jobs" on page 29 to ensure that all updates to device configurations are captured.
5. Set up the "discovery schedule" on page 26 to ensure that new devices are automatically discovered.

You use Configuration Source Management to do the following actions:

- Add, edit, search, and delete configuration sources.
- Configure or manage communication protocols for your devices. For more information, see "Configuring Protocols in JSA Risk Manager" on page 57.

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

For more information about adapters that are used to communicate with devices from specific manufacturers, see *Juniper Secure Analytics Risk Manager Adapter Configuration Guide*.

Credentials for Accessing Device Configurations

SUMMARY

In JSA Risk Manager, credentials are used to access and download the configuration of devices such as firewalls, routers, switches, or IPSs.

IN THIS SECTION

Configuration Source Management will no longer work after the end of 2020, when browsers discontinue support for Adobe Flash. You can configure credentials, protocols, and schedules in the "Configuration monitor" on page 45 on JSA 7.4.1, patch 1 and later. For more information about this change, see *Juniper Secure Analytics Risk Manager: Adobe Flash End of Life and Changes to Configuration Source Management (CSM)*.

Administrators use Configuration Source Management to input device credentials that give JSA Risk Manager access to specific devices. Individual device credentials can be saved for a specific network device. If multiple network devices use the same credentials, you can assign credentials to a group.

You can assign different devices in your network to network groups, to group credential sets 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 a set of credentials.

For example, the firewalls in your organization might have the same username and password. If so, the credentials that are associated with all the address sets for all the firewalls are used to back up 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 *Juniper Secure Analytics Risk Manager Adapter Configuration Guide*.

Configure JSA 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 network groups have the following composition:

- Network group 1 contains two credential sets.
- Network group 2 contains two credential sets.

JSA Risk Manager compiles a maximum of three credential sets, so the following credential sets are used:

- Both credential sets in network group 1 are used because network group 1 is higher in the list.
- Only the first credential set in the network group 2 is used because only three credential sets are required.

When a credential set is used to successfully access a device, JSA Risk Manager uses that same credential set for subsequent attempts to access the device. If the credentials on that device change, the authentication fails and for the next authentication attempt, JSA Risk Manager compiles the credentials again to ensure success.

Configuring Credentials for JSA Risk Manager

SUMMARY

Administrators must configure credentials to allow JSA Risk Manager to connect to devices in the network.

Configuration Source Management will no longer work after the end of 2020, when browsers discontinue support for Adobe Flash. You can configure credentials, protocols, and schedules in the "Configuration monitor" on page 45 on JSA 7.4.1, patch 1 and later. For more information about this change, see *Juniper Secure Analytics Risk Manager: Adobe Flash End of Life and Changes to Configuration Source Management (CSM)*.

1. Click the **Admin** tab.
2. Click **Apps**.
3. In the **Risk Manager** pane, click **Configuration Source Management**.
4. On the navigation menu, click **Credentials**.
5. In the **Network Groups** pane, click the **Add (+)** icon.
6. Type a name for a network group, and then click **OK**.
7. Make the network group that you want to have first priority the first item on the list. You can use the **Move Up** and **Move Down** arrow icons to prioritize a network group.
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.

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

   TIP: You can type an IP address range that uses 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 that meet that requirement are included.
9. In the **Credentials** pane, click the **Add (+)** icon.
10. Type a name for the new credential set, configure the values for the parameters, and then click **Save**.

    TIP:
    Move UpMove Down

Device Discovery Process

SUMMARY

In JSA Risk Manager, use the **Device Discovery** screen in the Configuration Monitor to add, edit, and run a defined discovery.

Configuration Source Management will no longer work after the end of 2020, when browsers discontinue support for Adobe Flash. You can configure credentials, protocols, and schedules in the "Configuration monitor" on page 45 on JSA 7.4.1, patch 1 and later. For more information about this change, see *Juniper Secure Analytics Risk Manager: Adobe Flash End of Life and Changes to Configuration Source Management (CSM)*.

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 ports 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.

This information is used to determine which adapter the device should be mapped to when added. JSA 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 might not be the assigned IP address for the new device. JSA Risk Manager adds a device by using the IP address for the lowest numbered interface on the device (or lowest loopback address, if any).

If you select the **Crawl the network from the addresses defined above** checkbox, the IP address of the neighbors that are collected from the device are reintroduced into the discovery process. The process repeats for each IP address.

Discovering Devices in your Network

SUMMARY

Administrators use Discover Devices to determine the type of device. During 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.

Configuration Source Management will no longer work after the end of 2020, when browsers discontinue support for Adobe Flash. You can configure credentials, protocols, and schedules in the "Configuration monitor" on page 45 on JSA 7.4.1, patch 1 and later. For more information about this change, see *Juniper Secure Analytics Risk Manager: Adobe Flash End of Life and Changes to Configuration Source Management (CSM)*.

1. Click the **Admin** tab.
2. Click **Apps**.
3. In the **Risk Manager** pane, click **Configuration Source Management**.
4. Configure the SNMP protocol, and add the IP address or CIDR range of the devices that you want to discover.
   a. On the navigation menu, click **Protocols**.
   b. From the **Network Groups** pane, click the **(+)** symbol.
   c. Type a name for the network group, and click **OK**.
   d. In the **Add address (IP CIDR Wildcard or Range)** field, type the IP address or CIDR range.
   e. Click **(+)** to add the IP address or CIDR range.
   f. Select the **SNMP** protocol, and click **OK**.
5. On the navigation menu, click **Discover Devices**.
6. Type an IP address or CIDR range.
   This IP address or CIDR range indicates the location of devices you want to discover.
7. Click the **Add (+)** icon.
8. 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** checkbox.
9. Click **Run**.

Importing Multiple Devices from a CSV File

SUMMARY

Use Device Import to add a list of adapters and their network IP addresses to the Configuration Source Manager in JSA Risk Manager by using a comma-separated value file (.CSV). You can easily import a principal device list or a bulk upload to Configuration Source Management by using a CSV file.

If you import a list of devices and then alter an IP address in the CSV file, then you might accidentally duplicate a device in the Configuration Source Management list. For this reason, delete a device from Configuration Source Management before you reimport your principal device list.

1. Click the **Admin** tab.
2. Click **Apps**, and in the **Apps** section, click **Device Import**.
3. Click **Browse**.
4. Locate your CSV file and click **Open**.

   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.

   Here's an example of a CSV file that lists the devices to import into the Configuration Source Manager in JSA Risk Manager:

```
Cisco::SecurityAppliance,10.225.80.1
Cisco::SecurityAppliance,10.225.78.3
CheckPoint::SecurePlatform,10.225.80.5
```

```
PaloAlto::PANOS,172.16.54.1
Sourcefire::3D,172.16.16.1
```

5. Click **Import Devices**.

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

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

Adding a Network Device to JSA Risk Manager

SUMMARY

You can add an individual device to the device list in Configuration Source Management or you can add multiple devices by using a CSV file.

1. Click the **Admin** tab.
2. Click **Apps**, and in the **Risk Manager** pane, click **Configuration Source Management**.
3. On the navigation pane, click **Add Device** and configure the parameters.
4. Click **Add**.

   If necessary, click **Go** to refresh the adapter list.
5. To correct the IP address or adapter type if there is an error or if your network changed and you need to reassign an IP address, select the device and click **Edit**.

Deleting a Device from JSA Risk Manager

SUMMARY

You can delete a device from JSA Risk Manager. A deleted device is removed from Configuration Source Management, Configuration Monitor, and the topology.

1. Click the **Admin** tab.
2. Click **Apps**, and in the **Risk Manager** pane, click **Configuration Source Management**.
3. Click the **Devices** tab, and select the device that you want to delete.
4. Click **Remove**, and then confirm the deletion.

After you delete a device, the process to remove the device from the topology might take several minutes.

Finding Network Devices in the Device List

SUMMARY

You can use filters to quickly find devices in the device list. JSA 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 tedious.

The following table describes the types of filters that you can apply to the device list to help you find devices faster.

Table 3: Filtering Search Options in the Device List

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 you want to search for 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.

Table 3: Filtering Search Options in the Device List *(Continued)*

Search Option	Description
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 you want to search for in the **IP/CIDR** field.
OS Version	Filters the device list based on the operating system version devices are running. Select values for the following parameters: **Adapter** - Select the type of adapter you want to search. **Version** - 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 you want to search for. 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** - Select the vendor that you want to search. **Model** - Type the model that you want to search.
Hostname	Filters the device list based on the hostname. Type the hostname you want to search for in the **Hostname** field.

1. Click the **Admin** tab.
2. Click **Apps**.
3. In the Risk Manager pane, click **Configuration Source Management**.
4. Click the **Devices** tab, select a filter from the list, and click **Go**.
5. To reset a filter, select **Interface IP Address**, clear the **IP/CIDR** address, then click **Go**.

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

Adding Device Information to the Topology

SUMMARY

After you configure credential sets and address sets to access network devices, you must backup your devices to download the device configuration so the device information is included in the topology.

1. Click the **Admin** tab.
2. Click **Apps**.
3. In the **Risk Manager** pane, click **Configuration Source Management**, and then click **Devices**.
4. To obtain the configuration for all devices, click **Backup All** in the navigation pane, and then click **Yes**.
5. To obtain the configuration for one device, select the device.
6. To select multiple devices, hold down the CTRL key and select all necessary devices. Click **Backup**.
7. If necessary, click **View Error** to view the details of an error. After correcting the error, click **Backup All** in the navigation pane.

Collecting Neighbor Data to Update the Topology

SUMMARY

Use the discovery process to obtain neighbor data from a device by 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.

1. Click the **Admin** tab.
2. Click **Apps**, and in the **Risk Manager** pane, click **Configuration Source Management**.
3. Click the **Devices** tab.
4. Select the device that you want to obtain data for. To select multiple devices, hold down the CTRL key and select all necessary devices.
5. Click **Discover**.

Use the **Discover** option 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.

6. Click **Yes** to continue.

If you select multiple devices, the discover process can take several minutes to complete. Select **Run in Background** to work on other tasks.

Configuring the Discovery Schedule to Populate Device Information

SUMMARY

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.

Configuration Source Management will no longer work after the end of 2020, when browsers discontinue support for Adobe Flash. You can configure credentials, protocols, and schedules in the "Configuration monitor" on page 45 on JSA 7.4.1, patch 1 and later. For more information about this change, see *Juniper Secure Analytics Risk Manager: Adobe Flash End of Life and Changes to Configuration Source Management (CSM)*.

1. Click the **Admin** tab.
2. Click **Apps**.
3. In the **Risk Manager** pane, click **Configuration Source Management**, and then click **Schedule Discovery**.
4. Select the **Enable periodic discovery** checkbox to enable schedule discovery.
5. Configure the following parameters:

Option	Description
Name	Type a unique 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 24-hour time.
Frequency	Select the frequency that you want to associate with this schedule.

(Continued)

Option	Description
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.
Crawl and discover new devices	If you want the discovery process to discover new devices, select the checkbox. If you do not want to add new devices to the inventory, clear the checkbox.

6. Click **OK**.

4

CHAPTER

Device Configuration Backup Jobs

Device Configuration Backup Jobs

SUMMARY

Use backup jobs to schedule automatic backup configuration information for all devices that are listed on the **Devices** tab.

IN THIS SECTION

Any backup job that you define in JSA Risk Manager does not affect the backup and recovery management functions that are available on the **Admin** tab of the JSA Console. The backup and recovery functions gather configuration information and data for JSA. The JSA Risk Manager backup job gathers only information for external devices.

Creating a Backup Job in JSA Risk Manager

SUMMARY

You can create backup jobs for all devices, or individual groups of devices in Configuration Source Management. After you define the search criteria, you define the job schedule. The triggers for a job represent the job schedule, and you can have multiple schedules that are configured.

1. Click the **Admin** tab.
2. Click **Apps**.
3. In the **Risk Manager** pane, click **Configuration Source Management**.
4. Click the **Jobs** tab, and then select **New Job** > **Backup**.
5. Configure values for the following parameters:
   a. Type the name that you want to apply to this job.
   b. From the Group list, select the group to which you want to assign this job. If there no groups are listed, you can type a group name. You can sort jobs after they are assigned to a group.

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

6. Click **OK**.
7. Select one of the following search methods:

   Static list You can use a static list to search for devices by using several options. Using the static list option, you can define the specific devices on which you want to run the job.

   Search Type an IP address or CIDR range that you want to include in the job. When you define the search criteria, the search for devices is performed after the job is run. Defining the criteria ensures that any new devices are included in the job.

8. If you chose Static list, define the search criteria:
   a. Click the **Devices** tab.
   b. From the list on the **Devices** tab, select the search criteria, and click **Go**.
   c. Select the devices that you want to include in the job.
   d. In the Job Details pane, click **Add selected from device view search**.
9. If you chose Search, define the search criteria:
   a. Click the **Devices** tab.
   b. Using the list in the **Devices** tab, select the search criteria, and click **Go**.
   c. In the Job Details pane, click **Use search from devices view**. This search criteria is used to determine devices that are associated with this job.
10. Click **Schedule**, and configure the following parameters:

Option	Description
Name	Type a unique 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 24-hour time.
Frequency	Select the frequency that you want to associate with this schedule.
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.

11. Click **Save** in the Trigger pane.
12. Repeat steps 10 and 11 to create multiple schedules.

13. If you want to run the job immediately, click **Run Now**.
14. Click **Yes** to continue.

You can rename the backup job at any time by selecting the job and clicking **Rename**. You can also delete a backup job by selecting the job and clicking **Delete**.

Viewing Backup Job Status and Logs

SUMMARY

You can troubleshoot backup job issues by using the backup status and log file information that is provided on the **Configuration Monitor** page.

1. To view backup job and status, go to **Risks** > **Configuration Monitor**.
2. To update the progress bar, click the **Refresh** icon on the **Configuration Monitor** page.
3. To open the **Backup Log Viewer** window for the backup job, click the **See Log** link in the Backup Log column.
4. To update the progress bar, click **Refresh** on the **Backup Log Viewer** window.

5
CHAPTER

Network Connections Overview

Network Connections Overview

SUMMARY

A connection is a recording of a communication, including denied communications, between two unique IP addresses to a specific destination port, as detected over a specific time interval.

IN THIS SECTION

If two IP addresses communicate on a port many times within a specific time interval, only one communication is recorded. The total number of bytes that are communicated and the number of flows are included in the connection information. The connection information is stored in the database for each time interval.

Bidirectional Flow Traffic

Connections data from unidirectional flows is not recorded. Connections from bidirectional flow traffic that is from a flow source and from firewall or router deny events is recorded in these situations:

- The destination is remote, which means that it is outside of your network hierarchy. The connection is local to remote, not remote to remote.
- The destination is local, which means that it is inside your network hierarchy. The destination IP address and port that are contained in the flow record are in the asset database and the destination port is open.

Investigating Network Connections

You can monitor and investigate network device connections or do advanced searches. Complete the following tasks on the **Connections** page.

- Search connections.
- Search a subset of connections.
- Mark search results as false positives to prevent false positive events from creating offenses.
- View connection information grouped by various options.
- Export connections in XML or CSV format.
- Use the interactive graph to view connections in your network.

Visualizing Network Connection Data

SUMMARY

You can view connection data by using various chart options. By default, you can view data by using records matched over time and connection graph.

By default, the **Connections** window displays the following graphs:

- **Records Matched Over Time** graph provides time-series information that shows the number of connections based on time.
- **Connection Graph** that provides a visual representation of the connections retrieved.

TIP: If a saved search is the default, the results for that saved search are displayed.

1. Click the **Risks** tab.
2. On the navigation menu, click **Connections**.
3. Select a timeframe by selecting the **Start Time** and **End Time** parameters, or use the **View** list.

In the table, right-click any cell (except cells from the **Last Packet Time** column) for a menu to apply more filtering or to **View Connection Events**.

"Visualizing Connection Data in Time Series Charts" on page 35

Visualizing Connection Data in Time Series Charts

SUMMARY

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

If you previously saved a search to be the default, the results for that saved search display on the **Connections** page. If that search included Group By options that are selected in the Advanced View Definitions box, the Time Series chart is not available. You must clear the search criteria before you can continue.

TIP: If you use an Adblock Plus browser extension with a Mozilla Firefox web browser, the charts might not display properly. For the charts to display, you must remove the Adblock Plus browser extension. For more information about removing add-ons, see your web browser documentation.

1. Click the **Risks** tab.
2. On the navigation menu, click **Connections**, and in the charts pane, click the **Settings** icon.
3. From the **Chart Type** list, select **Time Series**.
4. From the interactive time series charts, browse through a timeline to investigate connections.
5. To refresh the information in the graph, click **Update Details**.
6. View time series charts by using one of the following methods:

Function	Use
View connections in greater detail	Using the zoom feature, you can investigate smaller time segments of the connections.

Function	Use
	• Move your mouse pointer over the chart, and then use your mouse wheel to magnify the chart (roll the mouse wheel up). • Highlight the area of the chart you want to magnify. When you release your mouse button, the chart displays a smaller time segment. Now you can click and drag the chart to scan the chart. When you magnify a time series chart, the chart refreshes to display a smaller time segment.
View a larger time span of connections	Using the zoom feature, you can investigate larger time segments or return to the maximum time range.
Scan the chart	When you magnify a time series chart, you can click and drag the chart to the left or right to scan the timeline.

"Visualizing Network Connections in a Connection Graph" on page 36

Visualizing Network Connections in a Connection Graph

SUMMARY

The connection graph provides a visual representation of the connections in your network.

The Radial Data Viewer graph that is displayed in the **Connections** window is not interactive.

By default, the graph displays the following information about your network connections:

- Only allowed connections are displayed.
- All local IP addresses are collapsed to show only leaf networks.
- All country nodes are collapsed to a node called Remote Countries.

- All remote network nodes are collapsed to one node called Remote Networks.
- Preview thumbnail view of the graph displays a portion of the main graph, which is useful for large graphs.

TIP: If you use an Adblock Plus browser extension with a Mozilla Firefox web browser, the charts might not display properly. For the charts to display, you must remove the Adblock Plus browser extension. For more information about removing add-ons, see your web browser documentation.

1. Click the **Risks** tab.
2. On the navigation menu, click **Connections**, and in the charts pane, click the **Settings** icon.
3. Using the **Chart Type** list, select **Connection Graph**.
4. Click **Connection Type** in the menu and make a selection.

   By default, the radial graph displays accepted connections. If you want to view denied connections, select Deny from the **Connection Type** list.
5. To undo node expansion, click the **Undo** option in the menu. This action collapses the last node expansion.

   If you want to undo multiple expansions, click **Undo** for each expansion.
6. Click **Download** to save the current topology as a JPEG image file or a Visio drawing file (VDX).

   IMPORTANT: To download and save the current topology as a Visio drawing file (VDX), the minimum software version you require is Microsoft Visio Standard 2010.

7. View the connections by using any of the following methods:

Function	Description
Zoom in or zoom out	Use the slider on the upper-right side of the graph to change the scale.
Distribute nodes on the graph to view additional details	Drag the node to the preferred location to distribute nodes on the graph.
Expand a network node	Double-click the node to expand and view assets for that 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.
View additional details regarding a connection	Hover your mouse over the connection line to view more details.

Function	Description
	If the connection is between a network node to a remote network or remote country, right-click to display the following **Source** and **View Flows** menus: 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 that is involved in the connection. A thicker line indicates a greater amount of data. This information is based on the number of bytes involved in the communication.
Highlight a connection path	Hover 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	Hover 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.

"Visualizing Connection Data in Pie, Bar, and Table Charts" on page 38

Visualizing Connection Data in Pie, Bar, and Table Charts

SUMMARY

You can view connections data by using a pie, bar, or table chart.

The pie, bar, and table chart options display only if the search includes Group By options, which are selected in the Advanced View Definition options.

TIP: If you use an Adblock Plus browser extension with a Mozilla Firefox web browser, the charts might not display properly. For the charts to display, you must remove the Adblock Plus browser extension. For more information about removing add-ons, see your web browser documentation.

1. Click the **Risks** tab.
2. On the navigation menu, click **Connections**.
3. Perform a search.
4. In the charts pane, click the **Settings** icon.
5. From the **Value to Graph** list, select the object type that you want to graph on the chart. Options include all normalized and custom flow parameters that are included in your search parameters.
6. From the **Chart Type** list, select the chart type that you want to view.
7. Click **Save**.

   The data does not refresh automatically, unless your search criteria is displayed to automatically display details.
8. To refresh the data, click **Update Details**.

Searching Connections in JSA Risk Manager

SUMMARY

You can search connections by 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.

IN THIS SECTION

1. Click the **Risks** tab.
2. On the navigation menu, click **Connections**.
3. Using the **Search** list, select **New Search**.
4. To load a previously saved search, use one of the following options:

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

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

d. Click **Load**.

e. In the **Edit Search** pane, select the options that you want for this search.

5. In the Time Range pane, select an option for the time range you want to capture for this search.
6. If you are finished configuring the search and want to view the results, click **Search**.
7. In the Search Parameters pane, define your specific search criteria.
8. To automatically save the search results when the search is completed, select **Save Results** when search is complete checkbox and specify a name.
9. If you are finished configuring the search and want to view the results, click **Search**. Otherwise, proceed to next step.
10. Using the Column Definition pane, define the columns and column layout you want to use to view the results.
11. Click **Search**.

"Saving Search Criteria in JSA Risk Manager" on page 40

Saving Search Criteria in JSA Risk Manager

SUMMARY

You can create a search by specifying search criteria, and you can save the search for future use.

1. Click the **Risk**s tab.
2. On the navigation menu, click **Connections**.
3. Perform a search, and click **Save Criteria**.
4. Configure values for the following parameters:

Option	Description
Search Name	Type a name that you want to assign to this search criteria.
Assign Search to Group(s)	The group that 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.

(Continued)

Option	Description
Timespan options	Choose one of the following options: Recent - Specify the time range that you want to filter. Specific Interval - Specify the date and time range you want to filter.
Include in my Quick Searches	Select the checkbox if you want to include this search in your Quick Search items, which is available from the **Search** list.
Include in my Dashboard	If you want to include the data from your saved search in your Dashboard, select the checkbox. This parameter is only displayed if the search is grouped.
Set as Default	If you want to set this search as your default search, select the checkbox.
Share with Everyone	If you want to share these search requirements with all other JSA Risk Manager users, select the checkbox.

5. Click **OK**.

"Performing a Sub-search to Refine Search Results" on page 41

Performing a Sub-search to Refine Search Results

SUMMARY

Use a sub-search to search within a set of completed search results. You can refine your search results without searching the database again. Each time that you perform a search, the entire database is queried for connections that match your criteria. This process might take an extended amount of time, depending on the size of your database.

A sub-search is not available for grouped searches or searches in progress.

1. Click the **Risks** tab.
2. On the navigation menu, click **Connections**.
3. Perform a search.
4. When your search is complete, add a filter by completing the following steps:

a. Click **Add Filter**.

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

c. Using the second list, select the modifier that you want to use for the search. The list of modifiers that display depends on the attribute that is selected in the first list.

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

e. Click **Add Filter**.

> **TIP**:
> **Original FilterCurrent Filter**
> 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.

5. Click **Save Criteria** to save the sub-search.

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 is no longer based on a data set that was previously searched.

"Saving Search Results from a Connection Search or a Sub-search" on page 42

Saving Search Results from a Connection Search or a Sub-search

SUMMARY

You can save your search results. You can save results from both connection searches and sub-searches.

1. Click the **Risks** tab.
2. On the navigation menu, click **Connections**.
3. Perform a "connection search" on page 39 or "sub-search" on page 41.
4. From the **Search Results** window, select **Search** > **Manage Search Results** and select a search result.
5. Click **Save Results**.
6. Type a name for the search results.
7. Click **OK**.

"Exporting Connections" on page 43

RELATED DOCUMENTATION

Searching Connections in JSA Risk Manager | 39

Performing a Sub-search to Refine Search Results | 41

Exporting Connections

SUMMARY

You can export connections in Extensible Markup Language (XML) or Comma Separated Values (CSV) format. Exporting connections is useful for backing up your connection information or for sharing connections with other users.

1. Click the **Risks** tab.
2. On the navigation menu, click **Connections**.
3. If you want to export the connection in XML format, select **Actions** > **Export to XML**.
4. If you want to export the connection in CSV format, select **Actions > Export to CSV**.
5. If you want to resume your activities, click **Notify When Done**.

CHAPTER 6

Network Device Configuration and Monitoring

Network Device Configuration and Monitoring

SUMMARY

In JSA Risk Manager, you can manage the efficiency of your network devices, investigate your network device configuration, investigate firewall rules, and identify security risks that are created by invalid firewall rules.

IN THIS SECTION

1. Click the **Risks** tab.
2. In the navigation pane, click **Configuration Monitor**.
3. To search your network devices, enter an IP address or hostname in the **Device IP or Name** field.
4. Double-click the device that you want to investigate.

   The rule **Event Count** column displays the firewall rule trigger frequency. A zero event count rule is displayed for one of the following reasons:

   - A rule is not triggered and might cause a security risk. You can investigate your firewall device and remove any rules that are not triggered.
   - A JSA log source mapping is not configured.
5. To search the rules, on the **Rules** toolbar, click **Search** > **New Search**.
6. To investigate the device interfaces, click **Interfaces**.
7. To investigate access control list (ACL) device rules, click **ACLs**.

Each access control list defines the interfaces that the devices on your network are communicating over. When the conditions of an ACL are met, the rules that are associated with an ACL are triggered. Each rule is tested to allow or deny communication between devices.

8. To investigate network address translation (NAT) device rules, on the toolbar, click **NAT**.

   The **Phase** column specifies when to trigger the NAT rule, for example, before or after routing.

9. To investigate the history or compare device configurations, click **History**.

   You can view device rules in a normalized comparison view or the raw device configuration. The normalized device configuration is a graphical comparison that shows added, deleted, or modified rules between devices. The raw device configuration is an XML or plain text view of the device file.

"Searching Device Rules" on page 46

Searching Device Rules

In JSA Risk Manager, you can search for rules that changed on the devices in your topology. You can also discover rule changes that occur between device configuration backups.

The results that are returned for a rule search are based on the configuration source management backup of your device. To ensure that rule searches provide up-to-date information, you can schedule device backups in your firewall policy update page.

1. Click the **Risks** tab.
2. In the navigation pane, click **Configuration Monitor**.
3. Double-click a device from the **Configuration Monitor** page.
4. On the **Rules** pane toolbar, click **Search** > **New Search**.
5. In the **Search Criteria** area, click a time range.
6. To search your device rules, choose from the following options:

Search filter	Description
Shadowed, Deleted, or Other rule status	Click a status option. By default, all status options are enabled. To search for shadow rules only, clear the **Deleted** and **Other** options.
Access control list (ACL)	Type in the **List** field.
Order number	Type a numeric value in the **Entry** field.
Source or destination	Type an IP address, CIDR address, hostname, or object group reference.
Ports or object group references	Type in the **Service** field.

Search filter	Description
	The service can include 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 might be surrounded by parenthesis. For example, the negated port information might look like ! (100-200) or !80(TCP).
Vulnerability rule information	For information defined by the IPS device, type in the **Signature** field.
Applications by adapter	Click **Select Applications**, then type an adapter or application name.

7. Click **Search**.

RELATED DOCUMENTATION

Filtering Device Rules by User or Group | 47

Filtering Device Rules by User or Group

SUMMARY

In JSA Risk Manager, you can view and filter your device rules by user or group.

Search by user or group rule interaction, and get a sense of how the typical user or group interacts in your network. Knowing your users' rule interactions in your network is helpful in discovering any errant behavior, and helps to formulate efficient rule policies in your network.

1. Click the **Risks** tab.
2. On the navigation menu, click **Configuration Monitor**.
3. From the **Device List** table, double-click the table row for your device, and view your users and groups.

   Group results are displayed with hyperlinks to view the users in the selected group.
4. From the **Rules** pane, click **Search** > **New Search**.

5. Click **Select Users/Groups**.
6. Type a partial or full search term or leave the **User/Group Name** field empty, and then click **Search**.
7. Select the user or group name in the **Search Results** field, and then click **Add**, to add your selections to the **Selected Items** box.
8. Click **OK**, and then click **Search**.

   Use the rule information to establish benchmarks or profiles for user rule interaction, which can be used to optimize rule policies in your network.

"Comparing the Configuration of your Network Devices" on page 48

RELATED DOCUMENTATION

Network Risk Assessment | 86

Comparing the Configuration of your Network Devices

In JSA Risk Manager, 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.

Common configuration types can include the following items:

- **Standard Element Document** - Standard Element Document (SED) files are XML data files that contain information about your network device. Individual SED (standard element document) files are viewed in their raw XML format. If a SED (standard element document) file is compared to another SED (standard element document) 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.

Depending on the information that the adapter collects for your device, several other configuration types might be displayed. These files are displayed in plain text view when double-clicked.

1. Click the **Risks** tab.
2. On the navigation menu, click **Configuration Monitor**.
3. Double-click any device to view the detailed configuration information.
4. Click **History** to view the history for this device.
5. The following steps explain how to compare two configurations on a single device:

   a. Select a primary configuration.

   b. Press the **CTRL** key and select a second configuration for comparison.

   c. In the **History** pane, click **Compare Selected**.

If the comparison files are standard element documents (SEDs), then the **Normalized Device Configuration Comparison** window shows rule differences between the backups.

When you compare normalized configurations, the color of the text shows the following device updates:

- A green dotted outline shows a rule or configuration that was added to the device.
- A red dashed outline shows a rule or configuration that was deleted from the device.
- A yellow solid outline shows a rule or configuration that was modified on the device.

d. To view the raw configuration differences, click **View Raw Comparison**.

If the comparison is a configuration file or another backup type, then the raw comparison is displayed.

6. The following steps explain how to compare two configurations on different devices:
   a. Select a primary configuration from a device.
   b. Click **Mark for Comparison**.
   c. From the navigation menu, select **All Devices** to return to the device list.
   d. Double-click the device to compare and click **History**.
   e. Select a configuration that you want to compare with the marked configuration.
   f. Click **Compare with Marked**.
   g. To view the raw configuration differences, click **View Raw Comparison**.

"Adding or Deleting a Device in JSA Risk Manager" on page 49

Adding or Deleting a Device in JSA Risk Manager

SUMMARY

You can add individual network devices and adapters. Delete devices when you no longer need them.

1. Click the **Admin** tab.
2. In the **Plug-ins** section, click **Risk Manager** > **Configuration Source Management**.

3. Click **Add Device**.
4. Configure values for the following parameters:

Option	Description
IP Address	Type the management IP address of the device.
Adapter	Select the adapter that you want to assign to this device.
Back up now	Retrieves device information from adapters and adds the device to the backup job. Includes the device in the topology.

5. Click **OK**.
6. To delete a single or multiple devices, go to the **Actions** menu in the **Configuration Source Management** window, and click **Device Management**.
   - To delete one device, select the device and click **Remove**.
   - To delete multiple devices, hold down the **CTRL** key and select all necessary devices. Click **Remove**.

   The device or devices are removed from the Configuration Monitor, Configuration Source Management, and the topology.

"Backing up a Device to get its Configuration Data" on page 50

"Configuring Credentials for JSA Risk Manager" on page 52

RELATED DOCUMENTATION

Protocol Configuration for Network Devices | 56

Configuring Protocols in JSA Risk Manager | 57

Backing up a Device to get its Configuration Data

SUMMARY

The process of backing up a device to obtain a device configuration can be completed for a single device in the device list, or you can back up all devices simultaneously. After you configure credential sets and address sets to access network devices, you must back up your devices to download the device configuration, so the device information is included in the topology.

1. Click the **Admin** tab.
2. In the **Plug-ins** section, click **Risk Manager** > **Configuration Source Management**.
3. Select the device that you want to back up.
4. On the toolbar, click **Backup** to back up the selected device. To select multiple devices, hold down the **CTRL** key and select all necessary devices.
5. To obtain the configuration for all devices, click **Backup All** in the navigation pane.
6. Click **Yes**.
7. If necessary, click **View Error** to view the details of an error. After correcting the error, click **Backup All** in the navigation pane.

RELATED DOCUMENTATION

Viewing Backup Job Status and Logs | 31

Protocol Configuration for Network Devices | 56

Configuring Protocols in JSA Risk Manager | 57

Credentials for Accessing Device Configurations

SUMMARY

In JSA Risk Manager, credentials are used to access and download the configuration of devices such as firewalls, routers, switches, or IPSs.

IN THIS SECTION

You can configure credentials, protocols, and schedules in the Configuration monitor in JSA 7.4.1, fix pack 1 and later. For previous versions of JSA, see "Network Device Management" on page 15. For more information on this change, see *Juniper Secure Analytics Risk Manager: Adobe Flash End of Life and Changes to Configuration Source Management (CSM)*.

Administrators use the Configuration Monitor to input device credentials that give JSA Risk Manager access to specific devices. Individual device credentials can be saved for a specific network device. If multiple network devices use the same credentials, you can assign credentials to a group.

You can assign different devices in your network to network groups, to group credential sets 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 a set of credentials.

For example, the firewalls in your organization might have the same username and password. If so, the credentials that are associated with all the address sets for all the firewalls are used to back up 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. For a list of required adapter credentials, see the *Juniper Secure Analytics Risk Manager Adapter Configuration Guide*.

Configure JSA Risk Manager to Prioritize How Each Network Group is Evaluated

The network group that is first on the list has the highest priority. The first network group that matches the configured IP address are included as candidates when you are backing up a device. A maximum of three credential sets from a network group are considered.

For example, if your network groups have the following composition:

- Network group 1 contains two credential sets.
- Network group 2 contains two credential sets.

JSA Risk Manager compiles a maximum of three credential sets, so the following credential sets are used:

- Both credential sets in network group 1 are used because network group 1 is higher in the list.
- Only the first credential set in the network group 2 is used because only three credential sets are required.

When a credential set is used to successfully access a device, JSA Risk Manager uses that same credential set for subsequent attempts to access the device. If the credentials on that device change, the authentication fails and for the next authentication attempt, JSA Risk Manager compiles the credentials again to ensure success.

Configuring Credentials for JSA Risk Manager

SUMMARY

Administrators must configure credentials to allow JSA Risk Manager to connect to devices in the network.

You can configure credentials, protocols, and schedules in the Configuration monitor in JSA 7.4.1, fix pack 1 and later. For previous versions of JSA, see "Network Device Management" on page 15. For more information on this change, see *Juniper Secure Analytics Risk Manager: Adobe Flash End of Life and Changes to Configuration Source Management (CSM)*.

1. On the **Risk** tab, click **Configuration Monitor**.
2. In the navigation menu, click **Credentials**.
3. Select **Add** from the toolbar.
4. Type a **Name** for the new credentials.
5. In the **Address Sets** section, click **Add**.
6. In the **Add Address** field, type the IP address or CIDR range that you want to apply to the network group, then click **OK**.

   TIP:
   10.100.20.0-10.100.20.2401.1.1*1.1.1.*

7. In the **Credential Sets** pane, click **Add**.
8. Type a name for the new credential set, configure values for the parameters, and then click **Save**.

   TIP:
   Increase PriorityDecrease Priority

"Discovering Devices in your Network" on page 53

Discovering Devices in your Network

SUMMARY

In JSA Risk Manager, use the **Device Discovery** screen in the Configuration Monitor to add, edit, and run a defined discovery.

When you run a Discover with SNMP device discovery, any device that is not supported but responds to SNMP is added through the Generic SNMP adapter.

1. Access the **Device Discovery** screen by using the following steps:

a. Click the **Risks** tab.

b. Click **Configuration Monitor** > **Device Discovery** in the **Risk Manager** pane.

2. Add a device to JSA Risk Manager by using the following steps:

   a. On the navigation pane, click **Add**.

   b. Select a **Discovery Type** on the **Discovery Profile Configuration** screen. The following lists the methods that you can use to add a network device:

      - Discover with SNMP
      - Discover from Check Point OPSEC
      - Discover from Defense Center
      - Discover from NSM
      - Discover from SiteProtector
      - Discover from Check Point HTTPS

   c. Enter the **Device IP**, **Username**, and **Password** for the device.

   d. You can also search for devices in the network from the defined IP address with the Discover with SNMP option. Select the **Crawl the network from the addresses defined above** checkbox.

   e. To run the discovery immediately, click **Run Discovery Now**. Alternatively, you can save the profile configuration and run the discovery another time.

   f. Click **Save**.

3. Edit a device that is listed in the **Discovery list** by using the following steps:

   a. Select a device on the **Discovery list**, and click **Edit** on the navigation pane.

   b. Edit the discovery details, and select **Run Discovery Now** to run the discovery immediately. Alternatively, you can save the profile configuration and run the discovery another time.

4. To search for a device, enter the IP address/name in the **Device IP** field and click the **Search** icon.

5. To delete a device discovery job, select a device on the **Discovery List**, and click **Delete** on the navigation pane.

6. To monitor recent activities or troubleshoot devices, use the **Recent Activity** page.
   You can view all information that is related to the activity, including the type, state, and progress, or investigate the log.

Log Source Mapping in JSA

IN THIS SECTION

To monitor the trigger frequency of firewall rules and enable topology event searches, JSA Risk Manager identifies JSA log sources.
By understanding firewall rules, you can maintain firewall efficiency and prevent security risks.

A maximum of 255 devices can be mapped to a log source in JSA Risk Manager, but devices can have multiple log sources.

Log Source Mapping Display Options

If you configured your network device as a JSA log source, the **Configuration Monitor** page displays one of the following entries in the **Log Source** column:

- **Auto-Mapped** - If JSA Risk Manager identifies and maps the log source to the device automatically.
- **Username** - If an administrator manually added or edited a log source.
- **Blank** - If JSA Risk Manager is unable to identify a log source for the device, the **Log Source** column shows no value. You can manually create a log source mapping.

For more information about configuring log sources, see the *Juniper Secure Analytics Configuring DSMs Guide*.

Creating or Editing a Log Source Mapping

SUMMARY

If JSA Risk Manager cannot identify a log source in JSA, you can configure a log source mapping.

1. Click the **Risks** tab.
2. In the navigation pane, click **Configuration Monitor**.
3. Click the device without a log source mapping.

4. On the toolbar, click **Action** > **Log Source Mapping** > **Create/Edit Log Source Mapping**.
5. In the **Log Source Groups** list, select a group.
6. In the **Log Sources** list, select a log source and click (**>**).
7. Click **OK**.

RELATED DOCUMENTATION

Firewall Rule Event Counts of Check Point Devices | 64

RELATED DOCUMENTATION

Firewall Rule Event Counts of Check Point Devices | 64

Protocol Configuration for Network Devices

SUMMARY

For JSA Risk Manager to communicate with devices, you must define the communication method (protocol) required for your network devices.

IN THIS SECTION

You can configure credentials, protocols, and schedules in the Configuration monitor in JSA 7.4.1, fix pack 1 and later. For previous versions of JSA, see "Network Device Management" on page 15. For more information on this change, see *Juniper Secure Analytics Risk Manager: Adobe Flash End of Life and Changes to Configuration Source Management (CSM)*.

JSA Risk Manager provides default protocol configuration for your system. You can define protocols to allow JSA 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 *Juniper Secure Analytics Risk Manager Adapter Configuration Guide*.

JSA 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 protocol sets and address sets for your devices.

Protocol sets are 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.

Configuring Protocols in JSA Risk Manager

SUMMARY

You define protocols to obtain and update device configuration.

You can configure credentials, protocols, and schedules in the Configuration monitor in JSA 7.4.1, fix pack 1 and later. For previous versions of JSA, see "Network Device Management" on page 15. For more information on this change, see *Juniper Secure Analytics Risk Manager: Adobe Flash End of Life and Changes to Configuration Source Management (CSM)*.

1. On the **Risk** tab, click **Configuration Monitor**.
2. In the navigation menu, click **Protocols**.
3. Select **Add** from the toolbar.
4. Type a **Name** for the protocol set.
5. In the **Address Sets** section, click **Add**.
6. In the **Add Address** field, type the IP address or CIDR range that you want to apply to the network group, and then click **OK**.

   TIP: You can use IP4 or IP6 address or CIDR ranges.

7. Select the checkbox for each protocol you want to enable.

   TIP:
   Increase PriorityDecrease Priority

8. Select a protocol to configure its relevant properties.

   You can configure the following values for the protocol parameters:

Table 4: Configuring 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 following options are available: **Auto** - This option automatically detects the SSH version to use when communicating with network devices. **1** - Use SSH1 when communicating with network devices. **2** - Use SSH2 when communicating with network devices.
Telnet	Type the port number that you want the Telnet protocol to use when it is communicating with and backing up network devices. The default Telnet protocol port is 23.
HTTPS	Type the port number that you want the HTTPS protocol to use when it is communicating with and backing up network devices. The default HTTPS protocol port is 443.
HTTP	Type the port number that you want the HTTP protocol to use when it is communicating with and backing up network devices. The default HTTP protocol port is 80.
SCP	Type the port number that you want the SCP protocol to use when it is communicating with and backing up network devices. The default SCP protocol port is 22.
SFTP	Type the port number that you want the SFTP protocol to use when it is communicating with and backing up network devices. The default SFTP protocol port is 22.

Table 4: Configuring Protocol Parameters *(Continued)*

Protocol	Parameter
FTP	Type the port number that you want the FTP protocol to use when it is communicating with and backing up network devices. The default SFTP protocol port is 22.
TFTP	The TFTP protocol does not have any configurable options.
SNMP	Configure the following parameters: **Port** - Type the port number that you want the SNMP protocol to use when it is communicating 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 that you want to use to authenticate SNMP traps. **V3 Encryption** - Select the protocol that you want to use to decrypt SNMP traps.

9. Click **Save**.

TIP:
Increase PriorityDecrease Priority

RELATED DOCUMENTATION

Adding or Deleting a Device in JSA Risk Manager | 49

Backing up a Device to get its Configuration Data | 50

Schedules for Discovery and Backup

SUMMARY

Create schedules or edit existing schedules for regular neighbor discovery and device backup. You can create only one discovery schedule at a time, but you can create multiple backup schedules.

IN THIS SECTION

You can configure credentials, protocols, and schedules in the Configuration monitor in JSA 7.4.1, fix pack 1 and later. For previous versions of JSA, see "Network Device Management" on page 15. For more information on this change, see *Juniper Secure Analytics Risk Manager: Adobe Flash End of Life and Changes to Configuration Source Management (CSM)*.

You can create a schedule, or edit or delete an existing schedule.

Schedules that have a single frequency display the frequency type:

- Once
- Daily
- Weekly
- Monthly
- Cron

If a schedule has multiple frequencies, the frequency is displayed as Multiple.

Configuring a Schedule

SUMMARY

You can create schedules or edit an existing schedule for regular device discovery and backup.

You can configure credentials, protocols, and schedules in the Configuration monitor in JSA 7.4.1, fix pack 1 and later. For previous versions of JSA, see "Network Device Management" on page 15. For more information on this change, see *Juniper Secure Analytics Risk Manager: Adobe Flash End of Life and Changes to Configuration Source Management (CSM)*.

1. On the **Schedules** page, click **Add** to create a new schedule, or select an existing schedule and click **Edit**.
2. Type a unique **Name** for the schedule.
3. Select a **Group** from the drop-down list, or type a new **Group** name.
4. Select a schedule **Type**:

Option	Description
Backup	Backs up discovered devices.
Discovery	Updates the telemetry for devices and adds newly discovered devices. 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.

> **NOTE**:
> **BackupType**

5. If you are creating a discovery schedule and want to add newly discovered devices to the product, select **Crawl**.
6. If you are creating a backup schedule, click **Edit** to add or remove devices to be targeted for backup. Then, perform one of the following actions:
   - Use the arrows to move devices from the **Available Devices** list to the **Selected Devices** list.
   - Select **Search** to configure a search to dynamically target devices based on IP address, operating system, model, or hostname.

> **TIP**: You can search for Admin or Interface IP addresses by using a comma-separated list of IP addresses and CIDR ranges.

7. Select a Trigger to specify the frequency you want the schedule to run.

   You can select from the following frequency types:
   - Once
   - Daily
   - Weekly
   - Monthly
   - Cron

> **TIP**: Cron expressions that repeat more than once per hour are not accepted.

8. Click **Save**.
9. To run a schedule immediately instead of waiting for its start time, click **Run Now**.

CHAPTER 7

Firewall Rule Event Counts of Check Point Devices

Firewall Rule Event Counts of Check Point Devices

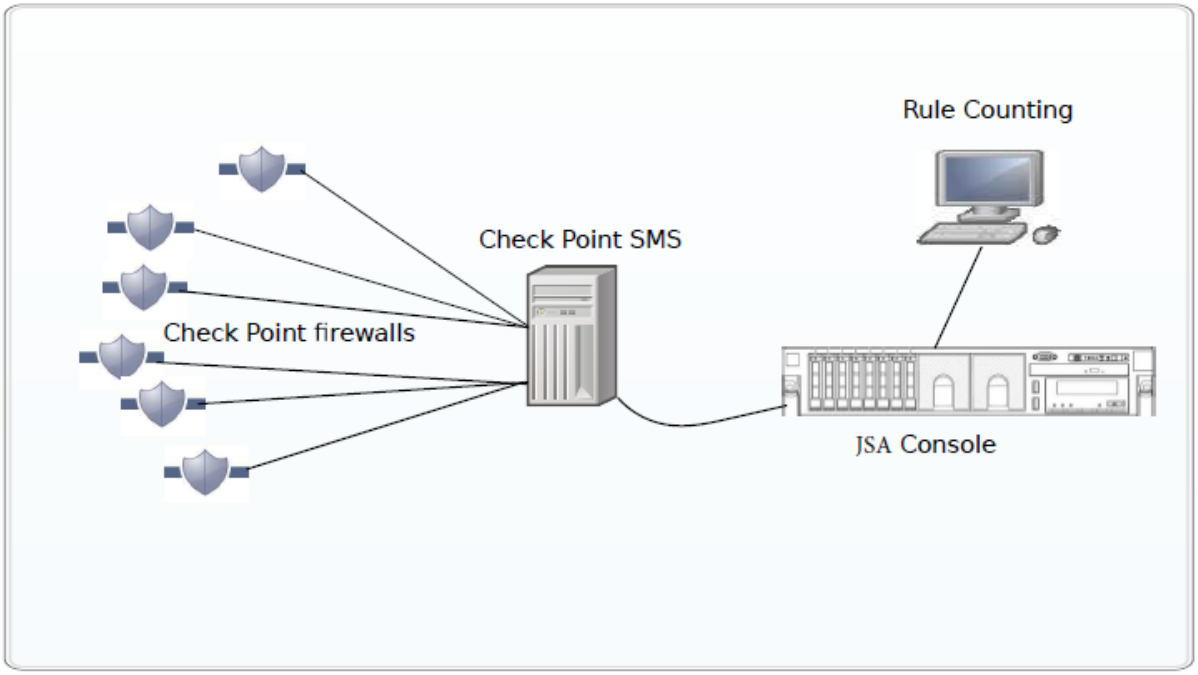
SUMMARY

In JSA Risk Manager, you can monitor the firewall rule event counts of your Check Point devices by integrating with the Check Point SMS. You can view these rule interactions in JSA Risk Manager, and use rule reports to manage the rule policy effectiveness of your network.

IN THIS SECTION

In the following image, JSA receives and processes rule event logs from Check Point firewall devices through the SMS.

Figure 1: Check Point rule counting



Scenario - Implementing Check Point firewall rule monitoring in JSA

You are a network systems administrator with responsibility for network security in an organization that uses Check Point to implement its network security policies. The network includes several Check Point firewalls that are managed from a Check Point Security Management Server (SMS).

You want to view reports on rule usage daily so that you have more visibility on your rule implementation.

You need to configure a connection between your Check Point SMS and JSA so that JSA receives rule event logs from Check Point firewall devices. JSA processes this rule event log information and displays rule event information for all devices that are managed by Check Point firewalls. From the JSA rules table, you can analyze the usage and effectiveness of the firewall rules by monitoring event counts, and fine-tune your rules for optimal performance.

Use the rule information to do the following tasks:

- View most and least used rules.
- Assess the practicality of rules that are triggered infrequently.
- View rules that might be blocking network access unnecessarily.

- View rules that are triggered excessively, and place a load on your network bandwidth.
- View detailed events.
- Schedule reports.

For more information, see "Configuring Rule Event Count Setup in JSA Risk Manager" on page 66.

Configuring Rule Event Count Setup in JSA Risk Manager

SUMMARY

You can set up rule count to monitor rule interactions and generate rule reports.

Download the most recent adapter bundle from Juniper Downloads, and install it on your JSA managed host.

1. Configure OPSEC applications in the Check Point SmartDashboard.
2. Create a log source in JSA.
3. Configure Configuration Source Management (CSM) in JSA Risk Manager. Discover and backup devices in Configuration Source Management.
4. Complete the configurations to view rule counting.

"Configuring OPSEC Applications in the SmartDashboard" on page 66

Configuring OPSEC Applications in the SmartDashboard

SUMMARY

Create and configure two OPSEC applications in your Check Point SmartDashboard, which facilitates the transfer of log files between Check Point and JSA.

Create two OPSEC (Open Platform for Security) applications. One needs a client entity property of CPMI (Check Point Management Interface) for JSA Risk Manager. The other needs a client entity property of LEA (Log Export API) for the JSA Risk Manager log source.

1. From the **Manage** menu on the toolbar, click **Servers and OPSEC Applications**.
2. Click **New** > **OPSEC Application**.
3. In the **Name** field, type a name for the application.
4. From the **Host** list, select a host, or click **New** to add a host.
5. Under **Client Entities**, select the **CPMI** checkbox .

   This option is required for JSA Risk Manager Configuration Source Management (CSM).
6. Click **Communication**.
7. In the **One-time password** field, type a password and then confirm it.

   The password is used several times during setup, and you need to reuse it so that JSA can use a security certificate from Check Point.
8. Click Initalize.

   The **Trust state** changes to Initialized but trust not established.
9. Click **Close**.
10. To populate the **DN** field in the **Secure Internal Communication** section, click **OK**.
11. To view the populated **DN** field, select your **OPSEC Application**, and click **Edit**

    The **DN** field is now populated. This information is used for the **Application Object SIC Attribute (SIC Name)** and the **SIC Attribute (SIC Name)** when you set up the log source and Configuration Source Management in JSA.
12. Create the second OPSEC application to use with the log source.

    Follow steps 1-11 for creating the first OPSEC Application, with two exceptions:

    - For the **Name** field in step 3, use a different name from the first OPSEC application.
    - For **Client Entities** in step 5, select the **LEA** checkbox.

    Make sure that the **Trust state** displays Initialized but trust not established.

    > **TIP**: Use the same one-time password for this OPSEC application to avoid any confusion with passwords.
13. In SmartDashboard, close all windows until you get back to the main **SmartDashboard** window.
14. From the **Policy** menu on the toolbar, click **Install**.
15. Click **Install on all selected gateways if it fails do not install on gateways of the same version**.

"Configuring the Check Point Log Source" on page 68

Configuring the Check Point Log Source

SUMMARY

Configure the log source in JSA to get a certificate from Check Point and to receive log information.

1. Log in to JSA.
2. On the navigation menu, click **Admin**.
3. Click **Data Sources**.
4. Click the **Log Sources** icon, and then click **Add**.
5. Configure the following values:

Table 5: Configuring Check Point log source parameters

Parameter	Description
Log Source Name	The identifier for the log source.
Log Source Description	The description is optional.
Log Source Type	Select **Check Point FireWall-1**.
Protocol Configuration	Select **OPSEC/LEA**.
Log Source Identifier	IP address of your SMS
Server IP	Type the IP address of your SMS.
Server Port	Use port 18184.
Use Server IP for Log Source	Do not select this checkbox.
Statistics Report Interval	Default of 600.

Table 5: Configuring Check Point log source parameters *(Continued)*

Parameter	Description
Authentication Type	From the list, select **sslca**.
OPSEC Application Object SIC Attribute (SIC Name)	From the Check Point SmartDashboard, click **Manage** > **Servers and OPSEC Applications**. Select the OPSEC application that has the client entity property of LEA, and click **Edit**. Copy and paste the entry from the **DN** field into the **OPSEC Application Object SIC Attribute (SIC Name)** field.
Log Source SIC Attribute (Entity SIC Name)	Use the entry that you entered in the **OPSEC Application Object SIC Attribute (SIC Name)** field, remove the text from the `CN= property value`, and make the following edits: For the **CN=** property value, use **cp_mgmt**. The following examples show an OPSEC Application DN and OPSEC Application Host, which is used to create the Entity SIC Name: OPSEC Application DN: **CN=cpsmsxxx,O=svxxx-CPSMS..bsaobx** OPSEC Application Host: **Srvxxx-SMS** Use text from the OPSEC Application DN and the OPSEC Application Host to form the **Entity SIC Name**: **CN=cp_mgmt,O=svxxx-CPSMS..bsaobx** The **Entity SIC Name** in this configuration is based on a Gateway to Management Server setup. If your SMS address is not used as a gateway, use the Management Server configuration for the **Entity SIC Name**, which is represented by the following text: `CN=cp_mgmt,O=<take_O_value_from_DN_field>`
Specify Certificate	Don't select this checkbox.
Certificate Authority IP	Type the IP address of the SMS.
Pull Certificate Password	The password that you specified for the **OPSEC Applications Properties** in the **One-time password** field of the **Communication** window.

Table 5: Configuring Check Point log source parameters *(Continued)*

Parameter	Description
OPSEC Application	The name that you specified in the **Name** field from the **OPSEC Applications Properties**.
Enabled	Select this checkbox to enable the log source. By default, the checkbox is selected.
Credibility	The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases when multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the **Target Event Collector** to use as the target for the log source.
Coalescing Events	Enables the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings properties in JSA. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Store Event Payload	Enables the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings properties in JSA. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

6. Click **Save**.
7. On the **Admin** tab, click **Deploy Changes**.

If you find that changes are implemented automatically, it's still good practice to click **Deploy Changes**.

Check that trust is established for the OPSEC application that has the client entity property of LEA, by viewing **Trust State** in the **Communication** window of **OPSEC Application Properties**.

The configuration of the log source is complete.

For more information about configuring log sources, see the *Juniper Secure Analytics Configuring DSMs Guide*.

"Establishing Secure Communication Between Check Point and JSA " on page 71

Establishing Secure Communication Between Check Point and JSA

SUMMARY

Configure Configuration Source Management in JSA to connect to the Check Point SMS. Add the OPSEC Application details from the SmartDashboard, and request a security certificate from Check Point.

Configure the OPSEC application details in Configuration Source Management and set up the certificate exchange. After the configuration is complete, use Configuration Source Management to discover the new entry.

1. Log in to JSA as an administrator.
2. On the navigation menu, click **Admin**.
3. Click **Apps** or scroll down to find the **Configuration Source Management** icon.
4. Click the **Configuration Source Management** icon.
5. On the navigation menu, click **Credentials**.
6. From the **Network Groups** pane, click the (**+**) symbol.
7. Type a name for the network group.
8. In the **Add address (IP, CIDR, Wildcard, or Range)** field, type the IP address of your SMS.
9. Click (**+**) to add the IP address.
10. Type your SMS SmartDashboard username and password.

    To configure the OPSEC fields, use the information from the **OPSEC Application Properties** window of the SmartDashboard, where you selected the **CPMI** checkbox for the client entity.
11. From the **DN** field, copy and paste this information into the **OPSEC Entity SIC Name** field.
12. Edit the entry that you pasted into the **OPSEC Entity SIC Name** by replacing the CN= property value with: cp_mgmt_*hostname* where <*hostname*> is the **Host** name that is used for the OPSEC application **Host** field.

    The following examples show an OPSEC Application DN and OPSEC Application Host, which is used to create the Entity SIC Name:

    - OPSEC Application DN: **CN=cpsmsxxx,O=svxxx-CPSMS..bsaobx**
    - OPSEC Application Host: **Srvxxx-SMS**

TIP: Use text from the OPSEC Application DN and the OPSEC Application Host to form the **Entity SIC Name**:

The **Entity SIC Name** is `CN=cp_mgmt_Srvxxx-SMS,O=svxxx-CPSMS..bsaobx`

The **Entity SIC Name** in this configuration is based on a Gateway to Management Server setup. If your SMS IP address is not used as a gateway, use the Management Server configuration from the table:

Table 6: Entity SIC Name Formats

Type	Name
Management Server	`CN=cp_mgmt,O=<take_O_value_from_DN_field>`
Gateway to Management Server	`CN=cp_mgmt_<gateway_hostname>,O=<take_O_value from_DN_field>`

13. From the **DN** field, copy the entry, and paste this information into the **OPSEC Application Object SIC Name** field.
14. Click **Get Certificate**.
15. Enter the SMS IP address in the **Certificate Authority IP** field.
16. Enter the one-time password in the **Pull Certificate Password** field.

    The one-time password is from the **Communication** window in the **OPSEC Application Properties** of the SmartDashboard, where you selected the **CPMI** checkbox for the client entity.
17. Click **OK**.

    If successful, the **OPSEC SSL Certificate** field is populated and disabled .

    Verify that the **Trust State** property, in the **Communication** window of the **OPSEC Application Properties**, changes to Trust established.

    The credentials are set up, and now you can run a discovery.
18. On the navigation menu, click **Discover From Check Point SMS**.
19. In the **CPSMS IP Address** field, type the IP address of the SMS.

"Initializing Rule Counting for Check Point" on page 73

Initializing Rule Counting for Check Point

SUMMARY

Complete the final configurations in JSA and Check Point to tie the configurations together so that you can use rule counting in JSA.

When trust is established and the policies are updated, you can view rule counting in JSA. JSA Risk Manager needs approximately 1 hour to process counts.

1. In JSA, click **Risks** > **Configuration Monitor**
2. Double-click a Check Point device to view the rule counting.
   - Verify that the log source is auto mapping by looking in the **Log Sources** column.
   - Look for the **Event Count** column of the rules table.

8
CHAPTER

Network Topology

Network Topology

SUMMARY

In JSA Risk Manager, you can use the topology model graph to view, filter, and investigate the physical connectivity of your network.

IN THIS SECTION

The network topology graph is generated from configuration information that is obtained from devices such as firewalls, routers, switches, and Intrusion Prevention System (IPS) systems. You can hover over connection lines to display network connection information. You can filter the topology by searching for potential attack paths on allowed protocols, ports, or vulnerabilities. You can view the traffic flow between devices or subnets, and you can view device rules.

You can use the topology graph to complete the following tasks:

- Visualize specific network paths and traffic direction for advanced threat analysis.
- Incorporate passive IPS security maps into the topology graph.
- Group devices to organize and simplify the view.
- Add devices to groups, and remove devices from groups.
- Reposition icons in the graph by using your mouse.
- Save topology graph layouts.
- Rename devices and groups.

- Create and save search filters for your network topology that is based on protocols, ports, or vulnerabilities.
- View detailed connection information between devices and subnets.
- View device rules on topology node connections with the allowed ports and protocols.
- View Network Address Translation (NAT) devices, NAT indicators, and information about NAT mappings.
- View virtual Network security devices that have multiple-contexts.
- Configure subnet color coding to indicate vulnerability status of assets in the subnets on your topology graph.

When you search and view the allowed ports and protocols between devices, you can see only connections that use TCP, UDP, and ICMP protocols in the topology graph.

Topology Searches

SUMMARY

Use the topology search feature to view and investigate various elements of your network infrastructure.

Topology searches appear in a tabbed view, and each topology search opens its own tab. The topology search results are cached for improved topology retrieval, resulting in faster processing time. The searches remain running in the background, so you can use other features of JSA Risk Manager.

Investigating Elements in your Network Infrastructure

SUMMARY

You can use the search feature to filter your topology view, and zone in on network paths, hosts, subnets, and other network elements. You can refine your search down to the port or protocol level, for example you can search for potential attack paths on allowed protocols or ports.

IN THIS SECTION

1. Click the **Risks** tab, and then click **Topology** on the navigation menu.
2. Click **Actions**.
3. Enter your search criteria in the **Search Criteria** pane.

   The following table describes examples of search options that you can use:

Search option	Description
Hosts	If you search for a host, all devices that communicate with that host are displayed. If the host does not match an interface on a device, but is included in the subnet, that subnet and all connected devices are displayed.
Networks	Search for a single CIDR, for example, **10.3.51.200/24**. If you're searching for multiple CIDRs, ensure that the CIDRs are valid and are separated by a comma, for example, **10.51.0.0/24,10.51.01/24**.
Paths	A path search displays the traffic direction, fully or partially allowed protocols, and device rules. If you select any path search criteria other than the mandatory source and destination IP addresses, a path summary is displayed. Refine your path search by searching for applications, vulnerabilities, and users or user groups.

4. To search events, right-click the device or subnet that you want to investigate.
5. To search flows, right-click any subnets that you want to investigate.

NAT Indicators in Search Results

SUMMARY

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

IN THIS SECTION

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

Table 7: 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 or ports, 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 or ports, if applicable.
Phase	The routing phase when the translation was applied. Translations are applied either pre- or post-routing.

Adding an Intrusion Prevention System (IPS)

SUMMARY

If your **Configuration Source Management** list includes an intrusion prevention system (IPS) device, you can add an IPS to connections between device-to-subnet nodes, and between device-to-device nodes. Adding an IPS connection is useful to determine the location of the IPS if the device is passive.

1. Click the **Risks** tab.
2. On the navigation menu, click **Topology**.
3. Move your mouse pointer over the connection line that links a device node and a subnet node.
4. Right-click the connection line, select **Add IPS**.
5. Select the device and interfaces to add from the following lists:

Option	Description
Place IPS	Select a placement from the list.
Connect IPS interface	Select an interface to connect to the device. If you have multiple devices, then you need to select a device (see next option).
To device	Select the device that you want to connect to the IPS. This option is available if you have multiple devices.
Connect IPS interface	Select an interface to connect to the subnet.

6. Using the lists, select the device and interfaces to add the IPS connection to your topology, and then click **OK**.

   If you want to add an IPS to a device that is in a group, expand the group to add the IPS.
7. To remove an IPS, right-click the connection line, select **Remove IPS**, and click **OK**.

Use Case: Offense Attack Path Visualization

SUMMARY

Offenses in JSA Risk Manager are events that are generated by the system to alert you about a network condition or event.

IN THIS SECTION

Attack path visualization ties offenses with topology searches. This visualization allows security operators to view the offense detail and the path the offense took through your network. The attack path provides you with a visual representation. The visual representation shows you the assets in your network that are communicating to allow an offense to travel through the network. This data is critical during auditing to prove that you monitor for offenses, but also proves that the offense does not have an alternative path in your network to a critical asset.

Viewing the Attack Path of an Offense

SUMMARY

The attack path of the offense shows the source, destination, and associated devices.

1. Click the **Offenses** tab.
2. On the navigation menu, click **All Offenses**.
   The **All Offenses** page displays a list of offenses that are on your network. Offenses are listed with the highest magnitude first.
3. Double-click an offense to open the offense summary.
4. On the **Offenses** toolbar, click **View Attack Path**.

Configuring Color Coding of Subnets to Indicate Vulnerability Status

SUMMARY

Use subnet color coding to highlight vulnerability-related information about assets in the subnets on your topology graph.

1. Click the **Risks** tab.
2. On the navigation menu, click **Topology**.
3. Click **Actions** > **Properties** > **Edit** to configure subnet color coding.
4. Select one of the following color-coding options:

Option	Description
No color coding of subnets	If you don't want to use color coding, click **No color coding of subnets**. All of the subnet icons are a gray color when you choose this option.
Highest Aggregated CVSS score (Risk score) for any asset in a subnet	Type a value for each color. When the risk score of any asset in a subnet exceeds the highest matching **Greater than** value, the color of the subnet icon changes to that color. For example, if you configure a value of 14 for the red color, the subnet icon changes to red when any asset in that subnet has a risk score greater than 14. Only the color for the highest matching value displays. The risk score is calculated by using the Common Vulnerability Scoring System (CVSS) and includes any risk adjustments that are made by JSA Risk Manager. You can view the **Aggregated CVSS** score for an asset on the **Assets** tab.
Number of vulnerabilities for any asset in a subnet	Type a value for each color. When the total number of vulnerabilities exceeds the highest matching **Greater than** value, the color of the subnet icon changes to the color that represents that value.
Impact of vulnerabilities for any asset in a subnet	Select a vulnerability impact for each color. When any asset in a subnet matches the highest listed impact, the color of the subnet icon changes to that color.

Option	Description
	For example, you might select red to represent system loss. The color of the subnet icon changes to red when any asset in the subnet is impacted by system loss because of a vulnerability. If you select the same vulnerability impact for two different colors, the color in the highest position is applied to the subnet icon when an asset is affected by the vulnerability impact.

5. To update the vulnerability status of assets in your topology when a scan completes or other vulnerability-related changes occur, you can take one of the following steps:
   - Reset your topology by clicking **Actions** > **Layout** > **Reset Layout**.
   - Clear your browser cache, and then refresh your browser.

> **NOTE**: The subnet color in the topology graph appears in a lighter shade.

RELATED DOCUMENTATION

Network Links | 82

Creating a Network Link | 83

Network Links

SUMMARY

Network links connect your core network to network branches that are not directly connected to your network or that you don't control directly.

IN THIS SECTION

- Creating a Network Link | 83

Use network links in JSA Risk Manager to address gaps in your network topology diagram. Network links are used where the true connection is through network equipment that can't be directly modeled in the normal JSA Risk Manager way. For example, network links display the WAN connectivity between your

core and branch networks that uses equipment that is owned by your network service provider when JSA Risk Manager can't retrieve the configuration.

You can also use network links to connect to disparate network sites that you're responsible for, but are owned by another corporate or government entity. For example, you can create a network links topology entry to represent a Multiprotocol Label Switching (MPLS) backbone that is controlled by your network service provider.

After you create network links to connect the branches in the topology, you can run path searches that show network paths across the links.

Creating a Network Link

SUMMARY

Create network links in the JSA Risk Manager topology to provide access to network branches that are not connected to your core network, but that are accessible through an Internet connection.

1. On the **Risks** tab, click **Topology**.
2. Click **Actions** > **Network Link**.
3. Type a **Display Name** for the link.
4. Type the **Admin IP** address of the core network node that you want to use to connect to the remote network, and click **Select Interface**.
5. Select the interface that you want to connect from, and click **OK**.
6. Type the **Admin IP** address of the network branch node that you want to connect to, and click **Select Interface**.
7. Select the interface that you want to connect, and click **OK**.
8. Click **OK**.

TIP:
TopologyConfiguration Monitor
To delete a network link from the topology, right-click the link and select **Delete**. Network links are also deleted if you delete all devices in the **Configuration Monitor**.

Configuring an Internet Override to Identify Internet Edge Devices

SUMMARY

JSA Risk Manager uses a default route mechanism to identify Internet edge devices (devices that are connected to the Internet). On some networks, this mechanism can falsely identify devices as edge devices. If you have modeled your network topology and identified edge devices, you can use the **Internet Override** option to identify those devices in JSA Risk Manager.

1. Click the **Risks** tab.
2. On the navigation menu, click **Topology**.
3. Click **Actions** > **Properties**.
4. Select the **Internet connections override** option, and then click **Edit**.
5. In the **Internet Connections Override** window, select **Networks connected to the Internet**, and then click **Edit**.
6. Modify the list by adding or removing networks or network groups in your network hierarchy.

   TIP: You must select at least one network to enable the override.
7. Click **OK**.
   The networks that you selected appear in the **Internet connections override** window.
8. Click **OK**.
   The **Internet connections override** field reads "By Network."
9. Click **OK**.

9

CHAPTER

Network Risk Assessment

Network Risk Assessment

SUMMARY

Create and define specific risk questions about your network to assess or monitor risk that is based on the analysis of risk indicators.

IN THIS SECTION

In Policy Monitor, you can define policies, assess adherence to a policy, evaluate results of questions, and monitor new risks.

Default question templates are available help you to assess and monitor the risk on your network. You can use one of the default question templates as a basis for your own questions or you can create a new question. You can find the default question templates in the **Group** menu on the **Policy Monitor** page.

You can choose from the following list of risk indicators:

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

You can define tests that are based on the risk indicators, and then restrict the test results to filter the query for specific results or violations.

Security professionals create questions for assets, devices, or rules to flag risks in their networks. The risk level for an asset, device, or rule is reported when a question is submitted to the Policy Monitor. You can approve results that are returned from assets or define how you want the system to respond to unapproved results.

Use Policy Monitor question results to assess risk for many security-risk scenarios such as the following scenarios:

- Use of forbidden protocols to communicate.

- Communication with forbidden networks or assets.
- Firewall rules don't comply with corporate policy.
- Systems prone to high-risk vulnerabilities because of their network configuration.

Policy Monitor Questions to Assess and Monitor Risk

SUMMARY

You can define questions in Policy Monitor to assess and monitor risk based on network activity, vulnerabilities, and firewall rules.

IN THIS SECTION

When you submit a question, the topology search is based on the data type that you selected:

- For questions based on assets, the search is based on the network assets that violated a defined policy or assets that introduced risk into the network.
- For questions based on devices or rules, the search either identifies the rules in a device that violated a defined policy or introduced risk into the network.
- If a question is based on asset compliance, the search identifies if an asset is compliant with a CIS benchmark.

IMPORTANT:
Domain ManagementAdmin*Juniper Secure Analytics Administration Guide*

Devices or rules questions look for violations in rules and policy and do not have restrictive test components. You can also ask devices or rules questions for applications.

Asset tests are divided into these categories:

- A *contributing test* uses the question parameters to examine the risk indicators that are specified in the question. Risk data results are generated, which can be further filtered by using a *restrictive test*. Contributing tests are shown in the **Which tests do you want to include in your question** area. Contributing tests return data based on assets detected that match the test question.
- A *restrictive test* narrows the results that are returned by a *contributing test* question. Restrictive tests display only in the **Which tests do you want to include in your question** area after a contributing

test is added. You can add restrictive tests only after you include a contributing test in the question. If you remove or delete a contributing test question, the restrictive test question cannot be saved.

Asset compliance questions look for assets that are not in compliance with CIS benchmarks. The tests that are included in the CIS benchmark are configured with the **Compliance Benchmark Editor**.

Policy Compliance and Policy Risk Changes

SUMMARY

Use the JSA Risk Manager **Policy Management** pages to view details about policy compliance and policy risk changes for assets, policies, and policy checks.

IN THIS SECTION

The JSA Risk Manager **Policy Management** pages display data from the last run policy. You can filter the data by asset, by policy, or by policy check.

NOTE:
"Monitoring a Policy Monitor Question and Generating Events" on page 119

Policy Management Use Cases

Use the **Policy Management** pages with **Risk** dashboard items to find more information about assets and policies that failed compliance.

- The **By Asset** page includes information and links to the policies that the assets failed.
- The **By Policy** page includes information about the number and percentage of assets that passed or failed and, if relevant, a link to the policy checks the policy uses.
- The **By Policy Check** page includes information about the number and percentages of assets that pass or fail individual policy checks.

Use the **Policy Management** pages with **Risk Change** dashboard items to investigate policies and policy checks that display increases in risk. The **Risk Change** dashboard item contains links to the **By Policy** and **By Policy Checks** pages. For more information about configuring dashboards for policy monitoring and monitoring risk change, see the *Juniper Secure Analytics Users Guide*.

Policy Monitor Question Parameters

SUMMARY

You can define test questions to identify risk in network devices or rules on network devices.

IN THIS SECTION

Generic and Test-specific Parameters for Policy Monitor Tests

You configure parameters for each Policy Monitor test. Configurable parameters are bolded and underlined. You click a parameter to view the available options for your question.

Policy Monitor tests use two types of parameters; generic and test-specific. Generic parameters provide 2 or more options to customize a test. Clicking a generic parameter toggles the choices that are available. Test-specific parameters require user-input. You click test-specific parameters to specify information.

For example, the asset test that is called **have accepted communication to destination remote network locations** contains two generic parameters and one test-specific parameter. Click the generic parameter **have accepted** to select either **have accepted** or **have rejected**. Click the generic parameter **to destination** to select either **to destination** or **from source**. Click the test-specific parameter **remote network locations** to add a remote location for the asset test.

Test Questions for Assets

Asset questions are used to identify assets on the network that violate a defined policy or introduce risk into the environment.

Asset test questions are categorized by communication type; actual or possible. Both communication types use contributing and restrictive tests.

Actual communication includes any assets on which communications were detected by using connections. Possible communication questions allow review for cases when specific communications are possible on assets, regardless of whether or not a communication was detected.

A contributing test question is the base test question that defines what type of actual communication you are trying to test.

A restrictive test question restricts the test results from the contributing test to further filter the actual communication for specific violations.

When you use a restrictive test, the direction of the restrictive test can follow the same direction as the contributing test. Restrictive tests that use a mix of inbound and outbound directions can be used in situations where you are trying to locate assets in between two points. For example, a restrictive test can locate assets in between two networks or IP addresses.

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.

Test Questions for Devices and Rules

Devices and rules are used to identify rules in a device that violate a defined policy that can introduce risk into the environment.

For a detailed list of device rule questions, see "Device/rules test questions" on page 102.

Contributing Questions for Actual Communication Tests

SUMMARY

The actual communication tests for assets include contributing questions and parameters that you choose when you create a Policy Monitor test.

IN THIS SECTION

When you apply the **have not** condition to a test, the **not** condition is associated with the parameter that you are testing.

For example, if you configure a test as **have not accepted communication to destination networks**, then the test detects assets that have accepted communications to networks other than the configured network. Another example is if you configure a test as **have not accepted communication to the Internet**. Then, the test detects assets that have accepted communications from or to areas other than the Internet.

The following table lists and describes the contributing question parameters for actual communication tests.

Table 8: Contributing Question Parameters for Actual Communication Tests

Test Name	Description
have accepted communication to any destination	Detects assets that have communications to any or from any configured network. Run this test to define a start or end point to your question. For example, to identify the assets that accepted communication from the DMZ, configure the test as follows: **have accepted communication from any source** You can use this test to detect out-of-policy communications.
have accepted communication to destination networks	Detects assets that have communications to or from the networks that you specify. Run this test 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.
have accepted communication to destination IP addresses	Detects assets that have communications to or from the IP address that you specify. Run this test 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>**
have accepted communication to destination asset building blocks	Detects assets that have communications to or from the asset building blocks that you specify. Run this test to reuse building blocks defined in the JSA Rules Wizard in your query. For more information about rules, assets, and building blocks, see the *Juniper Secure Analytics Administration Guide*.

Table 8: Contributing Question Parameters for Actual Communication Tests *(Continued)*

Test Name	Description
have accepted communication to destination asset saved searches	Detects assets that have communications to or from the assets that are returned by the saved search that you specify. For more information about creating and saving an asset search, see the *Juniper Secure Analytics Users Guide*.
have accepted communication to destination reference sets	Detects assets that communicated to or from the defined reference sets.
have accepted communication to destination remote network locations	Detects assets that communicated with networks defined as a remote network. For example, this test can identify hosts that communicated to botnets or other suspicious Internet address space.
have accepted communication to destination geographic network locations	Detects assets that communicated with networks defined as geographic networks. For example, this test can detect assets that attempted communications with countries in which you do not have business operations.
have accepted communication to the Internet	Detects source or destination communications to or from the Internet.
are susceptible to one of the following vulnerabilities	Detects specific vulnerabilities. If you want to detect vulnerabilities of a particular type, use the test, **are susceptible to vulnerabilities with one of the following classifications**. You can search for vulnerabilities by using the OSVDB ID, CVE ID, Bugtraq ID, or title.
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 might be Input Manipulation or Denial of Service.

Table 8: Contributing Question Parameters for Actual Communication Tests *(Continued)*

Test Name	Description
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 the CVSS score that you specify.
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.
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 entries. 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 expressions. Configure the **regular expressions** parameter to identify the asset name, vendor, version, or service you want this test to consider.
are susceptible to vulnerabilities contained in vulnerability saved searches	Detects risks that are associated with saved searches that are created in JSA Vulnerability Manager.

Deprecated Contributing Test Questions

Contributing questions that are replaced by another test are hidden in Policy Monitor.

The following tests are hidden in the Policy Monitor:

- assets that are susceptible to vulnerabilities

- assets that are susceptible to vulnerabilities from the following services

These contributing tests are replaced by other tests.

Restrictive Question Parameters for Actual Communication Tests

SUMMARY

The actual communication tests for assets include restrictive questions and parameters that you can choose when you create a Policy Monitor test.

When you apply the exclude condition to a test, the exclude condition applies to the protocols parameter.

For example, if you configure this test to **exclude the following protocols**, the test returns only assets that do not use the excluded protocols.

The following table lists and describes the restrictive question parameters for actual communication tests.

Table 9: Restrictive Question Parameters for Actual Communication Tests

Test Name	Description
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.
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.
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 filters connections that include only flow data.

Table 9: Restrictive Question Parameters for Actual Communication Tests *(Continued)*

Test Name	Description
include only if the source inbound and destination outbound bytes have a percentage difference less than 10	Filters assets from the contributing test question that is based on communications with a specific ratio of inbound to outbound (or outbound to inbound) bytes. This test is useful for detecting hosts that might be exhibiting proxy type behavior (inbound equals outbound).
include only if the inbound and outbound flow count has a percentage difference less than 10	Filters assets from the contributing test question that is based on communications with a specific ratio of inbound to outbound (or outbound to inbound) flows. This test filters connections that include flow data when flow count is selected. This restrictive test requires two contributing tests that specify a source and destination. The following test outlines a set of questions that are 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.
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. Run this test to detect out-of-policy communications. For example, if your corporate policy allows FTP communications between 1 and 3 AM, this test can detect any attempt to use FTP to communicate outside of that time range.

Table 9: Restrictive Question Parameters for Actual Communication Tests *(Continued)*

Test Name	Description
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. Run this test to detect out-of-policy communications.
include only if susceptible to vulnerabilities that are exploitable.	Filters assets from a contributing test question that is searching for specific vulnerabilities and restricts results to exploitable assets. This restrictive test does not contain configurable parameters, but is used along with the contributing test, **are susceptible to one of the following vulnerabilities**. This contributing rule that contains a vulnerabilities parameter is required.
include only the following networks	Filters assets from a contributing test question that includes or excludes the configured networks.
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.
include only the following asset saved searches	Filters assets from a contributing test question that are or are not associated with the asset saved search.
include only the following reference sets	Filters assets that are from a contributing test question that includes or excludes the configured reference sets.
include only the following IP addresses	Filters assets that are or are not associated with the configured IP addresses.
include only if the Microsoft Windows service pack for operating systems is below 0	Filters assets to determine whether a Microsoft Windows service pack level for an operating system is under the level your company policy specifies.
include only if the Microsoft Windows security setting is less than 0	Filters assets to determine whether a Microsoft Windows security setting is under the level your company policy specifies.

Table 9: Restrictive Question Parameters for Actual Communication Tests *(Continued)*

Test Name	Description
include only if the Microsoft Windows service equals status	Filters assets to determine whether a Microsoft Windows service is unknown, boot, kernel, auto, demand, or disabled.
include only if the Microsoft Windows setting equals regular expressions	Filters assets to determine whether a Microsoft Windows Setting is the specified regular expression.

Contributing Questions for Possible Communication Tests

SUMMARY

The possible communication tests for assets include contributing questions and parameters that you can choose when you create a Policy Monitor test.

IN THIS SECTION

The following table lists and describes the contributing question parameters for possible communication tests.

Table 10: Possible Communication Question Parameters for Contributing Tests

Test Name	Description
have accepted communication to any destination	Detects assets that have possible communications to or from any specified source or destination. For example, to determine whether 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 received any communications on port 21. Run this test to detect out-of-policy communications for that critical server.

Table 10: Possible Communication Question Parameters for Contributing Tests *(Continued)*

Test Name	Description
have accepted communication to destination networks	Detects assets that have possible communications to or from the configured network. Run this test 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.
have accepted communication to destination IP addresses	Detects assets that have possible communications to or from the configured IP address. Run this test 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>**
have accepted communication to destination asset building blocks	Detects assets that have possible communications to or from the configured asset by using building blocks. Run this test to reuse building blocks defined in the JSA 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 *Juniper Secure Analytics Administration Guide*.
have accepted communication to destination asset saved searches	Detects assets that have accepted communications to or from the assets that are returned by the saved search that you specify. A saved asset search must exist before you use this test. For more information about creating and saving an asset search, see the *Juniper Secure Analytics Users Guide*.
have accepted communication to destination reference sets	Detects if source or destination communication are possible to or from reference sets.

Table 10: Possible Communication Question Parameters for Contributing Tests *(Continued)*

Test Name	Description
have accepted communication to the Internet	Detects if source or destination communications are possible to or from the Internet. Specify the **to** or **from** parameter to consider communication traffic to the Internet or from the Internet.
are susceptible to one of the following vulnerabilities	Detects possible specific vulnerabilities. If you want to detect vulnerabilities of a particular type, use the test, **are susceptible to vulnerabilities with one of the following classifications**. Specify the vulnerabilities to which you want this test to apply. You can search for vulnerabilities by using the OSVDB ID, CVE ID, Bugtraq ID, or title.
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 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.
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.
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.

Table 10: Possible Communication Question Parameters for Contributing Tests *(Continued)*

Test Name	Description
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 entries. 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, vend, 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 expressions. Configure the **regular expressions** parameter to identify the asset name, vendor, version, or service you want this test to consider.
are susceptible to vulnerabilities contained in vulnerability saved searches	Detects risks that are associated with saved searches that are created in JSA Vulnerability Manager.

Deprecated Contributing Test Questions

If a test is replaced with another test, it is hidden in Policy Monitor.

The following tests are hidden in the Policy Monitor:

- **assets that are susceptible to vulnerabilities from the following vendors**
- **assets that are susceptible to vulnerabilities from the following services**

These contributing tests were replaced by other tests.

Restrictive Question Parameters for Possible Communication Tests

SUMMARY

Possible communication tests for assets include restrictive question parameters.

The following table lists and describes the restrictive question parameters for possible communication tests.

Table 11: Restrictive Tests for Possible Communication Tests

Test Name	Description
include only the following protocols	Filters assets that did or did not possibly communicate with the configured protocols, along with the other tests added to this question.
include only the following inbound ports	Filters assets that did or did not possibly communicate with the configured ports, along with the other tests added to this question.
include only ports other than the following inbound ports	Filters assets from a contributing test question that did or did not possibly communicate with ports other than the configured ports, along with the other tests added to this question.
include only if susceptible to vulnerabilities that are exploitable.	Filters assets from a contributing test question by searching for possible specific vulnerabilities and restricts results to exploitable assets. This restrictive test does not contain configurable parameters, but is used along with the contributing test, **are susceptible to one of the following vulnerabilities**. This contributing rule that contains 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.
include only the following asset building blocks	Filters assets from a contributing test question that include only or exclude the configured asset building blocks.
include only the following asset saved searches	Filters assets from a contributing test question that include only or exclude the associated asset saved search.
include only the following reference sets	Filters assets from a contributing test question that include only or exclude the configured.
include only the following IP addresses	Filters assets from a contributing test question that include only or exclude the configured IP addresses.
include only if the Microsoft Windows service pack for operating systems is below 0	Filters assets to determine whether a Microsoft Windows service pack level for an operating system is under the level your company policy specifies.

Table 11: Restrictive Tests for Possible Communication Tests *(Continued)*

Test Name	Description
include only if the Microsoft Windows security setting is less than 0	Filters assets to determine whether a Microsoft Windows security setting is under the level your company policy specifies.
include only if the Microsoft Windows service equals status	Filters assets to determine whether a Microsoft Windows service is unknown, boot, kernel, auto, demand, or disabled.
include only if the Microsoft Windows setting equals regular expressions	Filters assets to determine whether a Microsoft Windows Setting is the specified regular expression.

Test Questions to Find Rules in a Device

SUMMARY

Devices and rules test questions are used to identify rules in a device that violate a defined policy that can introduce risk into the environment.

The device and rules test questions are described in the following table.

Table 12: Device and Rules Tests

Test Name	Description
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.
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.

Table 12: Device and Rules Tests *(Continued)*

Test Name	Description
allow connections to the following asset building blocks	Filters device rules and connections to or from the configured asset building block.
allow connections to the following reference sets	Filters device rules and connections to or from the configured reference sets.
allow connections using the following destination ports and protocols	Filters device rules and connections to or from the configured ports and protocols
allow connections using the following protocols	Filters device rules and connections to or from the configured protocols.
allow connections to the Internet	Filters device rules and connections to and from the Internet.
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.
are one of the following reference sets	Filters device rule based on the reference sets that you specify.
are one of the following networks	Filters device rules based on the networks that you specify.
are using one of the following adapters	Filters device rules based on the adapters that you specify.

RELATED DOCUMENTATION

Contributing Questions for Actual Communication Tests | 90

Creating a Question that Tests for Rule Violations

SUMMARY

Create a question in Policy Monitor to identify the rules in a device that violated a defined policy, or introduced risk into the network.

IN THIS SECTION

Policy Monitor questions are evaluated in a top-down manner. The order of Policy Monitor questions impacts the results.

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. From the **Actions** menu, click **New Device/Rules Question**.
4. In the **What do you want to name this question** field, type a name for the question.
5. From the **Importance Factor** list, select the level of importance that you want to associate with this question.
6. From the **Which tests do you want to include in your question** field, select the add (+) icon next to the tests you want to include.
7. In the **Find Devices/Rules that** field, configure the parameters for your tests.

   Configurable parameters are bold and underlined. Click each parameter to view the available options for your question.
8. In the groups area, click the relevant check boxes to assign group membership to this question.
9. Click **Save Question**.

Investigating Rules that Allow Communication to the Internet

SUMMARY

In Policy Monitor, device tests are used to identify rules on a device that violate a defined policy, or changes that introduce risk into the environment.

Device tests are used to identify rules in a device that violate a defined policy or changes that introduce risk into the environment. From a network security perspective, it is important to know about changes to device rules. A common occurrence is when servers get unintentional access to the Internet because

of firewall change on the network. JSA Risk Manager can monitor for rule changes on network devices by creating a policy monitor question based on the device rules.

Create a Policy Monitor question that checks what devices have access to the Internet.

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. From the **Actions** menu, select **New Devices/Rules Question**.
4. In the **What type of data do you want to return**, click **Devices/Rules**.
5. From the **Importance Factor** list, select the level of importance that you want to associate with your question.
6. In the **Which tests do you want to include in your question** section, select the add (+) icon next to the test **allow connections to the Internet**. This action adds the test to your question.
7. Click **Save Question**.
8. Select the Policy Monitor question that you created for monitoring device rules.
9. Click **Submit Question**.
10. Review the results to see whether any rules allow access to the Internet.
11. Monitor your protected assets by putting the Policy Monitor question into monitoring mode.

Searching for Assets in your Network

SUMMARY

Create an asset question to search for assets in the network that violate a defined policy or assets that introduced risk.

IN THIS SECTION

Policy Monitor questions are evaluated in a top-down manner. The order of the questions impacts the results.

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.

3. From the **Actions** menu, select **New Asset Question**.
4. In the **What do you want to name this question** field, type a name for the question.
5. From the **Evaluate On** list, select one of the following options:

Option	Description
Actual Communication	Includes any assets on which communications were detected that use connections.
Possible Communication	Includes any assets on which communications are allowed through your network topology, such as firewalls. You use these questions to investigate whether specific communications are possible, regardless of whether a communication was detected.

6. From the **Importance Factor** list, 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 that are returned for a question.
7. Specify the time range for the question.
8. From the **Which tests do you want to include in your question** field, select the add (+) icon next to the tests you want to include.
9. Configure the parameters for your tests in the **Find Assets that** field.

   Configurable parameters are bold and underlined. Click each parameter to view the available options for your question.
10. In the groups area, click the relevant check boxes to assign group membership to this question.
11. Click **Save Question**.

Importance Factor in Risk Score Calculations

SUMMARY

The importance factor is used to calculate the risk score and define the number of results that are returned for a question.

The range is 1 (low importance) to 10 (high importance). The default is 5.

Table 13: Importance Factor Results Matrix

Importance Factor	Returned Results for Asset Tests	Returned Results for Device and 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. This factor is warranted because any results to the question are 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. The lower factor demonstrates that the results of the question do not indicate high risk, but you might monitor this communication for informational purposes.

Investigating External Communications that use Untrusted Protocols

SUMMARY

You can use a Policy Monitor question that is based on the known list of trusted protocols to monitor traffic in your DMZ. In most organizations, network traffic that crosses the DMZ is restricted to 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. Use JSA Risk Manager to accomplish this task by creating a Policy Monitor question based on an asset test for actual communications.

Select an option to create a Policy Monitor question based on the known list of trusted protocols for the DMZ.

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. From the **Actions** menu, select **New Asset Question**.
4. In the **What do you want to name this question** field, type a name for the question.
5. In the **What type of data do you want to return** drop-down list, select **Assets**.
6. In the **Evaluate On** menu, select **Actual Communication**.
7. From the **Importance Factor** menu, specify a level of importance to associate with your question.
8. In the **Time Range** section, specify a time range for the question.

9. In the **Which tests do you want to include in your question** panel, select **have accepted communication to destination networks**.
10. In the **Find Assets that** panel, click **destination networks** to further configure this test and specify your DMZ as the destination network.
11. Select **and include the following inbound ports**.
12. In the **Find Assets that** panel, click **include only** so that it changes to **exclude**.
13. Click **ports**.
14. Add port 80 and 443, and then click **OK**.
15. Click **Save Question**.
16. Select the Policy Monitor DMZ question that you created, and then click **Submit Question**.
17. Review the results to see whether any protocols other than port 80 and port 443 are communicating on the network.
18. Monitor your DMZ question by putting the question into monitoring mode when the results are tuned.

Finding Assets that Allow Communication from the Internet

SUMMARY

Find assets that allow communication from the Internet. JSA Risk Manager evaluates the question and displays the results of any internal assets that allow inbound connections from the Internet.

---

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. From the Group list, select **PCI 10**.
4. Select the test question **Assess any inbound connections from the Internet to anywhere on the internal network**.
5. Click **Submit Question**.

Assessing Devices that Allow Risky Protocols

SUMMARY

JSA Risk Manager evaluates a question and displays the results of any assets, in your topology, that match the test question. Security professionals, administrators, or auditors in your network can approve communications that are not risky to specific assets. They can also create an offense for the behavior.

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. From the Group list, select **PCI 1**.
4. Select the test question **Assess any devices (i.e. firewalls) that allow risky protocols (i.e. telnet and FTP traffic - port 21 & 23 respectively) from the Internet to the DMZ**.
5. Click **Submit Question**.

Investigating Possible Communication with Protected Assets

SUMMARY

You can create a Policy Monitor question based on IP addresses that detect possible communication with protected assets. From a risk perspective, it is important to know which users within your organization can communicate with critical network assets.

JSA Risk Manager accomplishes this task by creating a Policy Monitor question based on an asset test for possible communications.

You might 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 goal, create a Policy Monitor question that looks at the topology of the network by IP address.

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. From the **Actions** menu, select **New**.
4. In the **What do you want to name this question** field, type a name for the question.
5. In the **What type of data do you want to return** drop-down list, select **Assets**.
6. From the **Evaluate On** drop-down list, select **Possible Communication**.
7. From the **Importance Factor** drop-down list, specify a level of importance to associate with your question.
8. In the **Time Range section** , specify a time range for the question.

9. In the **Which tests do you want to include in your question** section, double-click to select **have accepted communication to destination asset building blocks**.
10. In the **Find Assets that** section, click **asset building blocks** to further configure this test and specify **Protected Assets**.

> **NOTE**: To define your network remote assets, your remote assets building block must be defined.

11. In the **Which tests do you want to include in your question** section, double-click to select the restrictive test **and include only the following IP addresses**.
12. In the **Find Assets that** section, click **IP Addresses**.
13. Specify the IP address range or CIDR address of your remote network.
14. Click **Save Question**.
15. Select the Policy Monitor question that you created for protected assets.
16. Click **Submit Question**.
17. Review the results to see whether any protected asset accepts communication from an unknown IP address or CIDR range.
18. Monitor your protected assets by putting the question into monitoring mode. If an unrecognized IP address connects to a protected asset, then JSA Risk Manager can generate an alert.

Submitting a Question to Determine Associated Risk

SUMMARY

When you submit a question, the resulting information depends on the data that is queried; assets or devices and rules.

IN THIS SECTION

After a Policy Monitor question is submitted, you can view how long the question takes to run. The time that is required to run the policy also indicates how much data is queried. For example, if the execution time is 3 hours then 3 hours of data is queried. You can view the time in the **Policy Execution Time** column to determine an efficient interval frequency to set for the questions that you want to monitor. For example, if the policy execution time is 3 hours, then the policy evaluation interval must be greater than 3 hours.

IMPORTANT: When you edit a question after it is submitted, and the edit affects associated tests, it might take up to an hour to view those changes.

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. Select the question that you want to submit.
4. Click **Submit Question**.

Asset Question Results

SUMMARY

Asset results display after you submit a Policy Monitor question. The **Risk Score** indicates the level of risk that is associated with the question.

The **Risk Score** calculation is based on the importance factor that is assigned to the question, and the number of results returned for the question.

The following table describes the parameters for asset results:

Table 14: Asset Result Parameters

Parameter	Description
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 *Juniper Secure Analytics Users Guide*.
VLAN	The name of the VLAN associated with the asset.
Weight	The weight of the asset, as obtained from the asset profile.

Table 14: Asset Result Parameters *(Continued)*

Parameter	Description
Destination Port(s)	The list of destination ports associated with this asset, in context of the question tests. If multiple ports are associated with this asset and question, this field indicates Multiple and the number of multiple ports. The list of ports is obtained by filtering the connections that are associated with this question to obtain all unique ports where the asset was either the source, destination, or the connection. Click Multiple (N) to view the connections. This display provides the aggregated connections by port, which is 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 multiple protocols are associated with this asset and question, this field indicates Multiple and the number of protocols. The list of protocols is obtained by filtering the connections that are associated with this question to obtain all unique protocols where the asset was either the source, destination, or the connection. Click Multiple (N) to view the Connections. This display provides the aggregated connections by protocol, which is 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 multiple applications are associated with this asset and question, this field indicates Multiple and the number of applications. The list of applications is obtained by filtering the connections that are associated with this question to obtain all unique applications where the asset was either the source, destination, or the connection. Click Multiple (N) to view the Connections. This display provides the aggregated connections by application, which is filtered by the asset IP address, and based on the time interval specified in the question.

Table 14: Asset Result Parameters *(Continued)*

Parameter	Description
Vuln(s)	The list of vulnerabilities associated with this asset, in context of the question tests. If multiple vulnerabilities are associated with this asset and question, this field indicates Multiple and the number of vulnerabilities. The list of vulnerabilities is obtained using a list of all vulnerabilities that are 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, which is 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 that are associated with this question to obtain the flow count total, where asset was either 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 multiple source IP addresses are associated with this asset and question, this field indicates Multiple and the number of source IP addresses. The list of source IP addresses is obtained by filtering the connections that are associated with this question. The obtained list contains 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 address, which is filtered by the asset IP address based on the time interval that is specified in the question.
Destination(s)	The list of destination IP addresses associated with this asset, in context of the question tests. If multiple destination IP addresses are associated with this asset and question, this field indicates Multiple and the number of destination IP addresses. The list of destination IP addresses is obtained by filtering the connections that are associated with this question. The obtained list contains 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 address, which is filtered by the asset IP address based on the time interval that is specified in the question.

Table 14: Asset Result Parameters *(Continued)*

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

Device and Rule Question Results

SUMMARY

Device and rule results display after you submit a Policy Monitor question. The **Risk Score** displayed indicates the level of risk that is associated with the question.

The **Risk Score** calculation is based on the importance factor that is assigned to the question, and the number of results returned for the question.

The following table describes the parameters for devices and rules results.

Table 15: Devices and Rules Result Parameters

Parameter	Description
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 *Juniper Secure Analytics Users Guide*.

Table 15: Devices and Rules Result Parameters *(Continued)*

Parameter	Description
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.
Source(s)	The source network associated with this asset. Sources with a hyperlink indicate an object group reference. Click the link to view detailed information about one or more object group references.

Table 15: Devices and Rules Result Parameters *(Continued)*

Parameter	Description

Source Service(s)	The source ports and the comparison that is associated with the relevant rule from the device are shown in the following format:
	
	`<comparison>:<port>`
	
	Where
	
	`<comparison>`
	
	might 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 this source service. If the parameter indicates lt:80, the range of applicable ports is 0 - 79.
	
	This parameter displays the source port for the device rule. If no port exists for this device rule, the term NA is displayed.
	
	Source services with a hyperlink indicate an object group reference. Click the link to view detailed information about one or more object group references.

Destination(s)	The destination network associated with the relevant rule from the device. Destinations with a hyperlink indicate an object group reference. Click the link to view detailed information about one or more object group references.

Table 15: Devices and Rules Result Parameters *(Continued)*

Parameter	Description

Destination Service(s)	The destination ports and the comparison that is associated with the relevant rule from the device is displayed in the following format:
	
	`<comparison>:<port>`
	
	Where
	
	`<comparison>`
	
	might 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 - 79.
	
	This parameter displays the destination port for the device rule. If no port exists for this device rule, the term NA is displayed.
	
	Destination services with a hyperlink indicate an object group reference. Click the link to view detailed information about one or more object group references .

User(s)Group(s)	The users or groups that are associated with the relevant rule from the device.
Protocol(s)	The protocol or group of protocols that are 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.

Table 15: Devices and Rules Result Parameters *(Continued)*

Parameter	Description
Applications	The applications that are associated with the relevant rule from the device.

Approving Results from Policy Monitor Questions

SUMMARY

You can evaluate the results that are returned from a Policy Monitor question in JSA Risk Manager. Approving a result of a question is similar to tuning your system to inform JSA Risk Manager that the asset that is associated with the question result is safe or can be ignored later.

When a user approves an asset result, the Policy Monitor detects that asset result as approved. Then, 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 display 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 or rule, and the date and time. Approve results to Policy Monitor questions that don't represent risk in your network.

1. In the results table, select the checkbox next to the results you want to accept.
2. Choose one of the following options:

Option	Description
Approve All	Select this option to approve all the results.
Approve Selected	Select the checkbox next to the results that you want to approve, and then click **Approve Selected**.

3. Type the reason for approval.
4. Click **OK**.
5. Click **OK**.
6. To view the approved results for the question, click **View Approved**.

The **Approved Question Results** window provides the following information:

Table 16: Visualizing Approved Question Results Parameters

Parameter	Description
Device/Rule	The device that is associated with this result in **Device/Rule Results**.
IP	The IP address that is associated with the asset in **Asset Results**.
Approved By	The user that approved the results.
Approved On	The date and time the results were approved.
Notes	Displays the text of the notes that are associated with this result and the reason why the question was approved.

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

Monitoring a Policy Monitor Question and Generating Events

SUMMARY

Monitor the results of Policy Monitor questions and configure the generation of events when the results of the monitored Policy Monitor questions change. You can set the policy evaluation interval, and configure events to send notifications.

When you monitor a policy question, JSA Risk Manager analyzes the question at the configured interval to determine if an asset or rule change generates an unapproved result. If JSA Risk Manager detects an unapproved result, an offense can be generated to alert you about a deviation in your defined policy. In monitor mode, JSA Risk Manager can simultaneously monitor the results of 10 questions.

Question monitoring provides the following key features:

- Monitor for rule or asset changes for unapproved results at the configured interval.
- Use your high and low-level event categories to categorize unapproved results.
- Generating offenses, emails, syslog messages, or dashboard notifications on unapproved results.
- Use event viewing, correlation, event reporting, custom rules, and dashboards in JSA.

1. Click the **Risks** tab.

2. On the navigation menu, click **Policy Monitor**.
3. Select the question that you want to monitor.
4. Click **Monitor**.
5. Configure values for the parameters.

   The parameters that you configure for an event are described in the following table.

Table 17: Configuring Question Event Parameters

Parameter	Description
Policy evaluation interval	The frequency for the event to run.
Event Name	The name of the event you want to display in the **Log Activity** and **Offenses** tabs.
Event Description	The description for the event. The description is displayed in the Annotations of the event details.
High-Level Category	The high-level event category that you want this rule to use when processing events.
Low-Level Category	The low-level event category that you want this rule to use when processing events.
Ensure the dispatched event is part of an offense	Forwards the events to the Magistrate component. If no offense is generated, a new offense is created. If an offense exists, the event is added. If you correlate by question or simulation, then all events from a question are associated to a single offense. If you correlate by asset, then a unique offense is created or updated for each unique asset.
Dispatch question passed events	Forwards events that pass the policy monitor question to the Magistrate component. **TIP**: You must enable this parameter to configure Vulnerability Score Adjustments because these adjustments can be made to assets that both pass and fail policy monitor questions.

Table 17: Configuring Question Event Parameters *(Continued)*

Parameter	Description
Vulnerability Score Adjustments	Adjusts the vulnerability risk score of an asset, depending if the question fails or passes. The vulnerability risk scores are adjusted in JSA Vulnerability Manager.

Additional Actions	The additional actions to be taken when an event is received.
	
	Separate multiple email addresses by using a comma.
	
	Select **Notify** if you want events that generate as a result of this monitored question to display events in the System Notifications item in the dashboard.
	
	The syslog output might resemble the following code:
	
	`Sep 28 12:39:01 localhost.localdomain ECS:`
	`Rule 'Name of Rule'`
	`Fired: 172.16.60.219:12642 -> 172.16.210.126:6666 6,`
	`Event Name:SCAN SYN FIN, QID: 1000398, Category: 1011,`
	` Notes: Event description`

Enable Monitor	Monitor the question.

6. Click **Save Monitor**.

Policy Monitor Question Backup

SUMMARY

Users with administrative privileges can export and import Policy Monitor questions.

IN THIS SECTION

Exporting and importing questions provides a method to back up questions and share questions with other JSA Risk Manager users.

Restrictions for Sensitive Information

Sensitive company or policy information might be included in dependencies. When you export or import Policy Monitor questions, the sensitive data that is contained in the dependencies is not included.

Policy Monitor questions might contain the following types of dependencies:

- Asset building blocks
- Asset saved searches
- Networks
- Remote network locations
- Geographic network locations
- Reference sets

Before you export questions that have dependencies, you might choose to provide more context about the type of information that is contained in the dependency. Providing this information allows other users to understand what type of information to reference when they import the question in their Policy Monitor.

Exporting Policy Monitor Questions

SUMMARY

You can export one or more of your Policy Monitor questions to an XML file. Exporting Policy Monitor questions is useful for backing up your questions or for sharing questions with other users.

If any Policy Monitor questions contain dependencies, then you can provide more context about the type of information that is contained in the dependency.

The default XML file name for the exported questions is **policy_monitor_questions_export.xml**.

1. On the **Risks** tab, click **Policy Monitor**.
2. Choose one of the following options:
   - To export all questions, from the **Actions** menu, select **Export All**.
   - To export specific questions, press the Ctrl key to select each question that you want to export, and then from the **Actions** menu, select **Export Selected**.

3. If any questions contain dependencies, click the parameter link to type more specific information. The maximum character length for this field is 255.
4. Click **Export Questions**.

A default file, called **policy_monitor_questions_export.xml**, is exported to your download directory.

Importing Policy Monitor Questions

SUMMARY

Import one or more Policy Monitor questions to JSA Risk Manager. The import process does not update existing questions. Each question that is imported becomes a new question in Policy Monitor. A timestamp is added to all imported questions.

If an imported question contains a dependency, a warning is displayed in the **Status** column. Imported questions with dependencies contain parameters with no values. To ensure that imported Policy Monitor questions work as expected, you must enter values for the parameters.

Monitoring is not enabled on imported questions. You can "create an event" on page 119 to monitor results of questions that were imported.

1. On the **Risks** tab, click **Policy Monitor**.
2. From the **Actions** menu, select **Import**.
3. Click **Choose File**, and then browse to select the XML file that you want to import.
4. Click **Open**.
5. Select one or more groups to assign the question to a group.
6. Click **Import Question**.
7. Check the **Status** column for warnings. If a question contains a warning, open the question and edit the dependent parameters. Save the question when you update parameters.

Integration with JSA Vulnerability Manager

IN THIS SECTION

JSA Vulnerability Manager integrates with JSA Risk Manager to help you prioritize the risks and vulnerabilities in your network.

You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or Juniper Customer Support.

Risk Policies and Vulnerability Prioritization

You can integrate JSA Vulnerability Manager with JSA Risk Manager by defining and monitoring asset or vulnerability risk policies.

When the risk policies that you define in JSA Risk Manager either pass or fail, vulnerability risk scores in JSA Vulnerability Manager are adjusted. The adjustment levels depend on the risk policies in your organization.

When the vulnerability risk scores are adjusted in JSA Vulnerability Manager, administrators can do the following tasks:

- Gain immediate visibility of the vulnerabilities that failed a risk policy.

  For example, new information might be displayed on the JSA dashboard or sent by email.

- Re-prioritize the vulnerabilities that require immediate attention.

  For example, an administrator can use the **Risk Score** to quickly identify high-risk vulnerabilities.

If you apply risk policies at an asset level in JSA Risk Manager, then all the vulnerabilities on that asset have their risk scores adjusted.

Prioritizing High Risk Vulnerabilities by Applying Risk Policies

In JSA Vulnerability Manager, you can alert administrators to high-risk vulnerabilities by applying risk policies to your vulnerabilities.

When you apply a risk policy, the risk score of a vulnerability is adjusted, which allows administrators to prioritize more accurately the vulnerabilities that require immediate attention.

In the following example, the vulnerability risk score is automatically increased by a percentage factor for any vulnerability that remains active on your network after 40 days.

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. On the toolbar, click **Search** > **New Search**.
4. In the **Search Parameters** pane, configure the following filters:
   a. **Risk Equals High**
   b. **Days since vulnerabilities discovered Greater than or equal to 40**
5. Click **Search** and then on the toolbar click **Save Search Criteria**.

Type a saved search name that is identifiable in JSA Risk Manager.

6. Click the **Risks** tab.
7. In the navigation pane, click **Policy Monitor**.
8. On the toolbar, click **Actions** > **New**.
9. In the **What do you want to name this question** field, type a name.
10. In the **Which tests do you want to include in your question** field, click **are susceptible to vulnerabilities contained in vulnerability saved searches**.
11. In the **Find Assets that** field, click the underlined parameter on the **are susceptible to vulnerabilities contained in vulnerability saved searches**.
12. Identify your JSA Vulnerability Manager high risk vulnerability saved search, click **Add**, then click **OK**.
13. Click **Save Question**.
14. In the **Questions** pane, select your question from the list and on the toolbar click **Monitor**.

    RESTRICTION:
    Event Description

15. Click **Dispatch question passed events**.
16. In the **Vulnerability Score Adjustments** field, type a risk adjustment percentage value in the **Percentage vulnerability score adjustment on question fail** field.
17. Click **Apply adjustment to all vulnerabilities on an asset** then click **Save Monitor**.

On the **Vulnerabilities** tab, you can search your high risk vulnerabilities and prioritize your vulnerabilities.

10
CHAPTER

CIS Benchmark Scans

CIS Benchmark Scans

SUMMARY

To set up a Center for Internet Security (CIS) benchmark scan, you must complete a range of configuration tasks on the Admin, Assets, Vulnerabilities, and Risks tabs in JSA.

IN THIS SECTION

To set up CIS benchmark scan, the following prerequisites are needed:

- Valid JSA Vulnerability Manager and JSA Risk Manager licenses.
- You must have the correct license capabilities to perform the following scanning operations. If you need assistance to obtain a new or updated license key, contact your local sales representative or Juniper Customer Support.
- If you patched from an earlier release of JSA, you must do an automatic update before you do a CIS benchmark scan.

The following eight steps are involved in setting up a CIS benchmark scan:

1. Adding assets.
2. Configuring a credential set.

   TIP: It is easier to add centralized credentials on the JSA Admin tab, but you can also add credentials when you create a benchmark profile.

3. Creating an asset saved search.

   You use the asset saved searches when you configure the asset compliance questions.

4. Modifying CIS benchmark checks in JSA Vulnerability Manager.
   You can create a custom CIS benchmark checklist by using the Compliance Benchmark Editor.
5. Configuring a CIS benchmark scan profile in JSA Vulnerability Manager.
6. Creating an asset compliance question in JSA Risk Manager.
7. Monitoring the asset compliance question that you created.
8. Viewing the CIS benchmark scan results.

Adding or Editing an Asset Profile

SUMMARY

Before you can do a CIS benchmark scan, you must add the network assets that you intend to scan to JSA. Asset profiles are automatically discovered and added; however, you might be required to manually add a profile.

You can enter information on each asset manually by creating an Asset Profile on the **Assets** tab. Alternatively, you can configure a scan profile on the **Vulnerabilities** tab to run a discovery scan. The discovery scan allows JSA to identify key asset characteristics such as operating system, device type, and services.

When assets are discovered by using the Server Discovery option, some asset profile details are automatically populated. You can manually add information to the asset profile and you can edit certain parameters.

You can edit only the parameters that were manually entered. Parameters that were system-generated are displayed in italics and are not editable. You can delete system-generated parameters, if needed.

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Choose one of the following options:

Option	Description
Add Asset	To add an asset, click **Add Asset** and type the IP address or CIDR range of the asset in the **New IP Address** field.

Option	Description
Edit Asset	Double click the asset that you want to view and click **Edit Asset**.

4. **NOTE**: When you edit an existing asset, the asset must have a MAC address before you can add an IP address.

   Configure the parameters in the **MAC & IP Address** pane. Configure one or more of the following options:

Parameter	Description
New MAC Address	Type a MAC address in the dialog box.
New IP Address	Type an IP address in the dialog box.
Unknown NIC	If this parameter is listed, you can select this item, click the **Edit** icon, and type a new MAC address in the dialog box.
Edit	Select a MAC or IP address from the list, click the **Edit** icon, and type a new MAC address in the dialog box.
Remove	Select a MAC or IP address from the list and click the **Remove** icon.

5. Configure the parameters in the **Names & Description** pane. Configure one or more of the following options:

Parameter	Description
DNS	Choose one of the following options: Type a DNS name and click **Add**. Select a DNS name from the list and click **Edit**. Select a DNS name from the list and click **Remove**.
NetBIOS	Choose one of the following options: Type a NetBIOS name and click **Add**. Select a NetBIOS name from the list and click **Edit**.

Parameter	Description
	Select a NetBIOS name from the list and click **Remove**.
Given Name	Type a name for this asset profile.
Location	Type a location for this asset profile.
Description	Type a description for the asset profile.
Wireless AP	Type the wireless Access Point (AP) for this asset profile.
Wireless SSID	Type the wireless Service Set Identifier (SSID) for this asset profile.
Switch ID	Type the switch ID for this asset profile.
Switch Port ID	Type the switch port ID for this asset profile.

6. Configure the parameters in the Operating System pane:
   a. From the **Vendor** list box, select an operating system vendor.
   b. From the **Product** list box, select the operating system for the asset profile.
   c. From the **Version** list box, select the version for the selected operating system.
   d. Click the **Add** icon.
   e. From the **Override** list box, select one of the following options:
      - **Until Next Scan** - Select this option to specify that the scanner provides operating system information and the information can be temporarily edited. If you edit the operating system parameters, the scanner restores the information at its next scan.
      - **Forever** - Select this option to specify that you want to manually enter operating system information and disable the scanner from updating the information.
   f. Select an operating system from the list.
   g. Select an operating system and click the **Toggle Override** icon.
7. Configure the parameters in the **CVSS & Weight** pane. Configure one or more of the following options:

Parameter	Description
Collateral Damage Potential	Configure this parameter to indicate the potential for loss of life or physical assets through damage or theft of this asset. You can also use this

Parameter	Description
	parameter to indicate potential for economic loss of productivity or revenue. Increased collateral damage potential increases the calculated value in the CVSS Score parameter. From the **Collateral Damage Potential** list box, select one of the following options: • None • Low • Low-medium • Medium-high • High • Not defined When you configure the **Collateral Damage Potential** parameter, the **Weight** parameter is automatically updated.
Confidentiality Requirement	Configure this parameter to indicate the impact on confidentiality of a successfully exploited vulnerability on this asset. Increased confidentiality impact increases the calculated value in the CVSS Score parameter. From the **Confidentiality Requirement** list box, select one of the following options: • Low • Medium • High • Not defined
Availability Requirement	Configure this parameter to indicate the impact to the asset's availability when a vulnerability is successfully exploited. Attacks that consume network bandwidth, processor cycles, or disk

Parameter	Description
	space impact the availability of an asset. Increased availability impact increases the calculated value in the CVSS Score parameter. From the **Availability Requirement** list box, select one of the following options: • Low • Medium • High • Not defined
Integrity Requirement	Configure this parameter to indicate the impact to the asset's integrity when a vulnerability is successfully exploited. Integrity refers to the trustworthiness and guaranteed veracity of information. Increased integrity impact increases the calculated value in the CVSS Score parameter. From the **Integrity Requirement** list box, select one of the following options: • Low • Medium • High • Not defined
Weight	From the **Weight** list box, select a weight for this asset profile. The range is 0 - 10. When you configure the **Weight** parameter, the **Collateral Damage Potential** parameter is automatically updated.

8. Configure the parameters in the Owner pane. Choose one or more of the following options:

Parameter	Description
Business Owner	Type the name of the business owner of the asset. An example of a business owner is a department manager. The maximum length is 255 characters.
Business Owner Contact	Type the contact information for the business owner. The maximum length is 255 characters.
Technical Owner	Type the technical owner of the asset. An example of a business owner is the IT manager or director. The maximum length is 255 characters.
Technical Owner Contact	Type the contact information for the technical owner. The maximum length is 255 characters.
Technical User	From the list box, select the username that you want to associate with this asset profile. You can also use this parameter to enable automatic vulnerability remediation for JSA Vulnerability Manager. For more information about automatic remediation, see the *Juniper Secure Analytics Vulnerability Manager User Guide*.

9. Click **Save**.

"Configuring a Credential Set" on page 133

Configuring a Credential Set

SUMMARY

In JSA Vulnerability Manager, you can create a credential set for the assets in your network. During a scan, if a scan tool requires the credentials for a Linux, UNIX, or Windows operating system, the credentials are automatically passed to the scan tool from the credential set.

1. On the navigation menu, click **Admin**.
2. In the **System Configuration** pane, click **Centralized Credentials**.
3. In the **Centralized Credentials** window, on the toolbar, click **Add**.

To configure a credential set, the only mandatory field in the **Credential Set** window is the **Name** field.

4. In the **Credential Set** window, click the **Assets** tab.
5. Type a CIDR range for the assets that you want to specify credentials for and click **Add**.

   Users must have network access permissions that are granted in their security profile for an IP address or CIDR address range that they use or create credentials for in **Centralized Credentials**.
6. Click the **Linux/Unix**, **Windows**, or **Network Devices (SNMP)** tabs, then type your credentials.
7. Click **Save**.

Saving Asset Search Criteria

SUMMARY

On the **Asset** tab, you can save configured search criteria so that you can reuse the criteria. Saved search criteria does not expire.

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Perform a search.
4. Click **Save Criteria** .
5. Enter values for the parameters:

Parameter	Description
Enter the name of this search	Type the unique name that you want to assign to this search criteria.
Manage Groups	Click **Manage Groups** to manage search groups. This option is only displayed if you have administrative permissions.
Assign Search to Group(s)	Select the check box for the group you want to assign this saved search. If you do not select a group, this saved search is assigned to the **Other** group by default.
Include in my Quick Searches	Select this check box to include this search in your **Quick Search** list box, which is on the **Assets** tab toolbar.

(Continued)

Parameter	Description
Set as Default	Select this check box to set this search as your default search when you access the **Assets** tab.
Share with Everyone	Select this check box to share these search requirements with all users.

Editing a compliance benchmark

Editing a Compliance Benchmark

SUMMARY

Use the **Compliance Benchmark Editor** in JSA Risk Manager to add or remove tests from the default CIS benchmarks.

1. Click the **Risks** tab.
2. Click **Policy Monitor**.
3. Click **Compliance** to open the **Compliance Benchmark Editor** window.
4. On the navigation menu, click the default CIS benchmark that you want to edit.
5. In the **Compliance** pane, click the **Enabled** checkbox in the row that is assigned to the test that you want to include.

   Click anywhere on a row to see a description of the benchmark test, a deployment rationale, and information on things to check before you enable the test.

   When you are building a custom CIS checklist, be aware that some benchmark tests that are not included by default can take a long time to run. For more information, see the CIS documentation.

"Creating a Benchmark Profile" on page 136

Creating a Benchmark Profile

SUMMARY

To create Center for Internet Security compliance scans, you must configure benchmark profiles. You use CIS compliance scans to test for Windows and Red Hat Enterprise Linux CIS benchmark compliance.

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Administrative** > **Scan Profiles**.
3. On the toolbar, click **Add Benchmark**.
4. If you want to use pre-defined centralized credentials, select the **Use Centralized Credentials** checkbox .

   Credentials that are used to scan Linux operating systems must have root privileges. Credentials that are used to scan Windows operating systems must have administrator privileges.
5. If you are not using dynamic scanning, select a JSA Vulnerability Manager scanner from the **Scan Server** list.
6. To enable dynamic scanning, click the **Dynamic server selection** checkbox.

   If you configured domains in the **Domain Management** window in the **Admin** tab, you can select a domain from the **Domain** list. Only assets within the CIDR ranges and domains that are configured for your scanners are scanned.
7. In the **When To Scan** tab, set the run schedule, scan start time, and any pre-defined operational windows.
8. In the **Email** tab, define what information to send about this scan and to whom to send it.
9. If you are not using centralized credentials, add the credentials that the scan requires in the **Additional Credentials** tab.

   Credentials that are used to scan Linux operating systems must have root privileges. Credentials that are used to scan Windows operating systems must have administrator privileges.
10. Click **Save**.

Creating an Asset Compliance Question

SUMMARY

Create an asset compliance question in Policy Monitor to search for assets in the network that fail CIS benchmark tests.

Policy Monitor questions are evaluated in a top-down manner. The order of Policy Monitor questions impacts the results.

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. From the **Actions** menu, select **New Asset Compliance Question**.
4. In the **What do you want to name this question** field, type a name for the question.
5. Select the level of importance you want to associate with this question from the **Importance Factor** list.
6. From the **Which tests do you want to include in your question** field, select the add (+) icon next to the **test compliance of assets in asset saved searches with CIS benchmarks** test.

   Select this test multiple times, if necessary.
7. Configure the parameters for your tests in the **Find Assets that** field.

   Click each parameter to view the available options for your question. Specify multiple assets saved searches and multiple checklists in this test, if necessary.
8. In the group area, click the relevant check boxes to assign group membership to this question.

   Asset compliance questions must be assigned to a group for inclusion in compliance dashboards or reports.
9. Click **Save Question**.

"Monitoring Asset Compliance Questions" on page 137

Monitoring Asset Compliance Questions

SUMMARY

Monitor asset compliance questions by selecting CIS scan profiles. CIS benchmark scans run against the assets.

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. In the **Questions** pane, select the asset compliance question that you want to monitor.
4. Click **Monitor** to open the **Monitor Results** window.
5. Select a benchmark profile from the **Which benchmark profile to associate with this question** list.

   The selected benchmark scan profile uses a JSA Vulnerability Manager scanner that is associated with a domain. The domain name is displayed in the **Benchmark Profile Details** area. For more information about domain management, see the *Juniper Secure Analytics Administration Guide*.
6. Select the **Enable the monitor results function for this question/simulation** checkbox.
7. Click **Save Monitor**.

   Monitoring begins at the scan start time that you set on the **When To Scan** tab when you created the benchmark scan profile.

"Viewing Scan Results" on page 138

Viewing Scan Results

The **Scan Results** page displays a summary list of the results that are generated by running a scan profile.

The **Scan Results** page provides the following information:

Table 18: Visualizing Scan Result Parameters

Parameter	Description
Profile	The name of the scan profile. Hover your mouse over the **Profile** to display information about the scan profile and the status of the scan.
Schedule	The run schedule that is applied to the scan profile. If you initiated a manual scan, then **Manual** is displayed.
Score	The average Common Vulnerability Scoring System (CVSS) score for the scan. This score helps you prioritize vulnerabilities.

Table 18: Visualizing Scan Result Parameters *(Continued)*

Parameter	Description
Hosts	The number of hosts that are found and scanned when the scan profile ran. Click the **Host** column link to display vulnerability data for the scanned hosts.
Vulnerabilities	The number of different types of vulnerabilities found by a scan. Click the **Vulnerabilities** column link to view all unique vulnerabilities.
Vulnerability Instances	The number of vulnerabilities found by the scan.
Open Services	The number of unique open services found by the scan. A unique open service is counted as a single open service. Click the **Open Services** column link to view vulnerabilities categorized by open service.
Status	The status of the Scan Profile, options include: Stopped - This status is displayed if the scan completed successfully or the scan was canceled. Running - The scan is running. Paused - The scan is paused. Not Started - The scan is not initiated.
Progress	Specifies the progress of the scan. Hover your mouse over the progress bar while the scan is running to display information about the status of a scan.
Start Date/Time	The date and time when the scan profile started to run.
Duration	Displays the time that it took for the scan to complete.

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Scan Results**.

CHAPTER 11

Network Simulations in JSA Risk Manager

Network Simulations in JSA Risk Manager

SUMMARY

Use simulations to define and run exploit simulations on your network. You can create, view, edit, duplicate, and delete simulations.

IN THIS SECTION

You can create simulations that are based on a series of rules that can be combined and configured. After a simulation is complete, you can review the results of the simulation and approve any acceptable or low risk result that is based on your network policy. When you review results, you can approve acceptable actions or traffic from your results.

Simulations can be modeled off a current topology or a topology model.

The **Simulation** page summarizes information about simulations and simulation results.

Simulation results display only after a simulation is complete. After a simulation is complete, the **Results** column lists the dates and the corresponding results of your simulation.

Simulation Tests

SUMMARY

Simulation tests can be configured to ensure that JSA Risk Manager is functioning properly to detect risks.

Parameters that can be configured for simulation tests are underlined. The following table describes the simulation tests that you can configure.

Table 19: Simulation Tests

Test Name	Description	Parameters
Attack targets one of the following IP addresses	Simulates attacks against specific IP addresses or CIDR ranges.	Configure the IP addresses parameter to specify the IP address or CIDR ranges to which you want this simulation to apply.
Attack targets one of the following networks	Simulates attacks that target 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	Simulates attacks that target 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 one of the following reference sets	Simulates attacks that target one or defined reference sets.	Configure the reference sets parameters to specify the reference sets to which you want this simulation to apply.
Attack targets a vulnerability on one of the following ports using protocols	Simulates attacks that target a vulnerability on one or more defined ports.	Configure the following parameters: Open Ports - Specify the ports that you want this simulation to consider. Protocols - Specify the protocol that you want this simulation to consider.

Table 19: Simulation Tests *(Continued)*

Test Name	Description	Parameters
Attack targets assets susceptible to one of the following vulnerabilities	Simulates attacks that target assets that are susceptible to one or more defined vulnerabilities.	Configure the **vulnerabilities** parameter to identify the vulnerabilities that want this test to apply. You can search for vulnerabilities in OSVDB ID, Bugtraq ID, CVE ID, or title.
Attack targets assets susceptible to vulnerabilities with one of the following classifications	Simulates attacks that target an asset that is susceptible to vulnerabilities for one or more defined classifications.	Configure the **classifications** parameter to identify the vulnerability classifications. For example, a vulnerability classification might be Input Manipulation or Denial of Service.
Attack targets assets 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. This simulation filters assets in your network that include the configured CVSS value. Simulates attacks that target an asset that is susceptible to vulnerabilities with a CVSS score greater than 5.	Click **Greater Than 5**, and then select an operator. The default operator is greater than **5**
Attack targets assets susceptible to vulnerabilities disclosed after this date	Simulates attacks that target 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	Simulates attacks that target an asset that is susceptible to vulnerabilities that match the asset name, vendor, version, or service based one or more text entries.	Configure the **text entries** parameter to identify the asset name, vendor, version, or service you want this simulation to consider.

Table 19: Simulation Tests *(Continued)*

Test Name	Description	Parameters
Attack targets assets susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions	Simulates attacks that target an asset that is susceptible to vulnerabilities that match the asset name, vendor, version, or service, which is based one or more regular expressions.	Configure the **regular expressions** parameter to identify the asset name, vendor, version, or service you want this simulation to consider.

The following contributing tests are deprecated and hidden in the Policy Monitor:

- **attack targets a vulnerability on one of the following operating systems**
- **attack targets assets susceptible to vulnerabilities from one of the following vendors**
- **attack targets assets susceptible to vulnerabilities from one of the following products**

The deprecated contributing tests are replaced by other tests.

RELATED DOCUMENTATION

Creating a Simulation | **144**

Duplicating a Simulation | **146**

Manually Running a Simulation | **146**

Creating a Simulation

SUMMARY

You can create simulations that are based on a series of rules that can be combined and configured.

1. Click the **Risks** tab.

2. On the navigation menu, select **Simulation** > **Simulations**.
3. From the **Actions menu**, select **New**.
4. Type a name for the simulation in the **What do you want to name this simulation** parameter.
5. From the **Which model do you want to base this on** drop-down list, select the type of data you want to return. All existing topology models are listed. If you select **Current Topology**, then the simulation uses the current topology model.
6. Choose one of the following options:

Option	Description
Select Use Connection Data	The simulation is based on connection and topology data.
Clear Use Connection Data	The simulation is only based on topology data. If your topology model does not include any data and you clear the **Use Connection Data** checkbox, the simulation does not return any results.

7. From the **Importance Factor** list, 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.
8. From the **Where do you want the simulation to begin** list, 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.
9. Add simulation attack targets to the simulation test.
10. Using the **Which simulations do you want to include in the attack field**, select the **+** sign next to the simulation you want to include.

    The simulation options are displayed in the **Generate a simulation where** window.
11. From the **Generate a simulation where** window, click any underlined parameters to further configure simulation parameters.
12. In the **Run this simulation for** menu, select the number of steps you want to run this simulation (1 - 5).
13. In the steps menu, choose the schedule for running the simulation.
14. In the groups area, select a checkbox for any group you want to assign this simulation.
15. Click **Save Simulation**.
16. To edit an existing simulation, click **Edit** from the **Actions** menu. After you update the parameters, click **Save Simulation**.
17. To delete an existing simulation, click **Delete** from the **Actions** menu. After you update the parameters, click **Save Simulation**.

Duplicating a Simulation

SUMMARY

Duplication simulations can save time and effort.

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. Select the simulation that you want to duplicate.
4. From the **Actions** menu, select **Duplicate**.
5. Type the name for the simulation.
6. Click **OK**.

Manually Running a Simulation

SUMMARY

Use the Simulation Editor to manually run a simulation and override the schedule.

1. Click the **Risks** tab.
2. From the **Actions** menu, select **Run Simulation**.
3. Click **OK**.

The simulation process can take an extended amount of time. While the simulation is running, the **Next Run** column indicates the percentage that it is complete. When complete, the Results column displays the simulation date and time.

If you run a simulation and then make changes that affect the tests that are associated with the simulation, these changes might take up to an hour to display.

Network Configuration Change Simulation

SUMMARY

You can use a topology model to define virtual network models based on your existing network. You can create a network model that is based on a series of modifications that can be combined and configured.

IN THIS SECTION

You can use a topology model to determine the effect of configuration changes on your network by using a simulation.

Topology models provide the following key functions:

- Create virtual topologies for testing network changes.
- Simulate attacks against virtual networks.
- Lower risk and exposure to protected assets through testing.
- Virtual network segments that you can use to confine and test sensitive portions of your network or assets.

To simulate a network configuration change, do the following tasks:

1. Create a topology model.
2. Simulate an attack against the topology model.

Creating a Topology Model

SUMMARY

Create a topology model to simulate the impact of network changes and simulate attacks.

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulations** > **Topology Models**.
3. From the **Actions** list, select **New**.
4. Type a name for the model.

5. Select any modifications that you want to apply to the topology.
6. Configure the tests added to the **Configure model as follows** pane.
7. Click **Save Model**.

Create a simulation for your new topology model.

Simulating an Attack

SUMMARY

Use the simulation feature to simulate an attack on open ports by using protocols such as TCP.

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. From the **Actions** list, select **New**.
4. Type a name for the simulation.
5. Select a topology model that you created.
6. From the **Where do you want the simulation to begin** list, select an origin for the simulation.
7. Add the simulation attack, **Attack targets one of the following open ports using protocols**.
8. For this simulation, click **open ports**, and then add port 22.
9. Click **protocols**, and then select **TCP**.
   SSH uses TCP.
10. Click **Add +** to add the protocol, and then **OK**.
11. Click **Save Simulation**.
12. From the **Actions** list, select **Run Simulation**.
    The results column contains a list that shows the run date of the simulation, and a link to view the results.
13. Click **View Results**.

Simulating an Attack on an SSH Protocol

SUMMARY

Simulate attacks on your network such as a network attack on an SSH protocol.

---

1. Click the **Risks** tab.
2. On the navigation menu, click **Simulation** > **Simulations**.
3. From the **Actions** list, select **New**.
4. Type a name for the simulation.
5. Select **Current Topology**.
6. Select the **Use Connection Data** checkbox .
7. From the **Where do you want the simulation to begin** list, select an origin for the simulation.
8. Add the simulation attack, **Attack targets one of the following open ports using protocols**.
9. For this simulation, click **open ports**, and then add port 22.
10. Click **protocols**, and then select **TCP**.
    SSH uses TCP.
11. Click **Add +** to add the protocol, and then click **OK**.
12. Click **Save Simulation**.
13. From the **Actions** list, select **Run Simulation**.
    The results column contains a list with the date the simulation was run and a link to view the results.
14. Click **View Results**.

A list of assets that have SSH vulnerabilities is displayed in the results, which allows network administrators to approve SSH connections that are allowed or expected in your network. The communications that are not approved can be monitored for events or offenses.

The results that are displayed provide your network administrators or security professionals with a visual representation of the attack path. For example, the first step provides a list of the directly connected assets that are affected by the simulation. The second step lists assets in your network that can communicate to first-level assets in your simulation.

The information that is provided in the attack helps you to strengthen and test your network against thousands of possible attack scenarios.

Viewing Simulation Results

SUMMARY

After a simulation runs, the **Results** column displays a drop-down list that contains the dates when the simulation was generated. Simulation results are retained for 30 days. Results display in the **Results** column only after a simulation runs.

Simulation results provide information on each step of the simulation.

For example, the first step of a simulation provides a list of the directly connected assets that are affected by the simulation. The second step lists assets in your network that can communicate to first-level assets in your simulation.

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. In the Results column, select the date and time of the simulation you want to view by using the list.
4. Click **View Result**. You can view the simulation result information, starting at step 1 of the simulation. The following information is provided:

Table 20: Viewing Simulation Result Information

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 that includes the step that is being displayed.

Table 20: Viewing Simulation Result Information *(Continued)*

Parameter	Description
Assets Compromised	The total number of assets that are 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 JSA Risk Manager does not validate those assets against the database. Therefore, those assets are not considered in the Asset Compromised total. JSA Risk Manager validates assets only in broader IP ranges, such as /24 to determine which assets exist.
Risk Score	Risk score is a calculated value based on the number of results, steps, the number of compromised assets, and the importance factor that is assigned to the simulation. This value indicates the severity level that is associated with the simulation for the displayed step.

Move your mouse pointer over the connection to highlight the path through the network, as defined by the subnet.

The 10 most important assets display when you move your mouse over the connection.

You can move your mouse pointer over a connection to determine the list of assets that are affected by this simulation.

5. View the Results for this Step table to determine the assets that are affected.

Table 21: Viewing Results for this Step Information

Parameter	Description
Approve	Used for approving simulation results. See "Approving simulation results" on page 152.
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.

6. To view the next step of the simulation results, click **Next Step**.

"Approving Simulation Results" on page 152

Approving Simulation Results

SUMMARY

In simulations, you can approve network traffic that is deemed low risk or normal communication on the asset. When you approve results, you filter the result list so that future simulations ignore these approved communications.

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. In the **Results** column, select the date and time of the simulation that you want to view by using the list.
4. Click **View Result**.
5. In the **Results for this step** table, use one of the following methods to approve assets:

Option	Description
Approve Selected	Click the checkbox for each asset that you want to approve, and then click **Approve Selected**.
Approve All	Click **Approve All** to approve all assets that are listed.

6. To view all approved assets, click **View Approved**.

"Revoking a Simulation Approval" on page 152

Revoking a Simulation Approval

SUMMARY

You can revoke an approved connection or communication from a simulation approved list. When an approved simulation result is revoked, any future simulations display non-approved communications in the simulation results.

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. In the `Results` column, select the date and time of the simulation you want to view by using the list.
4. Click **View Result**.
5. Click **View Approved** to view all approved assets.
6. Choose one of the following options:

Option	Description
Revoke Selected	Click the checkbox for each asset that you want to revoke, and then click **Revoke Selected**.
Revoke All	Click **Revoke All** to revoke all the assets that are listed.

Assigning Simulations to Group for Tracking

SUMMARY

Assigning simulations to groups is an efficient way to view and track all simulations. For example, you can view all simulations that are related to compliance.

As you create new simulations, you can assign the simulations to an existing group.

After you create a group, you can drag groups in the menu tree to change the organization.

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**, and then click **Groups**.
3. From the menu, select the group under which you want to create a new group, and click **New**.
4. In the **Name** field, type a name for the new group. The group name can be up to 255 characters in length.
5. In the **Description field,** type a description for the group. The description can be up to 255 characters in length.
6. Click **OK**.

12
CHAPTER

Topology models

Topology Models

SUMMARY

You can use a topology model to define virtual network models based on your existing network.

IN THIS SECTION

You can create a network model based on a series of modifications that can be combined and configured. By creating a network model, you can determine the effect of configuration changes on your network by using a simulation. For more information about simulations, see "Network Simulations in JSA Risk Manager" on page 141.

Topology models provide the following information:

Table 22: 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

SUMMARY

You can create a network model based on a series of modifications that can be combined and configured. By creating a network model, you can determine the effect of configuration changes on your network by using a simulation.

---

1. Click the **Risks** tab.
2. On the navigation menu, click **Simulation** > **Topology Models**
3. From the **Actions** menu, select **New**.
4. In the **What do you want to name this model** field, type a name for the model definition.
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.
6. Configure the tests added to the **Configure model as follows** pane.

   The following table describes the test names and parameters that you can configure.

Table 23: Configuring 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 that you want to add to this rule. In the **Customize Parameter** window, select the **All** checkbox to include all devices, or you can search devices by using one of the following search criteria: **IP/CIDR** - Select the IP/CIDR option and specify the IP address or CIDR that you want to add this rule to. **Hostname** - Select the **Hostname** option and specify the hostname that 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 menu to filter the device list by adapter. **Vendor** - Select the **Vendor** option and use the menu 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 that you want to add to this rule. **CIDRs** - Select any destination IP addresses or CIDR ranges that you want to add to this rule. **protocols** - Specify the protocols that you want to add to this rule. To include all protocols, select the **All** checkbox. **ports** - Specify the ports that you want to add to this rule. To include all ports, select the **All** checkbox.

Table 23: Configuring 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** checkbox. 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 that you want this topology model to include. **CIDRs** - Specify any destination IP addresses or CIDR ranges that 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 by 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** checkbox.
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** checkbox.

7. When the test is displayed in the pane, the configurable parameters are underlined. Click each parameter to further configure this modification for your model. In the groups area, select the checkbox to assign groups to this question.
8. Click **Save Model**.

You can edit, duplicate, and delete a topology model from the **Actions** menu.

RELATED DOCUMENTATION

Network Simulations in JSA Risk Manager | 141

Group Topology Models

SUMMARY

You can group and view your topology models based on your chosen criteria.

IN THIS SECTION

Categorizing your topology model is an efficient way to view and track your models.

As you create new topology models, you can assign the topology models to an existing group. For information about assigning a group, see "Creating a topology model" on page 155.

Viewing Groups

SUMMARY

You can view topology models by using groups. For example, you can view all topology models related to compliance.

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Topology Models**.
3. Using the **Group** list, select the group that you want to view.

Creating a Group

SUMMARY

You can create a group to efficiently view and track topology models.

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Topology Models**.
3. Click **Groups**.
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.
5. Click **New**.
6. Type the name that you want to assign to the new group. The name can be up to 255 characters in length.
7. Type a description for the group. The description can be up to 255 characters in length.
8. Click **OK**.
9. 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.

Assigning a Topology to a Group

SUMMARY

You can assign a topology model to a group.

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. Select the topology model that you want to assign to a group.
4. From the **Actions** menu, select **Assign Group**.
5. Select the group that you want the question to be assigned to.
6. Click **Assign Groups**.

Copying or Deleting Group Items

SUMMARY

Using the groups functionality, you can copy a topology model to one or many groups. You can also delete individual items from a group.

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulations** > **Topology Models**.
3. Click **Groups**.
4. To copy a topology model, use the following steps:
   a. From the menu tree, select the simulation question that you want to copy to another group, and then click **Copy**.
   b. Select the checkbox for the group to which you want to copy the simulation, and then click **Copy**.
5. To delete an item or group, use the following steps:
   a. From the menu tree, select the top-level group.
   b. From the list of groups, select the item or group you want to delete.
   c. Click **Remove**, and then click **OK**.

13
CHAPTER

Reports

Reports

SUMMARY

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

IN THIS SECTION

The following report options are specific to JSA Risk Manager:

Table 24: Report Options for JSA Risk Manager

Report option	Description
Connections	The connection diagrams for your network devices that occurred during your specified timeframe.
Device rules	The rules configured on your network device during your specified timeframe. You can view the following rule types for one or many network devices by 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	Produces a table with the name, configuration date and time, and a definition for any object reference groups that are not in use on the device. An object reference group is a collection of IP addresses, CIDR addresses, hostnames, ports, or other device parameters, which are grouped and assigned to rules on the device.

Creating a Report

SUMMARY

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

IN THIS SECTION

1. Click the **Reports** tab.
2. From the **Actions** list, select **Create**.
3. Click **Next** to move to the next page of the Report Wizard.
4. Select the frequency for the reporting schedule.
   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.
5. In the Allow this report to generate manually pane, select **Yes** to enable or **No** to disable manual generation of this report. This option is not available for manually generated reports.
6. Click **Next**.
7. Choose a layout of your report, and then click **Next**.
   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 many 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.
8. Enter a report title. The title can be up to 100 characters in length. Do not use special characters.
9. Choose a logo. The JSA logo is the default logo. For more information about branding your report, see the *Juniper Secure Analytics Administration Guide*.
10. From the **Chart Type** list, select one of the JSA Risk Manager specific reports.
11. Configure the report data for your chart.
12. Click **Save Container Details**, and then click **Next**.
13. Select report formats. You can select multiple options.
    Device Rules and Unused Object Rules reports support only the PDF and HTML report formats.
14. Click **Next**.
15. Select the distribution channels that you want for your report, and then click **Next**.

For more information, see "Generated Report Distribution Options" on page 165.

16. Type a description for this report. The description is displayed on the **Report Summary** page and in the generated report distribution email.
17. Select the groups that you want to assign this report to. For more information about groups, see Managing Reports in the *Juniper Secure Analytics Administration Guide*.
18. To run this report when the wizard setup is complete, click **Yes**. Click **Next** to view the report summary. You can select the tabs available on the summary report to preview the report selections.
19. Click **Finish**.

The report immediately generates. If you cleared the **Would you like to run the report now** checkbox 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 reconfigure 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.

Generated Report Distribution Options

SUMMARY

You can specify Report Console or email for report distribution options.

IN THIS SECTION

The following table describes the parameters for these distribution options.

Table 25: Generated Report Distribution Options

Option	Description
Report Console	Select this checkbox to send the generated report to the **Reports** tab. This distribution channel is the default.
Select the users that should be able to view the generated report	This option is only displayed after you select the **Report Console** checkbox. From the list of users, select the JSA Risk Manager users that you want to grant permission to view the generated reports. You must have appropriate network permissions to share the generated report with other users. For more information about permissions, see the *Juniper Secure Analytics Administration Guide*.

Table 25: Generated Report Distribution Options *(Continued)*

Option	Description
Select all users	This option is only displayed after you select the **Report Console** checkbox. Select this checkbox if you want to grant permission to all JSA Risk Manager users to view the generated reports. You must have appropriate network permissions to share the generated report with other users. For more information about permissions, see the *Juniper Secure Analytics Administration Guide*.
Email	Select this checkbox if you want to distribute the generated report by using email.
Enter the report distribution email address(es)	This option is only displayed after you select the **Email** checkbox. Type the email address for each generated report recipient; separate a list of email addresses with commas. The maximum characters for this parameter are 255.
Include Report as attachment (non-HTML only)	This option is only displayed after you select the **Email** checkbox. Select this checkbox to send the generated report as an attachment.
Include link to Report Console	This option is only displayed after you select the **Email** checkbox. Select this checkbox to include a link the Report Console in the email.

Connections Chart

SUMMARY

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.

You can customize the data that you want to display in the generated report. You can configure the chart to plot data over a configurable time period. This functionality helps you to detect connection trends.

The following table provides configuration information for the Connections Chart container.

Table 26: 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 checkbox to change the automatically created subtitle. Type a title to a maximum of 100 characters.
Graph Type	From the list, select the type of graph to display on the generated report. The following options are included: **Bar** - Displays the data in a bar chart. This graph type is the default. 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, select the number of connections to be displayed in the generated report.
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 that you want for the report, or select the date by using the **Calender** icon. The default is the current date. 2. From the list boxes, select the start time that you want for the report. Time is available in half-hour increments. The default is 1:00 AM. 3. From the **To** list, type the end date that you want for the report, or select the date by using the **Calender** icon. The default is the current date. 4. From the lists, select the end time that you want for the report. Time is available in half-hour increments. The default is 1:00 AM.

Table 26: Connections Chart Parameters *(Continued)*

Parameter	Description
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 lists, select the time period that you want for the generated report. Time is available in half-hour increments. The default is 1:00 am.
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 lists, select the time period that 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 lists, select the time period that you want for the generated report. The default is 1st to 31st.
Graph Content	
Group	From the list, select a saved search group to display the saved searches that belong to that group in the **Available Saved Searches** list.

Table 26: Connections Chart Parameters *(Continued)*

Parameter	Description
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. Typing the name of a known saved search in the **Type Saved Search or Select from List** field is another way to filter the list.
Create New Connection Search	Click **Create New Connection Search** to create a new search.

Device Rules Charts

SUMMARY

You can use the Device Rules chart to view firewall rules and the event count of firewall rules that are triggered in your network.

Device Rule reports are used 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 create better understanding of what rules are accepted, denied, unused, or untriggered across a single device, a specific adapter, or multiple devices. Reports allow JSA Risk

Manager to automate reporting about the status of your device rules and display the reports on the JSA 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 27: Device Rules Chart Parameters

Parameter	Description
Container Details - Device Rules	
Limit Rules to Top	From the list, 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-type rules based on the event count across all devices that are visible to JSA Risk Manager.

Table 27: Device Rules Chart Parameters *(Continued)*

Parameter	Description
Type	Select the type of device rules to display in the report. The following display options can be selected: **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 timeframe 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 timeframe 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 timeframe 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 timeframe 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 timeframe 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 that is creating the shadow. The rules can never trigger on your device because they are shadowed by a proceeding rule on the device. **IMPORTANT**: Shadowed rule reports can be run only against a single device. These rules have zero event counts for the timeframe you specified for the report and are identified with an icon in the Status column.

Table 27: Device Rules Chart Parameters *(Continued)*

Parameter	Description
Date/Time Range	Select the timeframe 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 timeframe 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 timeframe.
Timezone	Select the timezone that you want to use as a basis for your report. The default timezone is based on the configuration of your JSA Console. When you configure the Timezone parameter for your report, consider the location of the devices that are associated with the reported data. If the report uses data that spans multiple time zones, the data that is used for the report is based on the specific time range of the time zone. For example, you can configure your JSA Console. for Eastern Standard Time (EST) and schedule a daily report between 1pm and 3pm. Then, if you 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 a specific value. Using the Targeted Data Selection options, you can create a report to view your device rules from a defined time span. You also can include data only from the selected hours and days. For example, you can schedule a report to run from October 1 to October 31. From there, you can 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. **IMPORTANT**: **Targeted Data Selection**

Table 27: 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, you can create a report to display the top 10 most denied rules. An aggregate report displays the top 10 most denied rules across all of the devices that you 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, you can create a report to display the top 10 most denied rules. An aggregate report displays the top 10 most denied rules for each device that you selected for the report. This report returns the top 10 results for every device that is selected for the report. If you selected five devices, the report returns 50 results. **IMPORTANT**: Shadowed rule reports are only capable of displaying one report per device.

Table 27: 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 JSA Risk Manager in your report. **Adapter** - From the list, select an adapter type to include in your report. Only one adapter type can be selected from the list for a report. **Specific Devices** - Select this option to include only specific devices in your report. You can select and add devices to your report on the **Device Selection** window. 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 Charts

SUMMARY

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 hostnames that are unused by your network device.

When you configure a device unused objects container, you configure values for the following parameters:

Table 28: Device Unused Objects Report Parameters

Parameter	Description
Container Details - Device Unused Objects	
Limit Objects to Top	From the list, select the number of rules to be displayed in the generated report.
Devices	Select the devices included in the report. The options include: **All Devices** - Select this option to include all devices in JSA Risk Manager in your report. **Adapter** - From the list, select an adapter type to include in your report. Only one adapter type can be selected from the list for a report. **Specific Devices** - Select this option to include only specific devices in your report. Select and add devices to your report on the **Device Selection** window. 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**.

Editing a Report

SUMMARY

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

1. Click the **Reports** tab.
2. Select the report that you want to edit.
3. From the **Actions** list, select **Edit**.
4. Select the frequency for the new reporting schedule.
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.
6. Click **Next** to move to the next page of the Report Wizard.
7. Configure the layout of your report:
   a. From the **Orientation** list, select the page orientation.
   b. Select a layout option for your JSA Risk Manager report.
   c. Click **Next**.
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, select a logo. The JSA logo is the default logo. For more information about branding your report, see the *Juniper Secure Analytics Administration Guide*.
9. Configure the container for your report data:
   a. Click **Define**.
   b. Configure the report data for your chart.
   c. Click **Save Container Details**.
   d. If needed, repeat steps these steps to edit more containers.
   e. Click **Next** to move to the next page of the Report Wizard.

10. Click **Next** to move to the next step of the Report Wizard.
11. Select the check boxes for the report formats. You can select more than one option.
    JSA Risk Manager-specific reports, such as Device Rule and Device Unused Object reports support only PDF and HTML formats.
12. Click **Next** to move to the next page of the Report Wizard.
13. Select the distribution channels for your report.
14. Click **Next** to go to the final step of the Report Wizard.
15. Type a description for this report. The description is displayed on the **Report Summary** page and in the generated report distribution email.
16. Select the groups to which you want to assign this report. For more information about groups, see Managing Reports in the *Juniper Secure Analytics Administration Guide*.
17. To run this report when the wizard setup is complete, select **Yes**.
18. 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.
19. Click **Finish**.

Duplicating a Report

SUMMARY

You can duplicate any report, saving time and effort.

1. Click the **Reports** tab.
2. Select the report that you want to duplicate.
3. From the **Actions** list, click **Duplicate**.
4. Type a new name, without spaces, for the report.

Manually Generating a Report

SUMMARY

Reports can be started manually. 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 denials, then manually generate the report, the weekly report still generates on the schedule you initially configured.

1. Click the **Reports** tab.
2. Select the report that you want to generate.
3. Click **Run Report**.
   When a 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 that 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 runs next.
4. To refresh the view, including the information in the **Next Run Time** column, click **Refresh**.

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

Sharing a Report

SUMMARY

When you share a report with other users, 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.

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.

1. Click the **Reports** tab.
2. Select the reports that you want to share.
3. From the **Actions** list, click **Share**.
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.
5. Click **Share**.

   For more information about reports, see the *Juniper Secure Analytics Users Guide*.

14

CHAPTER

Audit Log Data

Audit Log Data

SUMMARY

Changes that are made by JSA Risk Manager users are recorded in the **Log Activity** tab of JSA.

IN THIS SECTION

All logs display in the Risk Manager Audit category. For more information about using the **Log Activity** tab in JSA, see the *Juniper Secure Analytics Users Guide*.

Logged Actions

SUMMARY

Actions are logged for components.

The following table lists the categories and corresponding actions that are logged.

Table 29: Logged Actions

Category	Action
Policy Monitor	Create a question.
	Edit a question.
	Delete a question.
	Submit a question manually.

Table 29: Logged Actions *(Continued)*

Category	Action
	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.
Simulations	Create a simulation.
	Edit a simulation.
	Delete a simulation.
	Manually run a simulation.
	Automatically run a simulation.

Table 29: Logged Actions *(Continued)*

Category	Action
	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 unsuccessful.
	After a backup job is completed processing and the configuration was persisted, no changes discovered.
	After a backup job is completed processing and the configuration was persisted, changes were discovered.

Table 29: Logged Actions *(Continued)*

Category	Action
	After a backup job is completed processing and the configuration was persisted, unpersisted changes were discovered.
	After a backup job is completed processing and the configuration that was previously persisted no longer lives on the device.
	Adapter operation attempt began, which includes protocols and credentials.
	Adapter operation attempt was successful, including the protocols and credentials.

Viewing User Activity

SUMMARY

You can view user activity for JSA Risk Manager users.

1. Click the **Log Activity** tab. If you previously saved a search as the default, the results for that saved search is displayed.
2. Click **Search** > **New Search** to create a search.
3. In the **Time Range** pane, select an option for the time range you want to capture for this search.
4. In the **Search Parameters** pane, define your search criteria:
   a. From the first list, select **Category**.
   b. From the **High Level Category** drop-down list, select **Risk Manager Audit**.
   c. To refine your search, select a category from the **Low Level Category** drop-down list.
5. Click **Add Filter**.
6. Click **Filter** to search for JSA Risk Manager events.

Viewing the JSA Risk Manager Log File

SUMMARY

Audit logs, which are stored in plain text, 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 audit.1.gz. The file number increments each time a log file is archived. JSA Risk Manager can store up to 50 archived log files.

The maximum size of any audit message (not including date, time, and hostname) is 1024 characters.

Each entry in the log file displays by using the following format.

```
<date_time> <host name> <user>@<IP address>
(thread ID) [<category>] [<sub-category>]
[<action>] <payload>
```

The following table describes the parameters that are used in the log file.

Table 30: Viewing Audit Log File Information

Parameter	Description
<date_time>	The date and time of the activity in the format: Month Date HH:MM:SS.
<host name>	The hostname of the Console where this activity was logged.
<user>	The name of the user that completed the action.
<IP address>	The IP address of the user that completed the action.
(thread ID)	The identifier of the Java thread that logged this activity.
<category>	The high-level category of this activity.
<sub-category>	The low-level category of this activity.

Table 30: Viewing Audit Log File Information *(Continued)*

Parameter	Description
<action>	The activity that occurred.
<payload>	The complete record that changed, if any.

1. Using SSH, log in to your JSA Console as the root user.
2. Using SSH from the JSA Console, log in to the JSA Risk Manager appliance as a root user.
3. Go to the following directory: **/var/log/audit**.
4. Open your audit log file.

Log File Details

SUMMARY

Administrators use JSA Risk Manager log files to view user activity and to troubleshoot system issues.

IN THIS SECTION

The following table describes the location and content of JSA Risk Manager log files.

Table 31: JSA Risk Manager Log Files

Log file name	Location	Description
audit.log	**/var/log/audit/**	Contains the current audit information.
audit.*<1-50>*.gz	**/var/log/audit/**	Contains archived audit information. When the **audit.log** file reaches 200 MB, it is compressed and renamed to **audit.1.gz**. The file number increments each time a log file is archived. JSA Risk Manager can store up to 50 archived log files.
qradar.log	**/var/log/**	Contains all process information that is logged by the JSA Risk Manager server.

Table 31: JSA Risk Manager Log Files *(Continued)*

Log file name	Location	Description
qradar.error	**/var/log/**	All exceptions and `System.out` and `System.err` messages that are generated by the JSA Risk Manager server are logged in this file.