



Extreme Networks Security Risk Manager User Guide

Copyright © 2016 All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:

www.extremenetworks.com/company/legal/trademarks

Support

For product support, including documentation, visit: <http://www.extremenetworks.com/support/>

For information, contact:

Extreme Networks, Inc.

145 Rio Robles

San Jose, California 95134

USA

Table of Contents

Introduction to Extreme Networks Security Risk Manager.....	6
Text Conventions.....	6
Providing Feedback to Us.....	7
Getting Help.....	7
Related Publications.....	8
Chapter 1: What's new for users in Risk Manager V7.7.2.7.....	10
Chapter 2: Extreme Networks Security Risk Manager.....	11
Supported web browsers	11
Access the Extreme Networks Security Risk Manager user interface.....	12
Unsupported features in Extreme Networks Security Risk Manager.....	12
Chapter 3: Overview of Risk Manager features.....	13
Chapter 4: Configure access to Risk Manager.....	16
Configuring system settings.....	16
Updating the system time.....	17
Chapter 5: Configuration Source Management.....	19
Credentials.....	20
Device discovery.....	21
Import devices.....	22
Manage devices.....	24
Viewing devices.....	24
Adding a device.....	24
Editing devices.....	24
Deleting a device.....	25
Filtering the device list.....	25
Obtaining device configuration.....	26
Collecting neighbor data.....	26
Manage backup jobs.....	27
View backup jobs.....	27
Viewing backup job status and logs.....	27
Adding a backup job.....	27
Editing a backup job.....	29
Rename a backup job.....	30
Deleting a backup job.....	30
Configure protocols.....	30
Configuring the discovery schedule.....	32
Chapter 6: Connections.....	34
Viewing connections.....	34
Use graphs to view connection data.....	36
Search for connections.....	39
Exporting connections.....	44
Chapter 7: Configuration monitor.....	45
Searching device rules.....	45
Comparing the configuration of your network devices.....	46

Log source mapping.....	47
Chapter 8: Filtering device rules by user or group.....	49
Chapter 9: Network topology graph.....	50
Topology graph searches.....	50
Adding an intrusion prevention system (IPS).....	52
Topology device groups.....	52
Use case: Visualize the attack path of an offense.....	52
Chapter 10: Policy Monitor.....	54
Policy Monitor questions.....	55
Policy Monitor question parameters.....	55
Creating an asset question.....	65
Creating a question that tests for rule violations.....	67
Submitting a question.....	68
Evaluation of results from policy monitor questions.....	72
Policy question monitoring.....	73
Group questions.....	74
Export and import policy monitor questions.....	75
Integration with Vulnerability Manager.....	76
Monitoring firewall rule event counts of Check Point devices.....	77
Policy Monitor use cases.....	82
CIS benchmark scans.....	83
Chapter 11: Policy Management.....	91
Chapter 12: Network simulations in Extreme Networks Security Risk Manager.....	92
Simulations.....	92
Simulation of a network configuration change.....	96
Simulating an attack on an SSH protocol.....	97
Managing simulation results.....	98
Monitoring simulations.....	100
Grouping simulations.....	101
Chapter 13: Topology models.....	102
Creating a topology model.....	102
Editing a topology model.....	104
Duplicating a topology model.....	104
Deleting a topology model.....	104
Group topology models.....	104
Chapter 14: Managing Extreme Networks Security Risk Manager reports.....	107
Manually generating a report.....	107
Use the report wizard.....	108
Creating a report.....	108
Editing a report.....	110
Duplicating a report.....	111
Sharing a report.....	111
Configuring charts.....	111
Chapter 15: Audit log data.....	117
Logged actions.....	117
Viewing user activity.....	119

Viewing the log file.....	119
Log file details.....	120
Appendix A: Glossary.....	121
A.....	121
C.....	122
M.....	122
N.....	122
R.....	122
S.....	122
T.....	122
V.....	123
Index.....	124

Introduction to Extreme Networks Security Risk Manager

This information is intended for use with Extreme Networks Security Risk Manager. Risk Manager is an appliance that is used to monitor device configurations, simulate network changes, and prioritize the risks and vulnerabilities in your network.

This guide contains instructions for configuring and using Extreme Networks Security Risk Manager on a Extreme SIEM console.

Intended audience

System administrators responsible for configuring and using Risk Manager must have administrative access to Extreme SIEM and to your network devices and firewalls. The system administrator must have knowledge of your corporate network and networking technologies.

Statement of good security practices

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

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons




Icon	Notice Type	Alerts you to...
	General Notice	Helpful tips and notices for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.

Table 1: Notice Icons (continued)



Icon	Notice Type	Alerts you to...
	Warning	Risk of severe personal injury.
	New	This command or section is new for this release.

Table 2: Text Conventions

Convention	Description
Screen displays	This typeface indicates command syntax, or represents information as it appears on the screen.
The words enter and type	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as [Return] or [Esc] . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del]
<i>Words in italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at internalinfodev@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- **Global Technical Assistance Center (GTAC) for Immediate Support**
 - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
 - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- **GTAC Knowledge** — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.

- **The Hub** — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- **Support Portal** — Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related Return Material Authorization (RMA) numbers

Related Publications

The ExtremeSecurity product documentation listed below can be downloaded from <http://documentation.extremenetworks.com>.

ExtremeSecurity Analytics

- *Extreme Security Release Notes*
- *Extreme SIEM Administration Guide*
- *Extreme SIEM Getting Started Guide*
- *Extreme SIEM High Availability Guide*
- *Extreme SIEM User Guide*
- *Extreme SIEM Tuning Guide*
- *ExtremeSecurity API Reference Guide*
- *ExtremeSecurity Ariel Query Language Guide*
- *ExtremeSecurity Application Configuration Guide*
- *ExtremeSecurity DSM Configuration Guide*
- *ExtremeSecurity Hardware Guide*
- *ExtremeSecurity Installation Guide*
- *Extreme Networks Security Juniper NSM Plug-in User Guide*
- *ExtremeSecurity Log Manager Administration Guide*
- *ExtremeSecurity Log Manager Users Guide*
- *Migrating ExtremeSecurity Log Manager to Extreme SIEM*
- *ExtremeSecurity Managing Log Sources Guide*
- *ExtremeSecurity Offboard Storage Guide*
- *ExtremeSecurity Release Notse*
- *ExtremeSecurity Risk Manager Adapter Configuration Guide*

- *ExtremeSecurity Risk Manager Getting Started Guide*
- *ExtremeSecurity Risk Manager Installation Guide*
- *ExtremeSecurity Troubleshooting System Notifications Guide*
- *ExtremeSecurity Upgrade Guide*
- *ExtremeSecurity Vulnerability Manager User Guide*
- *ExtremeSecurity Vulnerability Assessment Configuration Guide*
- *ExtremeSecurity WinCollect User Guide*



1 What's new for users in Risk Manager V7.7.2.7

Enhancements to searching device rules by user or group

Use the enhanced search functions to search device rules by user or group. **Search Criteria** fields are added to the **Rule Search** page to enhance your search experience when you search device rules by users and groups. [Learn more...](#)

Search by users or groups in a topology path search

You can refine your topology path search results by filtering on users and groups and view only the rules that impact your selected users or groups on the selected path. [Learn more...](#)

2 Extreme Networks Security Risk Manager

Supported web browsers

Access the Extreme Networks Security Risk Manager user interface

Unsupported features in Extreme Networks Security Risk Manager

Risk Manager is accessed by using the **Risks** tab on your Extreme Networks SIEM Console.

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

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 ExtremeSecurity processes. In 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 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 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.

Supported web browsers

When you access the ExtremeSecurity system, you are prompted for a user name and a password. The user name and password must be configured in advance by the administrator.

The following table lists the supported versions of web browsers.

Table 3: Supported web browsers for ExtremeSecurity products

Web browser	Supported versions
Mozilla Firefox	38.0 Extended Support Release
64-bit Microsoft™ Internet Explorer with Microsoft™ Edge mode enabled.	11.0
Google Chrome	Version 46

Enabling document mode and browser mode in Internet Explorer

- 1 In your Internet Explorer web browser, press F12 to open the **Developer Tools** window.
- 2 Click **Browser Mode** and select the version of your web browser.
- 3 Click **Document Mode**, and select the **Internet Explorer standards** for your Internet Explorer release.

Access the Extreme Networks Security Risk Manager user interface

You access Risk Manager through the Extreme Networks SIEM Console. Use the information in the following table when you log in to your Extreme Security Console.

Table 4: Default login information for Risk Manager

Login information	Default
URL	https://<IP address>, where <IP address> is the IP address of the Extreme Security Console.
User name	admin
Password	The password that is assigned to Risk Manager during the installation process.
License key	A default license key provides access to the system for 5 weeks.

Unsupported features in Extreme Networks Security Risk Manager

The following features are not supported in Risk Manager:

- High availability (HA)
- Dynamic Routing for Border Gateway Protocol (BGP)
- IPv6
- Non-contiguous network masks
- Load-balanced routes

3 Overview of Risk Manager features

The following list is an overview of the features that are provided by Risk Manager to monitor and manage risk in your network.

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 configuration monitor to review and compare device configurations, 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 from 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 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 Extreme Networks Security Risk Manager.

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

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

Policy Management

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

The 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.

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

Configuration Source Management

Configure **Configuration Source Management** to get device configuration information from the devices in your network, which give 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 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

4 Configure access to Risk Manager

Configuring system settings Updating the system time

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

Administrators can do the following tasks:

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

Configuring system settings

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

If you need to make network configuration changes, such as an IP address change to your Extreme Security Console and managed host systems after you install your ExtremeSecurity deployment, use the `qchange_netsetup` utility. For more information about network settings, see the [ExtremeSecurity Risk Manager Installation Guide](#).

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

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 Click the **System and License Management** icon.
- 4 From the **Display** menu, select **Systems**.
- 5 Select the host for which you want to configure firewall access settings.
- 6 From the **Actions** menu, click **View and Manage System**.



Note

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.

- 7 To configure your local firewall to allow access to this host from specified devices outside of your QRadar 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.
- 8 To configure network interfaces on your ExtremeSecurity 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 [Extreme SIEM Administration Guide](#).

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

- 9 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 host name or IP address of the email server that you want to use.

If you don't have an email server and you want to use the email server that ExtremeSecurity provides, type `localhost` to provide local email processing.

If you configure the mail server setting as `localhost`, then the mail messages do not leave the ExtremeSecurity box. If you want external mail delivery, use a valid mail relay server.



Note

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

- 10 Click **Save**.

Updating the system time

For more information about configuring the system time on your Console, and synchronizing time with managed hosts in your deployment, see the IBM Security QRadar Administration Guide.

- 1 Use SSH to log in to the Extreme Security Console as the root user.
- 2 Edit the `ntp.conf` file.


```
vi /etc/ntp.conf
```
- 3 In the `server` section of the `ntp.conf` file, you can leave the existing server entries or replace them with your own internal (Network Time Protocol) NTP server.

Server entries in the `ntp.conf` file begin with `'server'`.

You can use public servers from the [NTP project](http://www.ntp.org/) at (<http://www.ntp.org/>).

```
server 0.rhel.pool.ntp.org iburst
server 1.rhel.pool.ntp.org iburst
server 2.rhel.pool.ntp.org iburst
server 3.rhel.pool.ntp.org iburst
```

If you use public NTP servers, check that your firewall allows outbound NTP requests.

- 4 Save changes and close the file.
- 5 Enable the `ntpd` service to run at run level 3.

```
chkconfig --level 3 ntpd on
```

- 6 Verify that the `ntpd` service is enabled to run at restart.

```
chkconfig --list ntpd
```

Verify that `3:on` displays in the output. This confirms that the service is enabled.

```
ntpd 0:off 1:off 2:off 3:on 4:off 5:off 6:off
```

You must shut down services before you manually synchronize time with the NTP server.

- 7 To prevent data collection errors when you change the system time, shut down ExtremeSecurity services.

```
service hostcontext stop
```

```
service tomcat stop
```

```
service hostservices stop
```

- 8 Synchronize the time with your NTP server.

```
ntpdate <ntp.server.address>
```

- 9 Start the `ntpd` service.

```
service ntpd start
```

- 10 Restart ExtremeSecurity services.

```
service hostservices start
```

```
service tomcat start
```

```
service hostcontext start
```

- 11 Synchronize the time on all managed hosts with your Extreme Security Console by typing the following command.

```
/opt/qradar/support/all_servers.sh /opt/qradar/bin/time_sync.sh
```

- 12 From the **Admin** tab, click **Advanced > Deploy Full Configuration**, to restart services on all ExtremeSecurity managed hosts.

Time is now synchronized between the Extreme Security Console and the managed hosts.

5 Configuration Source Management

Credentials
Device discovery
Import devices
Manage devices
Viewing devices
Adding a device
Editing devices
Deleting a device
Filtering the device list
Obtaining device configuration
Collecting neighbor data
Manage backup jobs
View backup jobs
Viewing backup job status and logs
Adding a backup job
Editing a backup job
Rename a backup job
Deleting a backup job
Configure protocols
Configuring the discovery schedule

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 Extreme SIEM.

To set up your configuration sources, you must:

- 1 Configure your [device credentials](#).
- 2 Discover or import devices. There are two ways to add network devices to Risk Manager; [discover devices using Configuration Source Management](#) or [import a list of devices](#) from a CSV file using Device Import.
- 3 [Obtain device configuration](#) from each of your devices.
- 4 [Manage backup jobs](#) to ensure that all updates to device configurations are captured.
- 5 Set up the [discovery schedule](#) to ensure that new devices are automatically discovered.

You use Configuration Source Management to:

- Add, edit, search, and delete configuration sources. For more information, see [Manage devices](#).

- Configure or manage communication protocols for your devices. For more information, see [Configure protocols](#).

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

For detailed information about adapters used to communicate with devices from specific manufacturers, see [ExtremeSecurity Risk Manager Adapter Configuration Guide](#).

Credentials

Administrators use Configuration Source Management to input device credentials, which give 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 user name, 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, if all the firewalls in your organization have the same user name and password, then the credentials that are associated with 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 [ExtremeSecurity Risk Manager Adapter Configuration Guide](#).

You can configure your 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

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, 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, Risk Manager compiles the credentials again to ensure success.

Configuring credentials for Extreme Networks Security Risk Manager

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

- 1 Click the **Admin** tab.
- 2 In the navigation pane, click **Plug-ins**.
- 3 In the **Risk Manager** pane, click **Configuration Source Management**.
- 4 On the navigation menu, click **Credentials**.
- 5 On the **Network Groups** pane, click the **Add (+)** icon.
- 6 Type a name for a network group, and then click **OK**.
- 7 Move the network group that you want to have first priority to the top of the list. You can use the **Move Up** and **Move Down** arrow icons to prioritize a network group.
- 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.
- 9 In the **Credentials** pane, click the **Add (+)** icon.
- 10 Type a name for the new credential set, and then click **OK**.
- 11 Type values for the parameters:

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

- 12 Move the credential set you want to make first priority to the top of the list. Use the **Move Up** and **Move Down** arrow icons to prioritize a credential set.
- 13 Repeat for each credential set that you want to add.
- 14 Click **OK**.

Device discovery

The discovery process uses the Simple Networks Management Protocol (SNMP) and command line (CLI) to discover network devices.

After you configure an IP address or CIDR range, the discovery engine performs a TCP scan against the IP address to determine if port 22, 23, or 443 are monitoring for connections. If the TCP scan is successful, and SNMP query is configured to determine the type of device, the SNMP Get Community String is used based on the IP address.

This information is used to determine which adapter the device should be mapped to when added. Extreme Networks Security 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. Risk Manager adds a device using the IP address for the lowest numbered interface on the device (or lowest loopback address, if any).

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

Discovering devices

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

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 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.
 - d Click **OK**.
 - e In the **Add address (IP, CIDR, Wildcard, or Range)** field, type the IP address or CIDR range.
 - f Click **(+)** to add the IP address or CIDR range.
 - g Select the **SNMP** protocol.
 - h 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** check box.
- 9 Click **Run**.

Import devices

The device import list can contain up to 5000 devices, but the list must contain one line for each adapter and its associated IP address in the import file.

For example,

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

Where:

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

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

Table 5: Device import examples

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

Importing a CSV file

If you import a list of devices and then make a change to 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 re-importing your master device list.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 3 In the **Plug-Ins** pane, click **Device Import**.
- 4 Click **Browse**.
- 5 Locate your CSV file, click **Open**.
- 6 Click **Import Devices**.

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

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

Manage devices

From the devices tab, you can view, add, edit, and delete devices. You can also filter the device list, obtain device configuration information, collect neighbor data and discover devices that are in your deployment.

Viewing devices

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 3 In the **Risk Manager** pane, click **Configuration Source Management**.
- 4 Click the **Devices** tab.
- 5 To view detailed information for a device configuration, select the device you want to view and click **Open**.

Adding a device

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

For information about adding multiple devices, see [Import devices](#).

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 3 In the **Risk Manager** pane, click **Configuration Source Management**.
- 4 On the navigation pane, click **Add Device**.
- 5 Configure values for the following parameters:

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

- 6 Click **Add**.
If necessary, click **Go** to refresh the adapter list.

Editing devices

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 3 In the **Risk Manager** pane, click **Configuration Source Management**.
- 4 Select the device you want to edit.
- 5 Click **Edit**.
- 6 Configure values for the following parameters:

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

- 7 Click **Save**.

Deleting a device

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 3 In the **Risk Manager** pane, click **Configuration Source Management**.
- 4 Click the **Devices** tab.
- 5 Select the device that you want to delete.
- 6 Click **Remove**.
- 7 Click **Yes** to delete the device.

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

Filtering the device list

Extreme Networks Security 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 can be applied to the device list to help you find devices faster.

Table 6: Filter types for 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 on which you want to search in the IP/CIDR field. For example, if you type a search criteria of 10.100.22.6, the search results return a device with an IP address of 10.100.22.6. If you type a CIDR range of 10.100.22.0/24, all devices in the 10.100.22.* are returned.
Admin IP Address	Filters the device list based on the administrative Interface IP address. An administrative IP address is the IP address that uniquely identifies a device. Type the IP address or CIDR range on which you want to search in the IP/CIDR field.
OS Version	Filters the device list based on the operating system version devices are running. Select values for the following parameters: Adapter - Using the drop-down list, select the type of adapter you want to search. Version - Using the drop-down list, select the search criteria for the version. For example, greater than, less than, or equal to the specified value. Type the version number in the field on which you want to search. If you do not select a search option for Version, the results include all devices that are configured with the selected adapter, regardless of version.
Model	Filters the device list based on the vendor and model number. Configure values for the following parameters: Vendor - Using the drop-down list, select the vendor you want to search. Model - Type the model you want to search.
Hostname	Filters the device list based on the hostname. Type the host name on which you want to search in the Hostname field.

- 1 Click the **Admin** tab.

- 2 On the navigation menu, click **Plug-ins**.
- 3 In the Risk Manager pane, click **Configuration Source Management**.
- 4 Click the **Devices** tab.
- 5 Using the drop-down list to the left side of the device list, select a filter.
- 6 Click **Go**.

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

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

Obtaining device configuration

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

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

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 3 In the **Risk Manager** pane, click **Configuration Source Management**.
- 4 Click the **Devices** tab.
- 5 To obtain the configuration for all devices, click **Backup All** in the navigation pane, and then click **Yes** to continue.
- 6 To obtain the configuration for one device, select the device. 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

Neighbor data is used in the topology to draw the connection lines to display the graphical topology map of your network devices. The discover button allows you to select single or multiple devices and update the neighbor data for a device. This information is used to update the connection lines for one or many devices in the topology.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 3 In the **Risk Manager** pane, click **Configuration Source Management**.
- 4 Click the **Devices** tab.
- 5 Select the device for which you want to obtain data. To select multiple devices, hold down the CTRL key and select all necessary devices.
- 6 Click **Discover**.
- 7 Click **Yes** to continue.

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

Select **Run in Background** to work on other tasks.

Manage backup jobs

Using the **Jobs** tab from Configuration Source Management, you can create backup jobs for all devices, or individual groups of devices in Configuration Source Management.

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

View backup jobs

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 3 In the **Risk Manager** pane, click **Configuration Source Management**.
- 4 Click the **Jobs** tab.
- 5 Double-click any job you want to view in greater detail.

Viewing backup job status and logs

To view backup job status and progress, use the **Configuration Monitor** page. To view the backup job log file, use the **Backup Log Viewer**.

Go to **Risks > Configuration Monitor**. The following columns in the **Device List** table provide information on backup job status:

Column	Description
Backup Status	<p>Indicates the completion status of the backup job:</p> <p>COLLECTED. The backup job is waiting to be processed.</p> <p>RUNNING. The backup job is in progress.</p> <p>SUCCESS. The backup job completed successfully.</p> <p>FAILURE. The backup job did not complete.</p>
Progress	<p>Displays a progress bar that tracks the completion rate of the backup job.</p> <p>To update the progress bar, click the Refresh icon on the Configuration Monitor page.</p>
Backup Log	<p>To open the Backup Log Viewer window for the backup job, click the See Log link in this column.</p> <p>To update the progress bar, click Refresh on the Backup Log Viewer window.</p>

Adding a backup job

After you define the search criteria, you define the job schedule. The schedule configuration displays in the Triggers column. The triggers for a job represent the job schedule. You can have multiple schedules

that are configured. For example, you can configure two schedule options so a job runs every Monday and the first of every month.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 3 In the **Risk Manager** pane, click **Configuration Source Management**.
- 4 Click the **Jobs** tab.
- 5 Select **New Job > Backup**.
- 6 Configure values for the following parameters:

Option	Description
Job Name	Type the name you want to apply to this job.
Group	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.
Comment	Type any comment you want to associate with this backup job. You can type up to 255 characters in your description of the backup job.

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

Option	Description
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. This ensures that any new devices are included in the job.

- 9 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. For more information, see [Search criteria for a static list or search](#).
 - c Click **Go**.
 - d In the **Devices** tab, select the devices that you want to include in the job.
 - e In the Job Details pane, click **Add selected from device view search**.
- 10 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. For more information, see the [Search criteria for a static list or search](#).
 - c Click **Go**.
 - d 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.
- 11 Click **Schedule**, and configure values for the following parameters:

Option	Description
Name	Type a name for the schedule configuration.
Start time	Select a time and date you want to start the backup process. The time must be specified in military time.

Option	Description
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.

- 12 Click **Save** in the Trigger pane.
- 13 Repeat steps 11 and 12 to create multiple schedules.
- 14 If you want to run the job immediately, click **Run Now**.
- 15 Click **Yes** to continue.

Editing a backup job

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 3 In the **Risk Manager** pane, click **Configuration Source Management**.
- 4 Click the **Jobs** tab.
- 5 Double-click the job that you want to edit.
- 6 Choose one of the following search options from the **Selection Type** parameter:

Option	Description
Static list	A static list enables you 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 happens after the job is run. This ensures that any new devices are included in the job.

- 7 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.
 - c Click **Go**.
 - d From the **Devices** tab, select the devices that you want to include in the job.
 - e On the **Job Details** pane, click **Add selected from device view search**.
- 8 If you chose Search, define the criteria:
 - a Click the **Devices** tab.
 - b Using the list in the **Devices** tab, select the search criteria.
 - c Click **Go**.
 - d On the Job Details pane, click **Use search from devices view**. This search criteria is used to determine devices that are associated with this job.
- 9 Click **Schedule**, and configure values for the following parameters:

Option	Description
Name	Type a name for the schedule configuration.
Start time	Select a time and date you want to start the backup process. The time must be specified in military time.

Option	Description
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.

- 10 Click **Save**.
- 11 Click **Run Now**.
- 12 Repeat steps 9 and 10, as required.
- 13 Click **Yes** to continue.

Rename a backup job

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 3 In the **Risk Manager** pane, click **Configuration Source Management**.
- 4 Click the **Jobs** tab.
- 5 Select the backup job you want to rename.
- 6 Click **Rename**.
- 7 Configure values for the following parameters:

Option	Description
Job Name	Type the name you want to apply to this job.
Group	From the Group list, select the group to which you want to assign this job. You can also specify a new group name.
Comment	Optional. Type any comment you want to associate with this backup job. You can type up to 255 characters in your description of the backup job.

- 8 Click **OK**.

Deleting a backup job

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 3 In the **Risk Manager** pane, click **Configuration Source Management**.
- 4 Click the **Jobs** tab.
- 5 Select the backup job that you want to delete.
- 6 Click **Delete**.

Configure protocols

Risk Manager provides default protocol configuration for your system. If you need to define protocols, you can define protocols to allow 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 [ExtremeSecurity Risk Manager Adapter Configuration Guide](#).

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

Protocol sets 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

You can configure the following values for the protocol parameters.

Table 7: Protocol parameters

Protocol	Parameter
SSH	Configure the following parameters: Port - Type the port on which you want the SSH protocol to use when communicating with and backing up network devices. The default SSH protocol port is 22. Version - Select the version of SSH that you want this network group to use when communicating with network devices. The available options are as follows: Auto - This option automatically detects the SSH version to use when communicating with network devices. 1 - Use SSH-1 when communicating with network devices. 2 - Use SSH-2 when communicating with network devices.
Telnet	Type the port number you want the Telnet protocol to use when communicating with and backing up network devices. The default Telnet protocol port is 23.
HTTPS	Type the port number you want the HTTPS protocol to use when communicating with and backing up network devices. The default HTTPS protocol port is 443.
HTTP	Type the port number you want the HTTP protocol to use when communicating with and backing up network devices. The default HTTP protocol port is 80.
SCP	Type the port number you want the SCP protocol to use when communicating with and backing up network devices. The default SCP protocol port is 22.
SFTP	Type the port number you want the SFTP protocol to use when communicating with and backing up network devices. The default SFTP protocol port is 22.
FTP	Type the port number you want the FTP protocol to use when communicating with and backing up network devices. The default SFTP protocol port is 22.

Table 7: Protocol parameters (continued)

Protocol	Parameter
TFTP	The TFTP protocol does not have any configurable options.
SNMP	<p>Configure the following parameters:</p> <p>Port - Type the port number you want the SNMP protocol to use when communicate with and backing up network devices.</p> <p>Timeout(ms) - Select the amount of time, in milliseconds, that you want to use to determine a communication timeout.</p> <p>Retries - Select the number of times you want to attempt to retry communications to a device.</p> <p>Version - Select the version of SNMP you want to use for communications. The options are v1, v2, or v3.</p> <p>V3 Authentication - Select the algorithm you want to use to authenticate SNMP traps.</p> <p>V3 Encryption - Select the protocol you want to use to decrypt SNMP traps.</p>

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 3 In the **Risk Manager** pane, click **Configuration Source Management**.
- 4 On the navigation menu, click **Protocols**.
- 5 Configure a new network group:
 - a In the **Network Groups** pane, click the **Add (+)** icon.
 - b Type a name for a network group.
 - c Click **OK**.
 - d Use the **Move Up** and **Move Down** icons to prioritize the network groups. Move the network group you want to have first priority to the top of the list.
- 6 Configure the address set:
 - a In the **Add Address** field, type the IP address or CIDR range that you want to apply to the network group, then click the **Add (+)** icon. For example, type an IP address range using a dash or wildcard (*) to indicate a range, such as 10.100.20.0-10.100.20.240 or 1.1.1*. If you type 1.1.1.* , all IP addresses meeting that requirement are included.
 - b Repeat for all IP addresses you want to add to the address set for this network group.
- 7 Configure the protocol set:
 - a In the **Network Groups** pane, ensure the network group you want to configure protocols for is selected.
 - b Select check boxes to apply a protocol to the range of IP addresses assigned to the network group you created. Clearing the check box turns off the communication option for the protocol when attempting to back up a network device.
 - c For each protocol that you selected, configure values for the parameters.
 - d Use the **Move Up** and **Move Down** icons to prioritize the protocols. Move the protocol that you want to have first priority to the top of the list.
- 8 Click **OK**.

Configuring the discovery schedule

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 3 In the **Risk Manager** pane, click **Configuration Source Management**.

- 4 On the navigation menu, click **Schedule Discovery**.
- 5 Select the **Enable periodic discovery** check box to enable schedule discovery.
- 6 Configure values for the following parameters:

Option	Description
Name	Type a name for the schedule configuration.
Start time	Select a time and date you want to start the backup process. The time must be specified in military time.
Frequency	Select the frequency you want to associate with this schedule.
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	Select the check box if you want the discovery process to discover new devices. Clear the check box if you do not want to add new devices to the inventory.

- 7 Click **OK**.

6 Connections

Viewing connections

Use graphs to view connection data

Search for connections

Exporting connections

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, the connection is not remote to remote.
- The destination is local, which means that it is inside your network hierarchy, and 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. Do 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.

Viewing connections

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.



Note

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 time frame 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**.

The **Connections** window displays the following information:

Table 8: Connections window - default

Parameter	Description
Current Filters	This parameter displays only after you apply a filter. Details of the filter that is applied to the search result are displayed on top. To clear these filter values, click Clear Filter .
View	From the list, select the time range that you want to filter. Use the Expand option to adjust the time range.
Current Statistics	Current statistics include the following parameters: Total Results - The total number of results that matched your search criteria. Data Files Searched - The total number of data files searched during the specified time span. Compressed Data Files Searched - The total number of compressed data files searched within the specified time span. Index File Count - The total number of index files searched during the specified time span. Duration - The duration of search. Current Statistics are helpful for troubleshooting. When you contact Customer Support to troubleshoot an issue, you might be asked to provide current statistical information. Click the arrow next to Current Statistics to display or hide the statistics
Charts	Displays charts that represent the records that are matched by the time interval and/or grouping option. Click (Hide Charts) if you want to remove the graph from your display. Note: Remove Firefox <i>Adblock Plus</i> if it prevents charts from displaying in Firefox.
Last Packet Time	The date and time of the last processed packet for this connection.
Source Type	The Source Type for this connection, which can be: <i>Host</i> or <i>Remote</i> .
Source	The following are options for the Source : IP address - The IP address for the source of this connection. If the Source Type is Host , the IP address is displayed. Country - The source country (with the country flag) for this connection. The country flag is only displayed if the Source Type is remote.
Destination Type	The options for Destination Type are: <i>Host</i> or <i>Remote</i> .
Destination	The options for Destination are: <i>IP address</i> - If the Destination Type is host, the IP address is displayed. <i>Country</i> - The destination country (with the country flag) for this connection. The country flag is only displayed if the Destination Type is remote.

Table 8: Connections window - default (continued)

Parameter	Description
Protocol	The protocol that is used for this connection.
Destination Port	The destination port for this connection.
Flow Application	The flow application that generated the connection.
Flow Source	The source of flows that are associated with this connection. This parameter applies only to accepted connections.
Flow Count	The total number of flows that are associated with this connection.
Flow Source Bytes	The total number of flow source bytes associated with this connection.
Flow Destination Bytes	The total number of destination bytes associated with this connection.
Log Source	The source of events that contribute to this connection.
Event Count	The total number of events that are detected for the connection.
Connection Type	The options for connection type are: Allow or Deny .

Use graphs to view connection data

The **Records Matched Over Time** graph displays the number of connections based on time.

The **Connection Graph** provides a visual representation of the connection retrieved.

Graph options available for grouped connections are table, bar, and pie.

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.

Using the time series graph

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 selected in the Advanced View Definitions box, the Time Series chart is not available. You must clear the search criteria before continuing. Time series charts are useful for short-term and long-term trending of data. Using time series charts, you can access, navigate, and investigate connections from various views and perspectives.

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

Table 9: Time series chart functions

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

Procedure

- 1 Click the Risks tab.
- 2 On the navigation menu, click **Connections**.
- 3 In the charts pane, click the **Configure** icon.
- 4 Using the **Chart Type** drop-down list, select Time Series.
- 5 Using the interactive time series charts, you can navigate through a time line to investigate connections.
- 6 To refresh the information in the graph, click Update Details.

Use connection graph to view network connections

The graph that is displayed in the Connections window is not interactive. If you click the graph, the Radial Data Viewer window is displayed. The Radial Data Viewer window allows you to manipulate the graph, as required.

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

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

The Radial Data Viewer includes several menu options, including:

Table 10: Radial Data Viewer menu options

Menu Option	Description
Connection Type	By default, the radial graph displays accepted connections. If you want to view denied connections, select Deny from the Connection Type drop-down list.
Undo	Collapses the last node expansion. If you want to undo multiple expansions, click the Undo button for each expansion.
Download	Click Download to save the current topology as a JPEG image file or a Visio drawing file (VDX). To download and save the current topology as a Visio drawing file (VDX), the minimum software version you require is Microsoft™ Visio Standard 2010.

The following table provides additional functions to view connections including:

Table 11: Radial Data Viewer functions

If you want to	Then
Zoom in or zoom out	Use the slider on the top-right side of the graph to change the scale.
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	Point your mouse over the connection line to view additional details. If the connection is between a network node to a remote network or remote country, right-click to display the following 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 involved in the connection. A thicker line indicates a greater amount of data. This information is based on the amount of bytes involved in the communication
Highlight a connection path	Point 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	Pointer your mouse over the node. If the node is allowed, the path to the node and the node highlight in green. If the node is denied, the path to the node and the node highlights in red.
Change graph view	Using the preview thumbnail, move the thumbnail to the portion of the graph you want to display.

Using pie, bar, and table charts

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

- 1 Click the **Risks** tab.

- On the navigation menu, click **Connections**.

**Note**

The default saved search results display.

- Perform a search.
- In the charts pane, click the **Configuration** icon.
- Configure the parameters:

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

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

Search for connections

- Click the **Risks** tab.
- On the navigation menu, click **Connections**.
If applicable, the default saved search results display.
- Using the **Search** list, select **New Search**.
- If you want to load a previously saved search, use one of the following options:
 - From the **Group** list, select the group to which the saved search is associated.
 - From the **Available Saved Searches** list, select the saved search you want to load.
 - In the **Type Saved Search or Select from List** field, type the name of the search you want to load. From the Available Saved Searches list, select the saved search you want to load.
 - Click **Load**.
 - In the **Edit Search** pane, select the options you want for this search.

Option	Description
Include in my Quick Searches	Include this search in your Quick Search items.
Include in my Dashboard	Include the data from your saved search in your dashboard. This parameter is only available if the search is grouped.
Set as Default	Set this search as your default search.
Share with Everyone	Share these search requirements with all other Extreme Networks Security Risk Manager users.

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

Option	Description
Recent	Using the list, specify the time range you want to filter.
Specific Interval	Using the calendar, specify the date and time range you want to filter.

- 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:
- Using the first list, select an attribute on which you want to search. For example, Connection Type, Source Network, or Direction.
 - Using the second list, select the modifier you want to use for the search. The list of modifiers that display depends on the attribute selected in the first list.
 - In the text field, type specific information related to your search.
 - Click **Add Filter**.
 - Repeat steps a through d for each filter you want to add to the search criteria.
 - If you are finished configuring the search and want to view the results, click **Search**. Otherwise, proceed to the next step.
- 8 If you want to automatically save the search results when the search is completed, select the Save results when search is complete check box and specify a name.
- 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:
- Using the **Display** list, select the view you want to associate with this search.
 - Click the arrow next to **Advanced View Definition** to display advanced search parameters. Click the arrow again to hide the parameters.
- 11 Click **Search**.

Saving search criteria

You can customize the columns that display in the search results. These options are available in the Column Definition section and are called Advanced View Definition options.

Table 12: Advanced View Definition options

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

Table 12: Advanced View Definition options (continued)

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

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

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

- 6 Click **OK**.

Performing a sub-search

A sub-search allows you to search within a set of completed search results. You can refine your search results without searching the database again. 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.

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

- 4 To add a filter, perform 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 you want to use for the search. The list of modifiers that display depends on the attribute selected in the first list.
 - d In the text field, type specific information related to your search.
 - e Click **Add Filter**.



Note

If the search remains in progress, partial results are displayed. The Original Filter pane indicates the filter from which the original search was based. The Current Filter pane indicates the filter applied to the sub-search.



Tip

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 no longer bases the search on a previously searched dataset.

Manage search results

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

The search results toolbar provides the following options:

Parameter	Description
New Search	Click New Search to create a new search. When you click this button, the search window is displayed.
Save Results	Click Save Results to save search results. This option is only enabled when you have selected a row in the Manage Search Results list.
Cancel	Click Cancel to cancel searches that are in progress or are queued to start.
Delete	Click Delete to delete a search result.
Notify	Select the search(es) for which you want to receive notification, and then click Notify to enable email notification when the search is complete.
View	From the drop-down list, specify which search results you want to list in the search results window. The options are: Saved Search Results All Search Results Canceled/Erroneous Searches Searches in Progress

- 1 Click the **Risks** tab.
- 2 On the navigation menu, click **Connections**.
- 3 From the menu, select **Search > Manage Search Results**.

Saving Search Results

- 1 Click the **Risks** tab.
- 2 On the navigation menu, click **Connections**.
- 3 Perform a **connection search** or **sub-search**.
- 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**.

Canceling a search

If a search is in progress when canceled, the accumulated results, up until the cancellation of the search, are maintained.

- 1 From the **Manage Search Results** window, select the queued or in progress search result you want to cancel. You can select multiple searches to cancel.
- 2 Click **Cancel Search**.
- 3 Click **Yes**.

Deleting a search

- 1 From the **Manage Search Results** window, select the search result you want to delete.
- 2 Click **Delete**.
- 3 Click **Yes**.

Exporting connections

- 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**.

7 Configuration monitor

Searching device rules

Comparing the configuration of your network devices

Log source mapping

- 1 Click the **Risks** tab.
- 2 In the navigation pane, click **Configuration Monitor**.
- 3 To search your network devices, enter an IP address or Host Name in the **Input IP Address or Host 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 ExtremeSecurity log source mapping is not configured.
- 5 To search the rules, on the **Rules** toolbar, click **Search > New Search**.

If an icon is displayed in the **Status** column, you can hover your mouse over the status icon to display more information.
- 6 To investigate the device interfaces, on the toolbar, click **Interfaces**.
- 7 To investigate access control list (ACL) device rules, on the toolbar, click **ACLs**.

Each access control list defines the interfaces over which the devices on your network are communicating. 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, on the toolbar, 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

In Extreme Networks Security 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:
 - To search for **Shadowed, Deleted** or **Other** rules, click a status option.

By default all status options are enabled. To search for shadow rules only, clear the **Deleted** and **Other** options.
 - To search for an access control list (ACL), type in the **List** field.
 - To search on the order number of the rule entry, type a numeric value in the **Entry** field.
 - To search for a source or destination, type an IP address, CIDR address, host name, or object group reference.
 - To search for ports or object group references, type in the **Service** field.

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, !(100-200) or !80(TCP).
 - To search for vulnerability rule information as defined by the IPS device, type in the **Signature** field.
 - To search for applications by adapter, click **Select Applications**, then type an adapter or application name.
- 7 Click **Search**.

Comparing the configuration of your network devices

In Extreme Networks Security 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. You can view a configuration file by double-clicking it.

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 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 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**.

Log source mapping

To monitor the trigger frequency of firewall rules and enable topology event searches, Extreme Networks Security Risk Manager identifies ExtremeSecurity 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 Risk Manager, but devices can have multiple log sources.

Log source mapping display options

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

- **Auto-Mapped** - If 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 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 *ExtremeSecurity Log Sources User Guide*.

Creating or editing 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**.

8 Filtering 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 you in formulating 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.

From the **User(s)/Group(s)** column in the rules table, you can view your users and groups.

Group results are displayed with hyperlinks, which you can click, 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.

9 Network topology graph

Topology graph searches

Adding an intrusion prevention system (IPS)

Topology device groups

Use case: Visualize the attack path of an offense

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.

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 graph searches

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.

You can search events by right-clicking devices and subnets, or search flows by right-clicking subnets.

Click **Actions** to access the **Search** menu. Enter your search criteria in the **Search Criteria** pane. The following are some of the search options that you can use:

Searching 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, then that subnet and all connected devices are displayed.

Searching 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`.

Searching Paths

A path search displays the traffic direction, fully or partially allowed protocols, and device rules. A path summary is displayed if you select any path search criteria other than the mandatory source and destination IP addresses.

Refine your path search by searching for applications, vulnerabilities, and users/groups.

NAT indicators in search results

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 13: Information available from the NAT indicator

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

Adding an intrusion prevention system (IPS)

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 to device	Select an interface to connect to the device. If there are multiple choices devices, then you need to select a device (see next option).
Connect IPS interface	Select the device that you want to connect to the IPS. This option is available if there are 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.
- 7 Click **OK**.

If you want to add an IPS to a device that is in a group, expand the group to add the IPS.

Removing an Intrusion Prevention System (IPS)

- 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 the Remove IPS idp option.
- 5 Click **OK**.

Topology device groups

Select a device in the **Current Topology** window and click the **Actions** menu on the toolbar, or use the right-click menu to access the device **Groups** feature.

Use case: Visualize the attack path of an offense

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 the offense does not have an alternate path in your network to a critical asset.

The key features for visualization are:

- Leverages the existing rule and offense system from Extreme SIEM.
- Displays a visual path for all devices between the source and destination of the offense.

- Quick access to the device configurations and rules that allow the offense.

Viewing the attack path of an offense

- 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**.

10 Policy Monitor

Policy Monitor questions
Policy Monitor question parameters
Creating an asset question
Creating a question that tests for rule violations
Submitting a question
Evaluation of results from policy monitor questions
Policy question monitoring
Group questions
Export and import policy monitor questions
Integration with Vulnerability Manager
Monitoring firewall rule event counts of Check Point devices
Policy Monitor use cases
CIS benchmark scans

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 or devices/rules to flag risks in their networks. The risk level for an asset or a device/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

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

- For questions based on assets, then 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/rules, then 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, then the search identifies if an asset is compliant with a CIS benchmark.

Note



If you configured Extreme Networks Security Analytics for multiple domains, asset questions only monitor assets in your default domain. Asset compliance questions monitor assets in your default domain unless you configured another domain in the **Admin > Domain Management** window. For more information about domain management, see the *Extreme SIEM Administration Guide*.

Devices/rules questions look for violations in rules and policy and do not have restrictive test components. You can also ask devices/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 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 Monitor question parameters

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 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.

Asset test questions

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 have been detected using connections. Possible communication questions allow you to review if specific communications are possible on assets, regardless of whether or not a communication has been 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 should 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, such as 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.

Devices/Rules test questions

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](#).

Contributing questions for actual communication tests

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 14: 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. This test allows you to define a start or end point to your question. For example, to identify the assets that have accepted communication from the DMZ, configure the test as follows: have accepted communication from any source 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. This test allows you to define a start or end point to your question. For example, to identify the assets that communicated to the DMZ, configure the test as follows: have accepted communication from source <networks> You can use this test to detect out-of-policy communications.
have accepted communication to destination IP addresses	Detects assets that have communications to or from the IP address that you specify. This test allows you to specify IP or CIDR address. For example, if you want to identify all assets that communicated to a specific compliance server, configure the test as follows: have accepted communications to destination <compliance server IP address>
have accepted communication to destination asset building blocks	Detects assets that have communications to or from the asset building blocks that you specify. This test allows you to re-use building blocks defined in the ExtremeSecurity Rules Wizard in your query. For more information about rules, assets, and building blocks, see the <i>Extreme SIEM Administration Guide</i> .
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 information about creating and saving an asset search, see the <i>Extreme SIEM User Guide</i>
have accepted communication to destination reference sets	Detects assets that have communicated to or from the defined reference sets.
have accepted communication to destination remote network locations	Detects assets that have communicated with networks defined as a remote network. For example, this test can identify hosts that have communicated to botnets or other suspicious Internet address space.
have accepted communication to destination geographic network locations	Detects assets that have communicated with networks defined as geographic networks. For example, this test can detect assets that have attempted communications with countries in which you do not have business operations.

Table 14: Contributing question parameters for actual communication tests (continued)

Test Name	Description
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.
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 3 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 entry. Configure the text entries parameter to identify the asset name, vendor, version or service you want this test to consider.
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions	Detects assets in your network with a vulnerability that matches the asset name, vendor, version or service based one or more regular expression. Configure the regular expressions parameter to identify the asset name, vendor, version or service you want this test to consider.
are susceptible to vulnerabilities contained in vulnerability saved searches	Detects risks that are associated with saved searches that are created in Extreme Networks Security Vulnerability Manager.

Deprecated contributing test questions

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 have been replaced by other tests.

Restrictive questions for actual communication tests

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 will return only assets that do not use the excluded protocols.

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

Table 15: 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 only include flow data.
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 trying to determine what assets between two points have an inbound and outbound percentage difference greater than 40%. For example, Contributing test - have accepted communication to the internet. Contributing test - and have accepted communication from the internet. Restrictive test - and include only if the inbound and outbound flow count has a percentage difference greater than 40.

Table 15: Restrictive question parameters for actual communication tests (continued)

Test Name	Description
include only if the time is between start time and end time inclusive	Filters communications within your network that occurred within a specific time range. This allows you to detect out-of-policy communications. For example, if your corporate policy allows FTP communications between 1 and 3 am, this tests can detect any attempts to use FTP to communicate outside of that time range.
include only if the day of week is between start day and end day inclusive	Filters assets from the contributing test question based on network communications that occurred within a specific time range. This allows you to detect out-of-policy communications.
include only if susceptible to vulnerabilities that are exploitable.	Filters assets from a contributing test question searching for specific vulnerabilities and restricts results to exploitable assets. This restrictive test does not contain configurable parameters, but is used in conjunction with the contributing test, are susceptible to one of the following vulnerabilities . This contributing rule containing a vulnerabilities parameter is required.
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 if a Microsoft™ Windows™ service pack level for an operating system is below the level your company policy specifies.
include only if the Microsoft™ Windows™ security setting is less than 0	Filters assets to determine if a Microsoft™ Windows™ security setting is below the level your company policy specifies.
include only if the Microsoft™ Windows™ service equals status	Filters assets to determine if 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 if a Microsoft™ Windows™ Setting is the specified regular expression.

Contributing questions for possible communication tests

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

Table 16: 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 if a critical server can possibly receive communications from any source, configure the test as follows: have accepted communication from any source. You can then apply a restrictive test to return if that critical server has received any communications on port 21. This allows you to detect out-of-policy communications for that critical server.
have accepted communication to destination networks	Detects assets that have possible communications to or from the configured network. This test allows you to define a start or end point to your question. For example, to identify the assets that have the possibility of communicating to the DMZ, configure the test as follows: have accepted communication from source <networks> You can use this test to detect out-of-policy communications.
have accepted communication to destination IP addresses	Detects assets that have possible communications to or from the configured IP address. This test allows you to specify a single IP address as a focus for possible communications. For example, if you want to identify all assets that can communicate to a specific compliance server, configure the test as follows: have accepted communications to destination <compliance server IP address>
have accepted communication to destination asset building blocks	Detects assets that have possible communications to or from the configured asset using building blocks. This test allows you to re-use building blocks defined in the ExtremeSecurity 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 <i>Extreme SIEM Administration Guide</i> .
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 information about creating and saving an asset search, see the <i>Extreme SIEM User Guide</i>
have accepted communication to destination reference sets	Detects if source or destination communication are possible to or from reference sets.
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 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 classification. This test filters all assets that have possible vulnerabilities with a Common Vulnerability Scoring System (CVSS) score, as specified. Configure the classifications parameter to identify the vulnerability classifications that you want this test to apply.

Table 16: Possible communication question parameters for contributing 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 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.
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following text entries	Detects assets in your network with a vulnerability that matches the asset name, vendor, version or service based one or more text entry. Configure the text entries parameter to identify the asset name, vendor, version or service you want this test to consider.
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions	Detects assets in your network with a vulnerability that matches the asset name, vendor, version or service based one or more regular expression. Configure the regular expressions parameter to identify the asset name, vendor, version or service you want this test to consider.
are susceptible to vulnerabilities contained in vulnerability saved searches	Detects risks that are associated with saved searches that are created in Extreme Networks Security Vulnerability Manager.

Deprecated contributing test questions

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 have been replaced by other tests.

Restrictive question parameters for possible communication tests

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

Table 17: Restrictive tests for possible communication tests

Test Name	Description
include only the following protocols	Filters assets that have or have not possibly communicated with the configured protocols, in conjunction with the other tests added to this question.
include only the following inbound ports	Filters assets that have or have not possibly communicated with the configured ports, in conjunction with the other tests added to this question.
include only ports other than the following inbound ports	Filters assets from a contributing test question that have or have not possibly communicated with ports other than the configured ports, in conjunction with the other tests added to this question.
include only if susceptible to vulnerabilities that are exploitable.	Filters assets from a contributing test question searching for possible specific vulnerabilities and restricts results to exploitable assets. This restrictive test does not contain configurable parameters, but is used in conjunction with the contributing test, are susceptible to one of the following vulnerabilities . This contributing rule containing a vulnerabilities parameter is required.
include only the following networks	Filters assets from a contributing test question that include only or exclude the configured networks.
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 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 if a Microsoft™ Windows™ service pack level for an operating system is below the level your company policy specifies.
include only if the Microsoft™ Windows™ security setting is less than 0	Filters assets to determine if a Microsoft™ Windows™ security setting is below the level your company policy specifies.
include only if the Microsoft™ Windows™ service equals status	Filters assets to determine if 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 if a Microsoft™ Windows™ Setting is the specified regular expression.

Device/rules test questions

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

Table 18: Device/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.
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.

Importance factor

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

Table 19: Importance factor results matrix

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

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

Creating an asset question

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 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 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 beside 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**.

Investigating external communications that use untrusted protocols

From a risk perspective, it is important to continuously monitor traffic in the DMZ to ensure that only trusted protocols are present. Use Extreme Networks Security 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 the **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.
- 17 Click **Submit Question**.
- 18 Review the results to see whether any protocols other than port 80 and port 443 are communicating on the network.
- 19 Monitor your DMZ question by putting the question into monitoring mode when the results are tuned.

Finding assets that allow communication 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

Extreme Networks Security 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

Extreme Networks Security 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 objective, you can 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 Risk Manager can generate an alert.

View question information

If you want to view more information about any question, select the question to view the description.

If a question is in monitor mode when you select it, then you can view any events and offenses that are generated from the selected question.

Creating a question that tests for rule violations

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, click the + icon beside 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 devices/rules that allow communication to the Internet

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. Extreme Networks Security 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, click the plus icon beside the test, **allow connections to the internet** to add 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.

Submitting a question

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

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 there is 3 hours of data. 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.



Note

When you edit a question after it is submitted, and the edit affects associated tests, then 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

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

The parameters for asset results are described in the following table.

Table 20: Asset results

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 Extreme SIEM User Guide
Vlan	The name of the VLAN associated with the asset.
Weight	The weight of the asset, as obtained from the asset profile.
Destination Port(s)	The list of destination ports associated with this asset, in context of the question tests. If there are multiple ports associated with this asset and question, this field indicates Multiple and the number of multiple ports. The list of ports is obtained by filtering the connections associated with this question to obtain all unique ports where the asset has either been the source, destination, or the connection. Click Multiple (N) to view the connections. This display provides the aggregated connections by port, filtered by the asset IP address, and based on the time interval specified in the question.
Protocol(s)	The list of protocols associated with this asset, in context of the question tests. If there are multiple protocols associated with this asset and question, this field indicates Multiple and the number of protocols. The list of protocols is obtained by filtering the connections associated with this question to obtain all unique protocols where the asset has either been the source, destination, or the connection. Click Multiple (N) to view the Connections. This display provides the aggregated connections by protocol, filtered by the asset IP address, and based on the time interval specified in the question.

Table 20: Asset results (continued)

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

Device/Rule question results

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 assigned to the question, and the number of results returned for the question.

The parameters for devices and rules results are described in the following table.

Table 21: Devices and rules results

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 Extreme SIEM User Guide .
List	The name of the rule from the device.
Entry	The entry number of the rule.
Action	The action associated with the relevant rule from the device. The options are: permit, deny, or NA.
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 the object group reference(s).
Source Service(s)	The source ports and the comparison associated with the relevant rule from the device in the following format: <code><comparison>:<port></code> Where <code><comparison></code> could include one of the following options: eq - Equal ne - Not equal lt - Less than gt - Greater than For example, if the parameter indicates ne:80, any port other than 80 applies to this source service. If the parameter indicates lt:80, the range of applicable ports is 0 to 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 the object group reference(s).
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 the object group reference(s).

Table 21: Devices and rules results (continued)

Parameter	Description
Destination Service(s)	<p>The destination ports and the comparison associated with the relevant rule from the device is displayed in the following format:</p> <p style="text-align: center;"><code><comparison> : <port></code></p> <p>Where</p> <p style="text-align: center;"><code><comparison></code></p> <p>might include one of the following options: eq - Equal ne - Not equal lt - Less than gt - Greater than</p> <p>For example, if the parameter indicates ne:80, any port other than 80 applies to this destination service. If the parameter indicates lt:80, the range of applicable ports is 0 to 79. This parameter displays the destination port for the device rule. If no port exists for this device rule, the term NA is displayed.</p> <p>Destination services with a hyperlink indicate an object group reference. Click the link to view detailed information about the object group reference(s).</p>
User(s)Group(s)	The users or groups associated with the relevant rule from the device.
Protocol(s)	The protocol or group of protocols associated with the relevant rule from the device.
Signature(s)	The signature for this device, which is only displayed for a device rule on an IP device.
Applications	The applications that are associated with the relevant rule from the device.

Evaluation of results from policy monitor questions

Approving a result of a question is similar to tuning your system to inform Extreme Networks Security Risk Manager that the asset that is associated with the question result is safe or can be ignored in the future.

When a user approves an asset result, the policy monitor sees that asset result as approved, and when the policy monitor question is submitted or monitored in the future, the asset is not listed in the question results. The approved asset does not 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/Rule, and the date and time.

Approving results

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

- Choose one of the following options:

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

- Type the reason for approval.
- Click **OK**.
- Click **OK**.
- To view the approved results for the question, click **View Approved**.

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

Table 22: 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 check box for each result for which you want to remove approval and click **Revoke Selected**. To remove all approvals, click **Revoke All**.

Policy question monitoring

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

Question monitoring provides the following key features:

- Monitor for rule or asset changes hourly for unapproved results.
- 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 Extreme SIEM.

Monitoring a policy monitor question and generating events

- Click the **Risks** tab.
- On the navigation menu, click **Policy Monitor**.
- Select the question that you want to monitor.
- Click **Monitor**.

- 5 Configure values for the parameters.
- 6 Click **Save Monitor**.

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

Table 23: 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.
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 Extreme Networks Security 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: <pre>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</pre>
Enable Monitor	Monitor the question.

Group questions

Use groups to efficiently view and track your questions. For example, you can view all questions related to compliance. Do the following tasks with groups:

- Create a group for questions.
- Assign a question to a group.
- Edit or delete questions in a group.
- Copy a question to one or many groups.

Export and import policy monitor questions

Exporting and importing questions provides a method to back up questions and share questions with other Extreme Networks Security 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 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

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

The import process does not update existing questions. Each question that is imported becomes a new question in policy monitor. A time stamp 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.

- 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.

Monitoring is not enabled on imported questions. You can [create an event](#) to monitor results of questions that were imported.

Integration with Vulnerability Manager

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

Risk policies and vulnerability prioritization

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

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

When the vulnerability risk scores are adjusted in 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 ExtremeSecurity 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 Risk Manager, then all the vulnerabilities on that asset have their risk scores adjusted.

Monitoring firewall rule event counts of Check Point devices

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

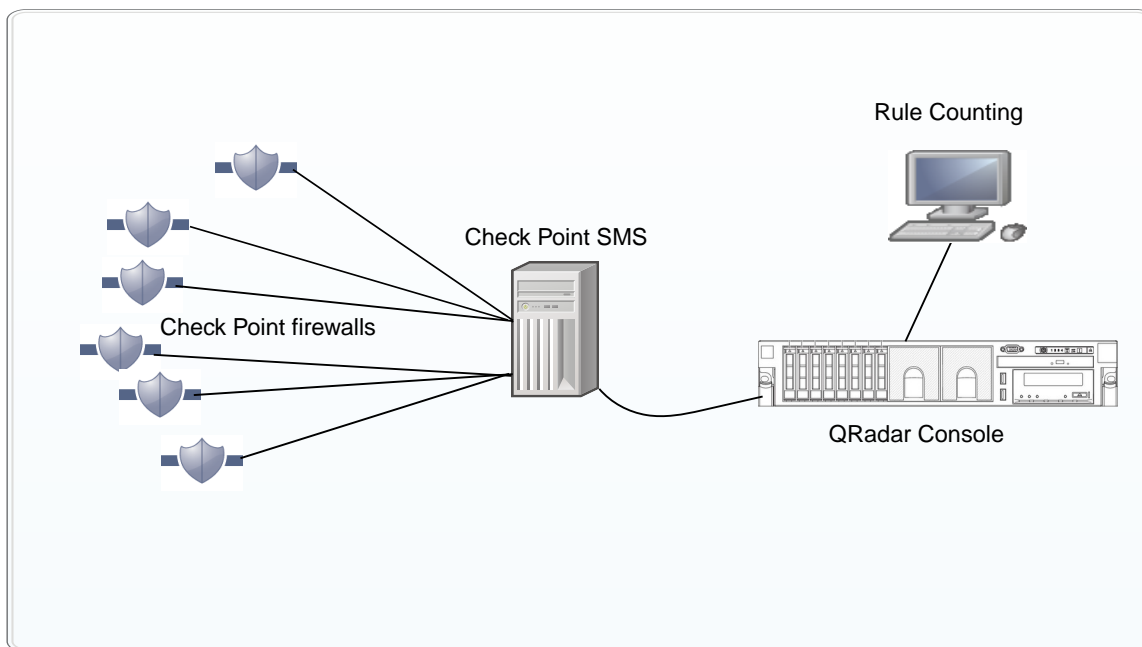


Figure 1: Check Point rule counting

Scenario - Implementing Check Point firewall rule monitoring in ExtremeSecurity

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 ExtremeSecurity, so that ExtremeSecurity receives rule event logs from Check Point firewall devices. ExtremeSecurity processes this rule event log information and displays rule event information for all devices that are managed by Check Point firewalls. From the ExtremeSecurity 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.

Before you begin, download the most recent adapter bundle from FixCentral, and install it on your ExtremeSecurity managed host.

Complete the following steps to set up rule counting:

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

Configuring OPSEC applications in the SmartDashboard

Create 2 OPSEC (Open Platform for Security) applications, one with a client entity property of CPMI (Check Point Management Interface) for Risk Manager, and the other with a client entity property of LEA (Log Export API) for the 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** check box.
This option is required for 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 ExtremeSecurity can use a security certificate from Check Point.
- 8 Click *Initialize*.
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 ExtremeSecurity
- 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** check box.
 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**.

The next step is to [configure the log source](#) in ExtremeSecurity.

Configuring the log source

- 1 Log on to ExtremeSecurity.
- 2 Click the **Admin** tab.
- 3 On the navigation menu, click **Data Sources**.
The **Data Sources** pane is displayed.
- 4 Click the **Log Sources** icon.
- 5 Click **Add**.
- 6 Configure the following values:

Table 24: 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 check box.
Statistics Report Interval	Default of 600.
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 and select the OPSEC application that has the client entity property of LEA. Click Edit , and copy the entry from the DN field, and paste into the OPSEC Application Object SIC Attribute (SIC Name) field.

Table 24: Check Point log source parameters (continued)

Parameter	Description
Log Source SIC Attribute (Entity SIC Name)	<p>Use the entry that you pasted into the OPSEC Application Object SIC Attribute (SIC Name) field, remove the text from the CN= property value, and make the following edits:</p> <p>For the CN= property value, use <code>cp_mgmt_ <hostname></code> where <code><hostname></code> is the Host name from the OPSEC Application Properties window.</p> <p>See the following examples of an OPSEC Application DN and OPSEC Application Host, which is used to create the Entity SIC Name:</p> <p>OPSEC Application DN: <code>CN=cpsmsxxx , O=svxxx-CPSMS . . bsaobx</code> OPSEC Application Host: <code>Srvxxx-SMS</code></p> <p>Use text from the OPSEC Application DN and the OPSEC Application Host to form the Entity SIC Name:</p> <p><code>CN=cp_mgmt_Srvxxx-SMS , O=svxxx-CPSMS . . bsaobx</code></p> <p>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:</p> <p><code>CN=cp_mgmt , O=<take_O_value_from_DN_field></code></p>
Specify Certificate	Don't select this check box.
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.
OPSEC Application	The name that you specified in the Name field from the OPSEC Applications Properties .
Enabled	Select this check box to enable the log source. By default, the check box 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 ExtremeSecurity. 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 ExtremeSecurity. 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.

7 Click **Save**.

- 8 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 the **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 [ExtremeSecurity Managing Log Sources Guide](#).

Establishing secure communication between Check Point and Extreme Networks Security Analytics

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 ExtremeSecurity as an administrator.
- 2 Click the **Admin** tab.
- 3 On the navigation menu, click **Plug-ins** 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 user name and password.

To configure the OPSEC fields, use the information from the **OPSEC Application Properties** window of the SmartDashboard, where you selected the **CPMI** check box 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.

See the following examples of 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**:

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 25: 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** check box for the client entity.
- 17 Click **OK**
If successful, the **OPSEC SSL Certificate** field is populated and grayed out.

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

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

- 1 In ExtremeSecurity, 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.

Policy Monitor use cases

The following Policy Monitor examples outline common use cases that you can use in your network environment.

Prioritizing high risk vulnerabilities by applying risk policies

In Extreme Networks Security 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 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 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

The **Event Description** field is mandatory.

- 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.

CIS benchmark scans

In order to set up CIS benchmark scan, the following prerequisites are needed:

Valid Extreme Networks Security Vulnerability Manager and Extreme Networks Security Risk Manager licenses

If you patched from an earlier version of Extreme Networks Security Analytics, you must do an automatic update before you do a CIS benchmark scan.

There are 8 steps involved in setting up a CIS benchmark scan:

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

It is easiest to add centralized credentials on the Extreme Networks Security Analytics 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 Extreme Security Vulnerability Manager.

You can create a custom CIS benchmark checklist by using the Compliance Benchmark Editor.

- 5 Configuring a CIS benchmark scan profile in Extreme Security Vulnerability Manager.
- 6 Creating an asset compliance question in Extreme Networks Security Risk Manager.
- 7 Monitoring the asset compliance question that you created.
- 8 Viewing the CIS benchmark scan results.

Adding or editing an asset 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 QRadar® to identify key asset characteristics such as operating system, device type, and services.

When assets are discovered 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 only edit 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 required.

- 1 Click the **Assets** tab.
- 2 On the navigation menu, click **Asset Profiles**.
- 3 Choose one of the following options:
To add an asset, click **Add Asset** and type the IP address or CIDR range of the asset in the **New IP Address** field.

To edit an asset, double-click the asset that you want to view and click **Edit Asset**.

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

Click the **New MAC Address** icon and type a MAC Address in the dialog box.

Click the **New IP Address** icon and type an IP address in the dialog box.

If **Unknown NIC** is listed, you can select this item, click the **Edit** icon, and type a new MAC address in the dialog box.

Select a MAC or IP address from the list, click the **Edit** icon, and type a new MAC address in the dialog box.

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 . 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:
- From the **Vendor** list box, select an operating system vendor.
 - From the **Product** list box, select the operating system for the asset profile.
 - From the **Version** list box, select the version for the selected operating system.
 - Click the **Add** icon.
 - 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.
 - Select an operating system from the list.
 - 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	<p>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 to indicate potential for economic loss of productivity or revenue. Increased collateral damage potential increases the calculated value in the CVSS Score parameter.</p> <p>From the Collateral Damage Potential list box, select one of the following options:</p> <ul style="list-style-type: none"> None Low Low-medium Medium-high High Not defined <p>When you configure the Collateral Damage Potential parameter, the Weight parameter is automatically updated.</p>
Confidentiality Requirement	<p>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.</p> <p>From the Confidentiality Requirement list box, select one of the following options:</p> <ul style="list-style-type: none"> Low Medium High Not defined
Availability Requirement	<p>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 space impact the availability of an asset. Increased availability impact increases the calculated value in the CVSS Score parameter.</p> <p>From the Availability Requirement list box, select one of the following options:</p> <ul style="list-style-type: none"> Low Medium High Not defined
Integrity Requirement	<p>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.</p> <p>From the Integrity Requirement list box, select one of the following options:</p> <ul style="list-style-type: none"> Low Medium High Not defined
Weight	<p>From the Weight list box, select a weight for this asset profile. The range is 0 - 10.</p> <p>When you configure the Weight parameter, the Collateral Damage Potential parameter is automatically updated.</p>

- 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.

Parameter	Description
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 IBM® Security QRadar® Vulnerability Manager. For more information about automatic remediation, see the <i>IBM® Security QRadar® Vulnerability Manager User Guide</i> .

- 9 Click **Save**.

Configuring a credential set

- 1 Click the **Admin** tab.
- 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

- 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.

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

- 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** check box 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, please refer to the CIS documentation.

Create an asset compliance question to test assets against the benchmark you edited.

Creating a benchmark profile

- 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** check box.

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 Vulnerability Manager scanner from the **Scan Server** list.
- 6 To enable dynamic scanning, click the **Dynamic server selection** check box.

If you configured domains in the **Admin > Domain Management** window, 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

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 beside 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**.

Associate a benchmark profile with, and monitor the results of, the question you created.

Monitoring asset compliance questions

- 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 Extreme Security 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 *Extreme SIEM Administration Guide*.
- 6 Select the **Enable the monitor results function for this question/simulation** check box.
- 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

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

The Scan Results page provides the following information:

Table 26: Scan results list 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.
Hosts	The number of hosts 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 running.
Duration	Displays the time taken for the scan to complete.

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

11 Policy Management

The 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.

Policy management use cases

Use the **Policy Management** pages with **Risk** dashboard items to find out 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 *Extreme SIEM* guide.

12 Network simulations in Extreme Networks Security Risk Manager

Simulations

Simulation of a network configuration change

Simulating an attack on an SSH protocol

Managing simulation results

Monitoring simulations

Grouping simulations

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

When you monitor a simulation, you can define how you want the system to respond when unapproved results are returned. A system response can be an email, the creation of an event, or to send the response to syslog.

Simulations can be modeled off of 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.

Simulations

The **Simulations** window provides the following information:

Table 27: Simulation definitions parameters

Parameter	Description
Simulation Name	The name of the simulation, as defined by the creator of the simulation.
Model	The model type. Simulations can be modeled from the current topology or another topology model. The options are: <ul style="list-style-type: none">• Current Topology• The name of the topology model
Groups	The groups that the simulation is associated with.
Created By	The user who created the simulation.

Table 27: Simulation definitions parameters (continued)

Parameter	Description
Creation Date	The date and time that the simulation was created.
Last Modified	The date and time that the simulation was last modified.
Schedule	The frequency the simulation is scheduled to run. The options include: Manual - The simulation runs when it is manually executed. Once - Specify the date and time the simulation is scheduled to run. Daily - Specify the time of day the simulation is scheduled to run. Weekly - Specify the day of the week and the time the simulation is scheduled to run. Monthly - Specify the day of the month and time the simulation is scheduled to run.
Last Run	The last date and time that the simulation was run.
Next Run	The date and time that the next simulation will be run.
Results	If the simulation is run, this parameter includes a list of dates for the results of your simulations. You can select a date and view the results.

Creating a simulation

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

Table 28: 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 targeting networks that are a member of one or more defined network locations.	Configure the networks parameter to specify the networks to which you want this simulation to apply.
Attack targets one of the following asset building blocks	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.
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.

Table 28: Simulation tests (continued)

Test Name	Description	Parameters
Attack targets assets susceptible to vulnerabilities with one of the following classifications	Allows you to simulate attacks targeting 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. Allows you to simulate attacks targeting 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	Allows you to simulate attacks targeting an asset that is susceptible to vulnerabilities discovered before, after, or on the configured date.	Configure the following parameters: before after on - Specify whether you want the simulation to consider the disclosed vulnerabilities to be after, before, or on the configured date on assets. The default is before. this date - Specify the date that you want this simulation to consider.
Attack targets assets susceptible to vulnerabilities where the name, vendor, version or service contains one of the following text entries	Allows you to simulate attacks targeting an asset that is susceptible to vulnerabilities matching the asset name, vendor, version or service based one or more text entry.	Configure the text entries parameter to identify the asset name, vendor, version, or service you want this simulation to consider.
Attack targets assets susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions	Allows you to simulate attacks targeting an asset that is susceptible to vulnerabilities matching the asset name, vendor, version or service based one or more regular expression.	Configure the regular expressions parameter to identify the asset name, vendor, version, or service you want this simulation to consider.

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.

- 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 check box, 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 beside 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 check box for any group you want to assign this simulation.
- 15 Click **Save Simulation**.

Editing a simulation

- 1 Click the **Risks** tab.
- 2 On the navigation menu, select **Simulation > Simulations**.
- 3 Select the simulation definition you want to edit.
- 4 From the **Actions** menu, select **Edit**.
- 5 Update parameters, as necessary.

For more information about the Simulation parameters, see [Simulation tests](#).
- 6 Click **Save Simulation**.

Duplicating a simulation

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

Deleting a simulation

- 1 Click the **Risks** tab.
- 2 On the navigation menu, select **Simulation > Simulations**.
- 3 Select the simulation you want to delete.
- 4 From the **Actions** menu, select **Delete**.
- 5 Click **OK**.

Manually running a simulation

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

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

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

Simulation of a network configuration change

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

Topology models provide the following key functionality:

- Create virtual topologies for testing network changes.
- Simulate attacks against virtual networks.
- Lower risk and exposure to protected assets through testing.
- Virtual network segments allow you 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

- 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

- 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

- 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** check box.
- 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 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.

Managing simulation results

Simulation results are retained for 30 days. Results only display in the Results column after a simulation runs.

Viewing simulation results

Results only display in the Results column 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.

When you click View Result, the following information is provided:

Table 29: 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 29: 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 Extreme Networks Security Risk Manager does not validate those assets against the database. Therefore, those assets are not considered in the Asset Compromised total. Risk Manager only validates assets 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.

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

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

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

The simulation result page provides a table called, Results for this step. This table provides the following information:

Table 30: Results for this step information

Parameter	Description
Approve	Allows you to approve simulation results. See Approving simulation results .
Parent	The originating IP address for the displayed step of the simulation.
IP	The IP address of the affected asset.
Network	The network of the target IP addresses, as defined in the network hierarchy.
Asset Name	The name of the affected asset, as defined by the asset profile.
Asset Weight	The weight of the affected asset, as defined in the asset profile.

- 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 using the list.
- 4 Click **View Result**. You can view the simulation result information, starting at step 1 of the simulation.
- 5 View the Results for this Step table to determine the assets that are affected.
- 6 To view the next step of the simulation results, click **Next Step**.

Approving simulation results

You can approve simulation results.

Results are only displayed in the **Results** column after a simulation runs.

- 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 check box 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 Click **View Approved** to view all approved assets.

Revoking a simulation approval

- 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 using the list.
- 4 **View Result**.
- 5 Click **View Approved** to view all approved assets.
- 6 Choose one of the following options:

Option	Description
Revoke Selected	Click the check box 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.

Monitoring simulations

When a simulation is in monitor mode, the defaults time range is 1 hour. This value overrides the configured time value when the simulation was created.

For information about event categories, see the [Extreme SIEM User Guide](#).

- 1 Click the **Risks** tab.
- 2 On the navigation menu, select **Simulation > Simulations**.
- 3 Select the simulation that you want to monitor.
- 4 Click **Monitor**.
- 5 In the **Event Name** field, type the name of the event you want to display on the **Log Activity** and **Offenses** tab.
- 6 In the **Event Description** field, type a description for the event. The description is displayed in the Annotations of the event details.
- 7 From the **High-Level Category** list, select the high-level event category that you want this simulation to use when processing events.
- 8 From the **Low-Level Category** list, select the low-level event category that you want this simulation to use when processing events.

- 9 Select the **Ensure the dispatched event is part of an offense** check box if you want, as a result of this monitored simulation, the events that are forwarded to the Magistrate component. If no offense was generated, then a new offense is created. If an offense exists, this event is added to the existing offense. If you select the check box, then choose one of the following options:

Option	Description
Question/Simulation	All events from a question are associated with a single offense.
Asset	A unique offense is created (or updated) for each unique asset.

- 10 In the **Additional Actions** section, select one or more of the following options:

Option	Description
Email	Select this check box and specify the email address to send notifications if the event is generated. Use a comma to separate multiple email addresses.
Send to Syslog	Select this check box if you want to log the event. For example, the syslog output might resemble: <pre>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: Eventdescription</pre>
Notify	Select this check box if you want events that generate as a result of this monitored question to display in the System Notifications item in the Dashboard.

- 11 In the **Enable Monitor** section, select the check box to monitor the simulation.
12 Click **Save Monitor**.

Grouping simulations

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**.
- 3 Click **Groups**.
- 4 From the menu tree, select the group under which you want to create a new group.
- 5 Click **New**.
- 6 In the **Name** field, type a name for the new group. The group name can be up to 255 characters in length.
- 7 In the **Description field**, type a description for the group. The description can be up to 255 characters in length.
- 8 Click **OK**.

13 Topology models

Creating a topology model
Editing a topology model
Duplicating a topology model
Deleting a topology model
Group topology models

You can create a network model based on a series of modifications that can be combined and configured. This allows you to determine the effect of configuration changes on your network using a simulation. For more information about simulations, see [Using simulations](#).

You can view topology models on the Simulations page. Topology models provides the following information:

Table 31: 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

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

Table 32: 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	<p>Configure the following parameters:</p> <p>devices - Specify the devices that you want to add to this rule. In the Customize Parameter window, select the All check box to include all devices or you can search devices by using one of the following search criteria:</p> <p>IP/CIDR - Select the IP/CIDR option and specify the IP address or CIDR that you want to add this rule to.</p> <p>Hostname - Select the Hostname option and specify the host name that you want to filter. To search for multiple host names, use a wildcard character (*) at the beginning or end of the string.</p> <p>Adapter - Select the Adapter option and use the menu to filter the device list by adapter.</p> <p>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.</p> <p>allows denies - Select the condition (accept or denied) for connections that you want this test to apply.</p> <p>CIDRs - Select any source IP addresses or CIDR ranges that you want to add to this rule.</p> <p>CIDRs - Select any destination IP addresses or CIDR ranges that you want to add to this rule.</p> <p>protocols - Specify the protocols that you want to add to this rule. To include all protocols, select the All check box.</p> <p>ports - Specify the ports that you want to add to this rule. To include all ports, select the All check box.</p>
A rule is added to the selected IPS devices that allows connections from source CIDRs to destination CIDRs with vulnerabilities	<p>Configure the following parameters:</p> <p>IPS devices - Specify the IPS devices that you want this topology model to include. To include all IPS devices, select the All check box.</p> <p>allows denies - Specify the condition (accept or denied) for connections that you want this test to apply.</p> <p>CIDRs - Specify any source IP addresses or CIDR ranges that you want this topology model to include.</p> <p>CIDRs - Specify any destination IP addresses or CIDR ranges that you want this topology model to include.</p> <p>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.</p>
The following assets allow connections to the selected ports	<p>Configure the following parameters:</p> <p>Assets - Specify the assets that you want this topology model to include.</p> <p>allow deny - Specify the condition (allow or deny) for connections that you want this topology model to apply. The default is allow.</p> <p>ports - Specify the ports that you want this topology model to include. To include all ports, select the All check box.</p>
Assets in the following asset building blocks allow connections to ports	<p>Configure the following parameters:</p> <p>Assets building blocks - Specify the building blocks that you want this topology model to include.</p> <p>allow deny - Specify the condition (allow or deny) that you want this topology model to apply. The default is allow.</p> <p>ports - Specify the ports that you want this topology model to include. To include all ports, select the All check box.</p>

- 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.
- 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 check box to assign groups to this question.
- 8 Click **Save Model**.

Editing a topology model

- 1 Click the **Risks** tab.
- 2 On the navigation menu, select **Simulation > Topology Models**.
- 3 Select the model definition you want to edit.
- 4 From the **Actions** menu, select **Edit**.
- 5 Update parameters, as necessary.
For more information about the Model Editor parameters, see [Creating a topology model](#).
- 6 Click **Save Model**.

Duplicating a topology model

- 1 Click the **Risks** tab.
- 2 On the navigation menu, select **Simulation > Topology Models**.
- 3 Select the model definition you want to duplicate.
- 4 From the **Actions** menu, select **Duplicate**.
- 5 Type a name that you want to assign to the copied topology model.
- 6 Click **OK**.
- 7 Edit the model.

Deleting a topology model

- 1 Click the **Risks** tab.
- 2 On the navigation menu, select **Simulation > Topology Models**.
- 3 Select the model definition you want to delete.
- 4 From the **Actions** menu, select **Delete**.
- 5 Click **OK**.

Group topology models

Categorizing your topology model is an efficient way to view and track your models. For example, you can view all topology models related to compliance.

As you create new topology models, you can assign the topology models to an existing group. For information on assigning a group, see [Creating a topology model](#).

Viewing groups

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

Creating a group

- 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.

Editing a group

- 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 you want to edit.
- 5 Click **Edit**.
- 6 Update values for the parameters
- 7 Click **OK**.
- 8 If you want to change the location of the group, click the new group and drag the folder to location in your menu tree.

Copying an item to another group

- 1 Click the **Risks** tab.
- 2 On the navigation menu, select **Simulations > Topology Models**.
- 3 Click **Groups**.
- 4 From the menu tree, select the question you want to copy to another group.
- 5 Click **Copy**.
- 6 Select the check box for the group to which you want to copy the simulation.

- 7 Click **Copy**.

Assign a topology to a group

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

Deleting an item from a group

- 1 Click the **Risks** tab.
- 2 On the navigation menu, select **Simulation > Simulations**.
- 3 Click **Groups**.
- 4 From the menu tree, select the top level group.
- 5 From the list of groups, select the item or group you want to delete.
- 6 Click **Remove**.
- 7 Click **OK**.

14 Managing Extreme Networks Security Risk Manager reports

Manually generating a report
Use the report wizard
Creating a report
Editing a report
Duplicating a report
Sharing a report
Configuring charts

The following report options are specific to Risk Manager:

Table 33: Report options for Risk Manager

Report option	Description
Connections	The connection diagrams for your network devices that occurred during your specified time frame.
Device rules	The rules configured on your network device during your specified time frame. You can view the following rule types for one or many network devices using this report option: Most used accept rules Most used deny rules Least used accept Least used deny rules Shadowed rules Unused object rules
Device unused objects	Produces a table with the name, configuration date/time, and a definition for any object reference groups that are not in use on the device. An object reference group is a generic term used to describe a collection of IP addresses, CIDR addresses, host names, ports, or other device parameters which are grouped together and assigned to rules on the device.

Manually generating a report

Manually generating a report does not reset the existing report schedule. For example, if you generate a weekly report for most active firewall denies, then manually generate the report, the weekly report still generates on the schedule you initially configured.

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 the report is in the queue. For example, 1 of 3.

- **(x hour(s) x min(s) y sec(s))** - The report is scheduled to run. The message is a count-down timer that specifies when the report will run next.

- 1 Click the **Reports** tab.
- 2 Select the report that you want to generate.
- 3 Click **Run Report**.
- 4 Optional. Click **Refresh** to refresh the view, including the information in the **Next Run Time** column.

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

Use the report wizard

The wizard uses the following key elements to help you create a report:

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

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

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

Creating a report

A report can consist of several data elements and can represent network and security data in a variety of styles, such as tables, line charts, pie charts, and bar charts.

You can specify Report Console or email for report distribution options. The following table describes the parameters on for these distribution options.

Table 34: Generated report distribution options

Option	Description
Report Console	Select this check box to send the generated report to the Reports tab. This is the default distribution channel.
Select the users that should be able to view the generated report.	This option is only displayed after you select the Report Console check box. From the list of users, select the Extreme Networks Security Risk Manager users 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 <i>Extreme SIEM Administration Guide</i> .

Table 34: Generated report distribution options (continued)

Option	Description
Select all users	This option is only displayed after you select the Report Console check box. Select this check box if you want to grant permission to all 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 <i>Extreme SIEM Administration Guide</i> .
Email	Select this check box if you want to distribute the generated report using email.
Enter the report distribution email address(es)	This option is only displayed after you select the Email check box. Type the email address for each generated report recipient; separate a list of email addresses with commas. The maximum characters for this parameter is 255. Email recipients receive this email from no_reply_reports@qradar.
Include Report as attachment (non-HTML only)	This option is only displayed after you select the Email check box. Select this check box to send the generated report as an attachment.
Include link to Report Console	This option is only displayed after you select the Email check box. Select this check box to include a link the Report Console in the email.

- 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.
- 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**.
- 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 ExtremeSecurity logo is the default logo. For more information about branding your report, see the *Extreme SIEM Administration Guide*.
- 10 From the **Chart Type** list, select one of the Risk Manager specific reports.
- 11 Configure the report data for your chart.
- 12 Click **Save Container Details**.
- 13 Click **Next**.
- 14 Select report formats. You can select multiple options.


Note

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

- 15 Click **Next**.
- 16 Select the distribution channels that you want for your report.
- 17 Click **Next**.
- 18 Type a description for this report. The description is displayed on the Report Summary page and in the generated report distribution email.

- 19 Select the groups to which you want to assign this report. For more information about groups, see Managing Reports in the *Extreme SIEM Administration Guide*.
- 20 Optional. Select yes to run this report when the wizard setup is complete. Click **Next** to view the report summary. You can select the tabs available on the summary report to preview the report selections.
- 21 Click **Finish**.

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

The report title is the default title for the generated report. If you 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.

Editing a 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 Extreme Networks Security 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 ExtremeSecurity logo is the default logo. For more information about branding your report, see the *Extreme SIEM 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 required, repeat steps these steps to edit additional 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.



Note

Risk Manager-specific reports, such as Device Rule and Device Unused Object reports only support PDF, HTML, and RTF 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 *Extreme SIEM Administration Guide*.
- 17 Optional. Select yes to run this report when the wizard setup is complete.
- 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

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

Sharing a 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

Any updates that the user makes to a shared report does not affect the original version of the report.

- 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 *Extreme SIEM User Guide*.

Configuring charts

The following chart types are specific to Risk Manager:

- [Connection](#)
- [Device rules](#)
- [Device Unused Objects](#)

Connection charts

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 35: Connections chart parameters

Parameter	Description
Container Details - Connections	
Chart Title	Type a chart title to a maximum of 100 characters.
Chart Sub-Title	Clear the check box to change the automatically created 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. Options include: Bar - Displays the data in a bar chart. This is the default graph type. This graph type requires the saved search to be a grouped search. Line - Displays the data in a line chart. Pie - Displays the data in a pie chart. This graph type requires the saved search to be a grouped search. Stacked Bar - Displays the data in a stacked bar chart. Stacked Line - Displays the data in a stacked line chart. Table - Displays the data in table format. The Table option is only available for the full page width container only.
Graph	From the list, 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: <ol style="list-style-type: none"> 1 From the From list box, type the start date that you want for the report, or select the date by using the Calendar 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 Calendar 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.
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.

Table 35: Connections chart parameters (continued)

Parameter	Description
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.
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 or typing the name of a known saved search in the Type Saved Search or Select from List field.
Create New Connection Search	Click Create New Connection Search to create a new search.

Device Rules charts

Device Rule reports allows you to create a report for the following firewall rules:

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

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

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

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

Table 36: 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 rules based on the event count across all devices that are visible to Risk Manager.
Type	<p>Select the type of device rules to display in the report. Options include:</p> <p>Most Used Accept Rules - Displays the most used accept rules by event count for a single device or a group of devices. This report lists the rules with highest accepted event counts, in descending order, for the time frame you specified in the report.</p> <p>Most Used Deny Rules - Displays the most used deny rules by event count for a single device or a group of devices. This report lists the rules with the highest deny event counts, in descending order, for the time frame you specified in the report.</p> <p>Unused Rules - Displays any rules for a single device or a group of devices that are unused. Unused rules have zero event counts for the time frame you specified for the report.</p> <p>Least Used Accept Rules - Displays the least used accept rules for a single device or a group of devices. This report lists rules with the lowest accept event counts, in ascending order, for the time frame you specified in the report.</p> <p>Least Used Deny Rules - Displays the least used deny rules for a single device or a group of devices. This report lists rules with the lowest denied event counts, in ascending order, for the time frame you specified in the report.</p> <p>Shadowed Rules - Displays any rules for a single device that can never trigger because the rule is blocked by a proceeding rule. The results display a table of the rule creating the shadow and any the rules that can never trigger on your device because they are shadowed by a proceeding rule on the device.</p> <p>Note: Shadowed rule reports can only be run against a single device. These rules have zero event counts for the time frame you specified for the report and are identified with an icon in the Status column.</p>
Date/Time Range	<p>Select the time frame for your report. The options include:</p> <p>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.</p> <p>Interval - The results of the Device Rules report is based on the rules that existed during the time frame of the interval. This report displays rules and event counts for the specified interval from the last hour to 30 days.</p> <p>Specific Range - The results of the Device Rules report is based on the rules that existed between the start time and end time of the time range. This report displays rules and event counts for the specified time frame.</p>
Timezone	<p>Select the timezone you want to use as a basis for your report. The default timezone is based on the configuration of your Extreme Networks SIEM Console. When configuring the Timezone parameter for your report, consider the location of the devices associated with the reported data. If the report uses data spanning multiple time zones, the data used for the report is based on the specific time range of the time zone. For example, if your Extreme Networks SIEM Console is configured for Eastern Standard Time (EST) and you schedule a daily report between 1pm and 3pm and set the timezone as Central Standard Time (CST), the results in the report contains information from 2pm and 4pm EST.</p>



Table 36: Device Rules Chart parameters (continued)

Parameter	Description
Targeted Data Selection	<p>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 over a custom defined period of time, with the option to only include data from the hours and days that you select.</p> <p>For example, you can schedule a report to run from October 1 to October 31 and view your most active, least active or unused rules and their rule counts that occur during your business hours, such as Monday to Friday, 8 AM to 9 PM.</p> <p>Note: The filter details only display when you select the Targeted Data Selection check box in the Report Wizard.</p>
Format	<p>Select the format for your device rules report. The options include:</p> <p>One aggregate report for specified devices - This report format aggregates the report data across multiple devices.</p> <p>For example, if you create a report to display the top ten most denied rules, then an aggregate report displays the top ten most denied rules across all of the devices you have selected for the report. This report returns 10 results in total for the report.</p> <p>One report per device - This report format displays the report data for one device.</p> <p>For example, if you create a report to display the top ten most denied rules, then an aggregate report displays the top ten most denied rules for each device you have selected for the report. This report returns the top 10 results for every device selected for the report. If you selected 5 devices, the report returns 50 results.</p> <p>Note: Shadowed rule reports are only capable of displaying one report per device.</p>
Devices	<p>Select the devices included in the report. The options include:</p> <p>All Devices - Select this option to include all devices in Risk Manager in your report.</p> <p>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.</p> <p>Specific Devices - Select this option to only include specific devices in your report. The Device Selection window allows you to select and add devices to your report.</p> <p>To add individual devices to your report:</p> <ol style="list-style-type: none"> 1 Click Browse to display the Device Selection window. 2 Select any devices and click Add Selected. <p>To add all devices to your report:</p> <ol style="list-style-type: none"> 1 Click Browse to display the Device Selection window. 2 Click Add All. <p>To search for devices to include in your report:</p> <ol style="list-style-type: none"> 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

This report displays object references, such as a collection of IP address, CIDR address ranges, or host names that are unused by your network device.

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

Table 37: 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	<p>Select the devices included in the report. The options include:</p> <p>All Devices - Select this option to include all devices in Extreme Networks Security Risk Manager in your report.</p> <p>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.</p> <p>Specific Devices - Select this option to only include specific devices in your report. The Device Selection window allows you to select and add devices to your report.</p> <p>To add individual devices to your report:</p> <ol style="list-style-type: none"> 1 Click Browse to display the Device Selection window. 2 Select any devices and click Add Selected. <p>To add all devices to your report:</p> <ol style="list-style-type: none"> 1 Click Browse to display the Device Selection window. 2 Click Add All. <p>To search for devices to include in your report:</p> <ol style="list-style-type: none"> 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.

15 Audit log data

Logged actions
Viewing user activity
Viewing the log file
Log file details

All logs display in the Risk Manager Audit category. For more information about using the **Log Activity** tab in Extreme SIEM, see the *Extreme SIEM User Guide*.

Logged actions

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

Table 38: Logged actions

Category	Action
Policy Monitor	Create a question.
	Edit a question.
	Delete a question.
	Submit a question manually.
	Submit a question automatically.
	Approve results.
	Revoke results approval.
Topology Model	Create a topology model.
	Edit a topology model.
	Delete a topology model.
Topology	Save layout.
	Create a topology saved search.
	Edit a topology saved search
	Delete a topology saved search
	Placing an IPS.
Configuration Monitor	Create a log source mapping
	Edit a log source mapping
	Delete a log source mapping
Simulations	Create a simulation.

Table 38: Logged actions (continued)

Category	Action
	Edit a simulation.
	Delete a simulation.
	Manually run a simulation.
	Automatically run a simulation.
	Approve simulation results.
	Revoke simulation results.
Configuration Source Management	Successfully authenticate for the first time on a session.
	Add a device.
	Remove a device.
	Edit the IP address or adapter for a device.
	Save a credential configuration.
	Delete a credential configuration.
	Save a protocol configuration.
	Remove a protocol configuration.
	Create a schedule for a backup job.
	Delete a schedule for a backup job.
	Edit a backup job.
	Add a backup job.
	Delete a backup job.
	Run a scheduled backup job.
	Complete a scheduled job whether the job is successful or has failed.
	After a backup job has completed processing and the configuration was persisted, no changes discovered.
	After a backup job has completed processing and the configuration was persisted, changes were discovered.
	After a backup job has completed processing and the configuration was persisted, unpersisted changes were discovered.
	After a backup job has completed processing and the configuration that was previously persisted no longer resides on the device.
	Adapter operation attempt has begun, which includes protocols and credentials.
	Adapter operation attempt has been successful, including the protocols and credentials.

Viewing user activity

- 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 Optional. From the **Low Level Category** drop-down list, select a category to refine your search.
- 5 Click **Add Filter**.
- 6 Click **Filter** to search for Risk Manager events.

Viewing the log file

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. Extreme Networks Security Risk Manager can store up to 50 archived log files.

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

Each entry in the log file displays using the following format:

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

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

Table 39: 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 host name of the Console where this activity was logged.
<user>	The name of the user that performed the action.
<IP address>	The IP address of the user that performed 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.
<action>	The activity that occurred.
<payload>	The complete record that has changed, if any.

- 1 Using SSH, log in to your Extreme Networks SIEM Console as the root user.
- 2 Using SSH from the Extreme Networks SIEM Console, log in to the 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

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

Table 40: Risk Manager log files

Log file name	Location	Description
<code>audit.log</code>	<code>/var/log/audit/</code>	Contains the current audit information.
<code>audit.<1-50>.gz</code>	<code>/var/log/audit/</code>	Contains archived audit information. When the <code>audit.log</code> file reaches 200 MB in size, it is compressed and renamed to <code>audit.1.gz</code> . The file number increments each time a log file is archived. Risk Manager can store up to 50 archived log files.
<code>qradar.log</code>	<code>/var/log/</code>	Contains all process information that is logged by the Risk Manager server.
<code>qradar.error</code>	<code>/var/log/</code>	All exceptions and <code>System.out</code> and <code>System.err</code> messages that are generated by the Risk Manager server are logged in this file.

A Glossary

A
C
M
N
R
S
T
V

This glossary provides terms and definitions for the Extreme Networks Security Risk Manager software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the [IBM® Terminology website](#) (opens in new window).

[A](#) on page 121 [C](#) on page 122 [M](#) on page 122 [N](#) on page 122 [R](#) on page 122 [S](#) on page 122 [T](#) on page 122 [V](#) on page 123

A

adapter	An intermediary software component that allows two other software components to communicate with one another.
asset	A manageable object that is either deployed or intended to be deployed in an operational environment.
asset test	A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.
attack	Any attempt by an unauthorized person to compromise the operation of a software program or networked system.
attack path	The source, destination, and devices associated with an attack.
attribute	Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

C

- connection graph** A graph that shows connections from remote network nodes and local IP addresses to local network nodes.
- connection line** A line on the connection graph between a remote network node and a local network node or between two local network nodes.
- contributing test** A test that examines the risk indicators that are specified in a question.

M

- multiple-context device** A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

- NAT** See [Network Address Translation](#).
- NAT indicator** An indicator on the topology graph that shows that the path between two network connections contains either source or destination address translations.
- neighbor data** Data collected from adapters that is used to discover information about devices that are connected to ExtremeSecurity Quality Manager managed hosts.
- Network Address Translation (NAT)** In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

R

- restrictive test** A test that filters the results returned by a contributing test question.
- risk indicator** A measure of the potential exposure of a system to a security breach.
- risky protocol** A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.
- rule** A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

- sub-search** A function that allows a search query to be performed within a set of completed search results.

T

- time series chart** A graphical representation of network connections over time.
- topology graph** A graph that describes subnets, devices, and firewalls.
- topology model** A virtual representation of the arrangement of network assets that is used to simulate an attack.

V

violation An act that bypasses or contravenes corporate policy.

vulnerability A security exposure in an operating system, system software, or application software component.

Index

A

- actual communication
 - contributing questions 56
- add asset 84
- assess devices 66
- asset compliance question 89
- asset profile 84
- asset profiles 87
- asset question 65
- Asset results 69
- assets 66
- assets tab 84
- attack path 52
- audit log
 - actions 117
- audit log data 117

B

- back up information 27
- backup configuration information 27
- backup job 27, 29, 30
- backup job renaming 30
- backup log 27
- Backup Log Viewer 27
- backup status 27
- browser mode
 - Internet Explorer web browser 12

C

- charts
 - configuring 111
 - connections 112
 - Device Rules 113
 - Device Unused Objects 116
- CheckPoint SmartConsole
 - rule counting 77
- compliance 88
- compliance benchmarks 88
- configuration 16
- configuration source management 19
- connection graph 37
- connections
 - searching 39
- Conventions
 - notice icons 6
 - text 6
- CPSMS 79
- creating
 - benchmark scan profiles 88
- credentials
 - configuring 21

D

- default log in information 12
- deprecated contributing questions 58
- Deprecated contributing test questions 62
- device
 - adding 24
 - deleting 25
 - importing 22
- device configuration
 - comparing 46
- device discovery 21, 22
- device groups
 - grouping devices 52
- device import, CSV file 23
- device list
 - filtering 25
- device results 71
- device rules filtering 49
- Device/rules test questions 63
- devices
 - adding 24
- devices/rules question 67
- discovery schedule 32
- document mode
 - Internet Explorer web browser 12
- Documentation feedback 7
- Documentation, related 8
- dynamic routing 12

E

- edit asset 84
- export 75
- exporting 44

G

- glossary 121
- graph 36–38
- graphs 36

H

- high availability (HA) 12

I

- import 75
- importance factor 64
- introduction 6
- Intrusion Prevention System
 - removing 52
- IPS 52
- IPv6 12

L

- log data 117
- log file 119, 120
- log in information 12
- log locations 120
- log source mapping
 - creating 48

M

- monitor mode 73, 89
- monitor questions 73, 89

N

- NAT indicators 51
- neighbor data
 - collecting 26
- network administrator 6
- network configuration 96
- network connections
 - monitor 13-15
- network device configuration
 - investigating 45
- new features
 - version 7.2.7 user guide overview 10
- non-contiguous network masks 12

O

- offense 52
- open port 97

P

- password 12
- PCI section 1 66
- PCI section 10 66
- policy monitor
 - delete item from question group 106
 - managing questions 55
 - use cases 82
- policy monitor questions
 - evaluating results 72
 - exporting 75
 - grouping 74
 - importing 76
- policy monitor use case
 - actual communication for DMZ 65
 - device test communication for Internet access 68
 - possible communication on protected assets 66
- possible communication tests
 - contributing questions 60
 - restrictive tests 62
- protocol 97
- protocols 30, 31, 97
- protocols:risky 66

Q

- QRadar Risk Manager
 - integration 76
- QRadar Risk Manager overview 11
- question
 - submitting 68

R

- report
 - duplicating 111
 - editing 110
 - sharing 111
- report wizard 108
- reports
 - managing 107
 - manually generating 107
- restrictive questions 59
- results
 - approving 72
- risks for networks 96

S

- save asset search criteria 87
- save criteria 87
- saving 43
- scan results
 - viewing 89
- search
 - canceling 43
 - CSM 81
 - rule counting configuration 82
 - SmartDashboard 78
- search criteria 40
- search results 42, 43
- searching 42
- security integrations
 - QRadar Risk Manager 76
- simulation
 - deleting 96
 - duplicating 96
 - manual simulation 96
- simulation approval
 - revoking 100
- simulation creation 97
- simulation results
 - approving 99
 - managing 98
- simulation tests 93
- simulations
 - editing 95
 - grouping 101
 - monitoring 100
- Simulations 92
- SSH simulation 97
- sub-search 42
- Support 7

system information 16
system time 17

T

Technical support
 contacting 7
time series graph 36, 38
topology models
 group 104
topology graph 50
topology model
 assign to a group 106
 copy models to groups 105
 creating 102
 creating a group 105
 deleting 104
 duplicating 104
 editing 104
 editing a group 105
 viewing groups 105

U

unsupported features 12
user activity
 audit log 117, 119
user name 12

V

viewing
 scan results 89
violations 73

W

what's new
 version 7.2.7 user guide overview 10