



Extreme Networks Security Risk Manager Getting Started Guide

Copyright © 2011–2015 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: www.extremenetworks.com/documentation/

For information, contact:

Extreme Networks, Inc.
145 Rio Robles
San Jose, California 95134
USA

Table of Contents

Preface.....	4
Conventions.....	4
Providing Feedback to Us.....	5
Getting Help.....	5
Related Publications.....	6
Chapter 1: Get Started with Risk Manager.....	8
Chapter 2: Deploy Risk Manager.....	9
Before You Install.....	9
Configure Port Access on Firewalls.....	10
Identify Network Settings.....	10
Unsupported Features in Risk Manager.....	10
Access the Risk Manager User Interface.....	11
Setting Up a Risk Manager Appliance.....	11
Adding Risk Manager to SIEM Console.....	11
Establishing Communication.....	13
Adding the Risk Manager User Role.....	13
Chapter 3: Network Data Collection.....	14
Credentials.....	14
Discovering Devices.....	16
Obtaining Device Configuration.....	16
Import Devices.....	16
Chapter 4: Manage Audits.....	19
Use Case: Configuration Audit.....	19
Use Case: View Network Paths in the Topology.....	21
Use case: Visualize the Attack Path of an Offense.....	22
Chapter 5: Use Case: Monitor Policies	24
Use Case: Assess Assets That Have Suspicious Configurations.....	25
Use Case: Assess Assets with Suspicious Communication.....	25
Use Case: Monitor Policies for Violations.....	26
Use Case: Use Vulnerabilities to Prioritize Risks.....	27
Use Case: Prioritize Asset Vulnerabilities by Zone or Network Communications.....	27
Chapter 6: Use Cases for Simulations.....	29
Use Case: Simulate Attacks on Network Assets.....	29
Use Case: Simulate the Risk of Network Configuration Changes.....	30

Preface

Conventions

This section discusses the conventions used in this guide.

Text Conventions

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

Table 1: Notice Icons






Icon	Notice Type	Alerts you to...
	Tip	Helpful tips for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	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]
Words in <i>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.

Platform-Dependent Conventions

Unless otherwise noted, all information applies to all platforms supported by ExtremeXOS software, which are the following:

- BlackDiamond® X series switch
- BlackDiamond 8800 series switches
- Cell Site Routers (E4G-200 and E4G-400)
- Summit® family switches
- SummitStack™

When a feature or feature implementation applies to specific platforms, the specific platform is noted in the heading for the section describing that implementation in the ExtremeXOS command documentation. In many cases, although the command is available on all platforms, each platform uses specific keywords. These keywords specific to each platform are shown in the Syntax Description and discussed in the Usage Guidelines.

Terminology

When features, functionality, or operation is specific to a switch family, the family name is used. Explanations about features and operations that are the same across all product families simply refer to the product as the "switch."

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 Global Technical Assistance Center using one of the following methods:

Web	www.extremenetworks.com/support
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-603-952-5000 For the Extreme Networks support phone number in your country: www.extremenetworks.com/support/contact
Email	support@extremenetworks.com To expedite your message, enter the product name or model number in the subject line.

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

- Your Extreme Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)

- The serial and revision numbers of all involved Extreme Networks products in the network
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load and frame size 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 previous Return Material Authorization (RMA) numbers

Related Publications

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

Extreme Security Analytics Threat Protection

- *Extreme Networks Security API Reference Guide*
- *Extreme Networks Security Application Configuration Guide*
- *Extreme Networks Security Ariel Query Language Guide*
- *Extreme Networks Security DSM Configuration Guide*
- *Extreme Security DSM Configuration Guide Addendum*
- *Extreme Networks Security Hardware Guide*
- *Extreme Networks Security Installation Guide*
- *Extreme Networks Security Juniper NSM Plug-in User Guide*
- *Extreme Networks Security Log Manager Administration Guide*
- *Extreme Networks Security Log Sources User Guide*
- *Extreme Networks Security Managing Log Sources Guide*
- *Extreme Networks Security Offboard Storage Guide*
- *Extreme Security Release Notes*
- *Extreme Networks Security Risk Manager Adapter Configuration Guide*
- *Extreme Networks Security Risk Manager Getting Started Guide*
- *Extreme Networks Security Risk Manager Installation Guide*
- *Extreme Networks Security Risk Manager Migration Guide*
- *Extreme Networks Security Risk Manager User Guide*
- *Extreme Networks Security Troubleshooting System Notifications Guide*
- *Extreme Networks Security Upgrade Guide*
- *Extreme Networks Security Vulnerability Manager Release Notes*
- *Extreme Networks Security Vulnerability Manager User Guide*
- *Extreme Networks Security WinCollect User Guide*
- *Extreme Networks SIEM Administration Guide*
- *Extreme Networks SIEM Getting Started Guide*
- *Extreme Networks SIEM High Availability Guide*
- *Extreme Networks SIEM Troubleshooting Guide*
- *Extreme Networks SIEM Tuning Guide*

- *Extreme Networks SIEM Users Guide*
- *Migrating Extreme Security Log Manager to Extreme SIEM*

Extreme Security Threat Protection

- *Extreme Security Intrusion Prevention System Hardware Replacement Guide*
- *Extreme Security Threat Protection Release Notes*

1 Get Started with Risk Manager

Risk Manager is a separately installed appliance. Use Risk Monitor to monitor device configurations, simulating changes to your network environment, and prioritize risks and vulnerabilities in your network.

Risk Manager is accessed from the **Risks** tab on the SIEM Console.

Risk Manager enhances SIEM by providing administrator with tools to complete the following tasks:

- Centralize risk management.
- Use a topology to view your network.
- Configure and monitor network devices.
- View connections between network devices.
- Search firewall rules.
- View existing rules and the event count for triggered rules.
- Search for devices and paths for your network devices.
- Monitor and audit your network to ensure compliance.
- Define, schedule, and run exploit simulations on your network.
- Search for vulnerabilities.

Centralized risk management and compliance for increased intelligence of information might involve the cooperation of many internal teams. As a next generation SIEM with an additional Risk Management appliance, we reduce the number of steps that are required from first-generation SIEM products. We provide network topology and risk assessment for assets that are managed in SIEM.

During the evaluation process, you consolidate your system, security, risk analysis, and network information through aggregation and correlation, providing complete visibility into your network environment. You also define a portal to your environment, which provides visibility and efficiency that you cannot achieve by using manual processes and other point product technologies.

2 Deploy Risk Manager

Before You Install

[Configure Port Access on Firewalls](#)

[Identify Network Settings](#)

[Unsupported Features in Risk Manager](#)

[Access the Risk Manager User Interface](#)

[Setting Up a Risk Manager Appliance](#)

[Adding Risk Manager to SIEM Console](#)

[Establishing Communication](#)

[Adding the Risk Manager User Role](#)

Your Risk Manager appliance is installed with the latest version of Risk Manager software.

You must install the Risk Manager evaluation appliance. The software requires activation and you must assign an IP address to the Risk Manager appliance.

If you need assistance to activate your software and assigning an IP address, contact customer support.

The appliance is ready to accept information from your network devices.

For information about using Risk Manager, see the *Risk Manager User Guide*.

To deploy Risk Manager in your environment, you must:

- 1 Ensure that the latest version of SIEM is installed.
- 2 Ensure all pre-installation requirements are met.
- 3 Set-up and power on your Risk Manager appliance.
- 4 Install the Risk Manager plug-in on your SIEM console.
- 5 Establish communication between SIEM and the Risk Manager appliance.
- 6 Define user roles for your Risk Manager users.

Before You Install

You must complete the installation process for an SIEM Console before you install Risk Manager. As a best practice, install SIEM and Risk Manager on the same network switch.

You must review the following information:

- [Configure firewall port access](#)
- [Identify network settings](#)
- [Unsupported features in Risk Manager](#)
- [Supported web browsers](#)

Before you install the Risk Manager evaluation appliance, ensure that you have:

- space for a two-unit appliance
- rack rails and shelving that are mounted

Optionally, you might want a USB keyboard and standard VGA monitor to access the SIEM Console.

Configure Port Access on Firewalls

Firewalls between the SIEM Console and Risk Manager must allow traffic on certain ports.

Ensure that any firewall located between the SIEM console and Risk Manager allows traffic on the following ports:

- Port 443 (HTTPS)
- Port 22 (SSH)
- Port 37 UDP (Time)

Identify Network Settings

You must gather information about your network settings before starting the installation process.

Gather the following information for your network settings:

- Host name
- IP address
- Network mask address
- Subnet mask
- Default gateway address
- Primary Domain Name System (DNS) server address
- Secondary DNS server (optional) address
- Public IP address for networks that use Network Address Translation (NAT) email server name
- Email server name
- Network Time Protocol (NTP) server (Console only) or time server name

Unsupported Features in Risk Manager

It is important to be aware of the features that are not supported by Risk Manager.

The following features are not supported in Risk Manager:

- High availability (HA)
- Dynamic Routing for Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), or Routing Information Protocol (RIP)
- IPv6
- Non-contiguous network masks
- Load-balanced routes
- Reference maps
- Store and Forward

Access the Risk Manager User Interface

Risk Manager uses default login information for the URL, user name, and password.

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

Table 3: Default login information for Risk Manager

Login information	Default
URL	https://<IP address>, where <IP address> is the IP address of the SIEM 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.

Setting Up a Risk Manager Appliance

You must connect the management interface and ensure that the power connections are plugged into the Risk Manager appliance.

[Read, understand, and obtain the prerequisites.](#)

The Risk Manager evaluation appliance is a two-unit rack mount server. Rack rails and shelving are not provided with evaluation equipment.

The Risk Manager appliance includes four network interfaces. For this evaluation, use the network interface that is labeled ETH0 as the management interface. The other interfaces are monitoring interfaces. All of the interfaces are on the back panel of the Risk Manager appliance.

The power button is on the front panel.

- 1 Connect the management network interface to the port labeled ETH0.
- 2 Ensure that the dedicated power connections are plugged into the rear of the appliance.
- 3 Optional. To access the SIEM console, connect the USB keyboard and a standard VGA monitor.
- 4 If there is a front pane on the appliance, remove the pane by pushing in the tabs on either side and pull the pane away from the appliance.
- 5 Press the power button on the front to turn on the appliance.

The appliance begins the boot process.

Adding Risk Manager to SIEM Console

You must add Risk Manager as a managed host to SIEM Console.

If you want to enable compression, then the minimum version for each managed host must be SIEM Console 7.1 or Risk Manager 7.1.

To add a non-NATed managed host to your deployment when the Console is NATed, you must change the SIEM Console to a NATed host. You must change the console before you add the managed host to your deployment. For more information, see the *Extreme Networks SIEM Administration Guide*.

- 1 Open your web browser.
- 2 Type the URL, `https://<IP Address>`, where <IP Address> is the IP address of the SIEM Console.
- 3 Type your user name and password.
- 4 On the **Admin** tab, click **Deployment Editor**.
- 5 From the menu, select **Actions**, and then select **Add a Managed Host**.
- 6 Click **Next**.
- 7 Enter values for the following parameters:

Option	Description
Enter the IP of the server or appliance to add	The IP address of Risk Manager.
Enter the root password of the host	The root password for the host.
Confirm the root password of the host	Confirmation for your password.
Host is NATed	To enable NAT for a managed host, the NATed network must be using static NAT translation. For more information, see the <i>Extreme Networks SIEM Administration Guide</i> .
Enable Encryption	Creates an SSH encryption tunnel for the host. To enable encryption between two managed hosts, each managed host must be running Extreme Security console 7.1 or Risk Manager 7.1.
Enable Compression	Enables data compression between two managed hosts.

- 8 Choose one of the following options:

- If you selected the **Host is NATed** check box, then you must enter values for the NAT parameters.

Option	Description
Enter public IP of the server or appliance to add	The public IP address of the managed host. The managed host uses this IP address to communicate with other managed hosts in different networks that use NAT.
Select NATed network	The network that you want this managed host to use. If the managed host is on the same subnet as the Extreme Security console, select the console of the NATed network. If the managed host is not on the same subnet as the SIEM Console, select the managed host of the NATed network.

- If you did not select the **Host is NATed** check box, click **Next**.

- 9 Click **Finish**.

This process can take several minutes to complete. If your deployment includes changes, then you must deploy all changes.

- 10 Click **Deploy**.

Clear your web browser cache and then log in to Extreme Security console. The **Risks** tab is now available.

Establishing Communication

You must establish communication between your Risk Manager appliance and your SIEM console before you set up and configure Risk Manager.

The process to establish communications might take several minutes to complete. If you change the IP address of your Risk Manager appliance or need to connect Risk Manager to another SIEM console, you can use the **Risk Manager Settings** on the SIEM **Admin** tab.

- 1 Open your web browser, and then clear the web browser cache.
- 2 Log in to SIEM. For information about the IP address, user name or root password, see [Accessing the Risk Manager user interface](#).
- 3 Click the **Risks** tab.
- 4 Type values for the following parameters:

Option	Description
IP/Host	The IP address or host name of the Risk Manager appliance
Root Password	The root password of the Risk Manager appliance.

- 5 Click **Save**.

[Define user roles.](#)

Adding the Risk Manager User Role

You must assign the Risk Manager user role to provide access to Risk Manager.

By default, SIEM provides a default administrative role, which provides access to everything in Risk Manager. A user that is assigned administrative privileges, including the default administrative role, cannot edit their own account. Another administrative user must make any required changes.

For information about creating and managing user roles, see the *SIEM Administration Guide*.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **System Configuration**.
- 3 In the **User Management** pane, click **User Roles**.
- 4 In the left pane, select the user role that you want to edit.
- 5 Select the **Risk Manager** check box.
- 6 Click **Save**.
- 7 Click **Close**.
- 8 On the **Admin** tab, click **Deploy Changes**.

3 Network Data Collection

Credentials

Discovering Devices

Obtaining Device Configuration

Import Devices

You must configure Risk Manager to read configuration information from the devices in your network.

The configuration information that is collected from your network devices generates the topology for your network and allows Risk Manager to understand your network configuration.

Data that is collected in Risk Manager is used to populate the topology with key information about your network environment.

Data collection is a three-step process:

- Provide Risk Manager **with the credentials** to download network device configurations.
- **Discover devices** to create a device list in Configuration Source Management.
- Back up the device list to **obtain the device configurations** and populate the topology with data about your network.

Credentials

Risk Manager must be configured with the credentials to access and download the device configurations. Credentials allow Risk Manager to connect to firewalls, routers, switches, or Intrusion Prevention System (IPS) devices.

Administrators use **Configuration Source Management** to input device credentials, which provide Risk Manager with access to a specific device. Risk Manager can save individual device credentials for a specific network device. If multiple network devices use the same credentials, you can assign credentials to a group. For example, you can assign credentials to a group if all firewalls in the organization have the same user name and password. The credentials are associated with the address sets for all the firewalls and are used to back up device configurations for all firewalls in your organization.



Note

If a network credential is not required for a specific device, then the parameter can be left blank in **Configuration Source Management**.

Configuring Credentials

You configure network devices to provide Risk Manager with access to the devices.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 3 On the **Risk Manager** pane, click **Configuration Source Management**.
- 4 On the navigation menu, click **Credentials**.
- 5 On the **Network Groups** pane, click **Add a new network group**.
- 6 Type a name for the network group, and click **OK**.
- 7 On the **Add address** field, type the IP address of your device and click **Add**. Repeat this step for each address that you must add.



Note

Ensure that the addresses that you add display in the Network address section beside the **Add address** box. Do not replicate device addresses that already exist in other network groups in **Configuration Source Management**.

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

- 8 On the **Credentials** pane, click **Add a new credential set**.
- 9 Type a name for the new credential set, and click **OK**.
- 10 Select the name of the credential set that you created, and then configure values for the following parameters:

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

- 11 Click **OK**.

Discovering Devices

The discovery process adds network devices to the topology interface by using the credentials that you added.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 3 In the **Risk Manager** section, click **Configuration Source Management**.
- 4 On the navigation menu, click **Discover Devices**.
- 5 Type an IP address or CIDR range to specify the location of devices that you want to discover.
- 6 Click the **Add (+)** icon.
- 7 If you want to search for devices in the network from the defined IP address or CIDR range, select the **Crawl the network from the addresses defined above** box.
- 8 Click **Run**.

Obtaining Device Configuration

You back up your devices to download the device configuration so Risk Manager can include the device information in the topology.

You must **configure credentials** sets before you can download device configurations.

You can back up a single device or all devices.

For information about scheduling automated backups of device configurations from the **Jobs** tab, see the *Risk Manager User Guide*.

- 1 Click the **Admin** tab.
- 2 On the navigation menu, click **Plug-ins**.
- 3 On 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. Click **Yes** to continue.
- 6 To obtain the configuration for specific devices, select the individual device. To select multiple devices to back up, hold down the Ctrl key. Click **Backup**.

Import Devices

Use Device Import to add a list of adapters and their network IP addresses to the Configuration Source Manager using a comma-separated value file (.CSV).

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

For example,

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


Where:

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

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

Table 4: 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

You can import a master device list to Configuration Source Management using a comma-separated value (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.

Troubleshoot Device Import

If you receive an error message after you try to import your device, it might be because the import of the CSV file failed.

Importing a device can fail if the device list is structured incorrectly. For example, the CSV file might be missing colons or a command, or multiple devices might be on a single line.

Alternatively, the import might fail if the device list contains incorrect information. For example, a typographical error for an adapter name.

If the device import aborts, then no devices from the CSV file are added to Configuration Source Management. A list of valid adapter names for your installed adapters is displayed in the message. If an error is displayed, then you must review your CSV file to correct any errors. You can re-import the file after the errors are fixed.

4 Manage Audits

Use Case: Configuration Audit

Use Case: View Network Paths in the Topology

Use case: Visualize the Attack Path of an Offense

Risk Manager helps to simplify the assessment of network security policies and compliance requirements by helping you answer questions.

Compliance auditing is a necessary and complex task for security administrators. Risk Manager helps you answer the following questions:

- How are my network devices configured?
- How are my network resources communicating?
- Where is my network vulnerable?

Use Case: Configuration Audit

You can use the configuration information for network devices, which is captured by Risk Manager, for audit compliance and to schedule configuration backups.

Configuration backups provide a centralized and automatic method of recording device changes for your audit compliance. Configuration backups archive configuration changes and provide a historical reference; you can capture a historical record or compare a configuration against another network device.

Configuration auditing in Risk Manager provides you with the following options:

- A historical record of your network device configurations.
- A normalized view, which displays device changes when you compare configurations.
- A tool to search for rules on your device.

The configuration information for your devices is collected from device backups in Configuration Source Management. Each time Risk Manager backs up your device list, it archives a copy of your device configuration to provide a historical reference. The more often you schedule Configuration Source Management, the more configuration records you have for comparison and for historical reference.

Viewing Device Configuration History

You can view the configuration history of a network device.

You can view history information for network devices that were backed up. This information is accessible from the **History** pane on the **Configuration Monitor** page. The history pane provides information about a network device configuration and the date that the device configuration was last backed up using Configuration Source Management.

The configuration displays the type of files that are stored for your network device in Risk Manager. The common configuration types are:

- **Standard-Element-Document (SED)**, which are XML data files that contain information about your network device. Individual SED files are viewed in their raw XML format. If an SED is compared to another SED file, then the view is normalized to display the rule differences.
- **Config**, which are configuration files that are provided by certain network devices. These files depend on the device manufacturer. A configuration file can be viewed by double-clicking the configuration file.



Note

Depending on your device, several other configuration files might be displayed. Double-clicking these files displays the contents in plain text. The plain text view supports the find (Ctrl+f), paste (Ctrl+v), and copy (Ctrl+C) functions from the web browser window.

- 1 Click the **Risks** tab.
- 2 On the navigation menu, click **Configuration Monitor**.
- 3 Double-click a configuration to view the detailed device information.
- 4 Click **History**.
- 5 On the **History** pane, select a configuration.
- 6 Click **View Selected**.

Comparing Device Configurations for a Single Device

You can compare device configurations for a single device.

If the files that you compare are Standard-Element-Documents (SEDs), then you can view the rule differences between the configuration files.

When you compare normalized configurations, the color of the text indicates the following rules:

- Green dotted outline indicates a rule or configuration that was added to the device.
- Red dashed outline indicates a rule or configuration that was deleted from the device.
- Yellow solid outline indicates a rule or configuration that was modified on the device.

- 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 Select a primary configuration.
- 6 Press the Ctrl key and select a second configuration for comparison.
- 7 On the **History** pane, click **Compare Selected**.
- 8 Optional. To view the raw configuration differences, click **View Raw Comparison**.

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

Comparing Device Configurations for Different Devices

You can compare two configurations for different devices.

If the files that you compare are Standard-Element-Documents (SEDs), then you can view the rule differences between the configuration files.

When you compare normalized configurations, the color of the text indicates the following rules:

- Green dotted outline indicates a rule or configuration that was added to the device.
- Red dashed outline indicates a rule or configuration that was deleted from the device.
- Yellow solid outline indicates a rule or configuration that was modified on the device.

- 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 Select a primary configuration.
- 6 Click **Mark for Comparison**.
- 7 From the navigation menu, select **All Devices** to return to the device list.
- 8 Double-click the device to compare and click **History**.
- 9 Select another configuration backup to compare with the marked configuration.
- 10 Click **Compare with Marked**.
- 11 Optional. To view the raw configuration differences, click **View Raw Comparison**.

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

Use Case: View Network Paths in the Topology

The topology in Risk Manager displays a graphical representation of your network 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 visibly display the path between a source and destination, along with the ports, protocols, and rules.

You can view how devices communicate, which is important on secured or restricted access assets.

Key features include:

- Ability to view communications between devices on your network.
- Use filters to search the topology for network devices.
- Quick access to view device rules and configuration.
- Ability to view events that are generated from a path search.

Searching the Topology

You can view device communication by searching the topology.

A path search is used to filter the topology model. A path search includes all network subnets containing the source IP addresses or CIDR ranges and subnets containing destination IP addresses or

CIDR ranges that are also allowed to communicate using the configured protocol and port. The search examines your existing topology model and includes the devices that are involved in the communication path between the source and destination and detailed connection information.

You can use vulnerabilities to filter the search if your topology includes an Intrusion Prevention System (IPS). For more information, see the *Risk Manager User Guide*.

- 1 Click the **Risks** tab.
- 2 On the navigation menu, click **Topology**.
- 3 From the **Search** list box, select **New Search**.
- 4 In the **Search Criteria** pane, select **Path**.
- 5 In the **Source IP/CIDR** field, type the IP address or CIDR range on which you want to filter the topology model. Separate multiple entries by using a comma.
- 6 In the **Destination IP/CIDR** field, type the destination IP address or CIDR range on which you want to filter the topology model. Separate multiple entries by using a comma.
- 7 Optional. From the **Protocol** list, select the protocol that you want to use to filter the topology model.
- 8 Optional. In the **Destination Port** field, type the destination port on which you want to filter the topology model. Separate multiple ports by using a comma.
- 9 Click **OK**.
- 10 Move your mouse over a connection line to view details about the connection.

If the search connects to a device that contains rules, a device rules link is displayed in the dialog.

Use case: Visualize the Attack Path of an Offense

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

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 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

You can view the attack path of an offense. The attack path shows the source, destination, and associated devices.

- 1 Click the **Offenses** tab.

- 2 On the navigation menu, click **All Offenses**.

The **All Offenses** page displays a list of offenses that are on your network. Offenses are listed with the highest magnitude first.

- 3 Double-click an offense to open the offense summary.
- 4 On the **Offenses** toolbar, click **View Attack Path**.

5 Use Case: Monitor Policies

Use Case: Assess Assets That Have Suspicious Configurations

Use Case: Assess Assets with Suspicious Communication

Use Case: Monitor Policies for Violations

Use Case: Use Vulnerabilities to Prioritize Risks

Use Case: Prioritize Asset Vulnerabilities by Zone or Network Communications

Policy auditing and change control are fundamental processes that allow administrators and security professionals to control access and communications between critical business assets.

The criteria for policy monitoring can include monitoring of assets and communications for the following scenarios:

- Does my network contain assets with risky configurations for PCI Section 1 audits?
- Do my assets allow communications using risky protocols for PCI Section 10 audits?
- How do I know when a policy change puts my network in violation?
- How do I view vulnerabilities for hardened or high risk assets?
- How do I view assets in the network with vulnerabilities and Internet access?

Use Policy Monitor to define tests that are based on the risk indicators, and then restrict the test results to filter the query for specific results, violations, protocols, or vulnerabilities.

Risk Manager includes several Policy Monitor questions that are grouped by PCI category. For example, PCI 1, PCI 6, and PCI 10 questions. Questions can be created for assets or devices and rules to expose network security risk. After a question about an asset or a device/rule is submitted to Policy Monitor, the returned results specify the level of risk. You can approve results that are returned from assets or define how you want the system to respond to unapproved results.

Policy Monitor provides the following key features:

- Predefined Policy Monitor questions to assist with workflow.
- Determines if users used forbidden protocols to communicate.
- Assessing if users on specific networks can communicate to forbidden networks or assets.
- Assessing if firewall rules meet corporate policy.
- Continuous monitoring of policies that generate offenses or alerts to administrators.
- Prioritizing vulnerabilities by assessing which systems can be compromised as a result of device configuration.
- Help identifying compliance issues.

Use Case: Assess Assets That Have Suspicious Configurations

Organizations use corporate security policies to define risks and the communications that are allowed between assets and networks. To assist with compliance and corporate policy breaches, organizations use Policy Monitor to assess and monitor risks that might be unknown.

PCI compliance dictates that you identify devices that contain cardholder data, then diagram, verify communications, and monitor firewall configurations to protect assets that contain sensitive data. Policy Monitor provides methods for quickly meeting these requirements and allows administrators to adhere to corporate policies. Common methods of reducing risk include identifying and monitoring assets that communicate with unsecured protocols. These are protocols such as routers, firewalls, or switches that allow FTP or telnet connections. Use Policy Monitor to identify assets in your topology with risky configurations.

PCI section 1 questions might include the following criteria:

- Assets that allow banned protocols.
- Assets that allow risky protocols.
- Assets that allow out-of-policy applications across the network.
- Assets that allow out-of-policy applications to networks that contain protected assets.

Assessing Devices That Allow Risky Protocols

Use Policy Monitor to assess devices that allow risky protocols.

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 offenses for the behavior.

- 1 Click the **Risks** tab.
- 2 On the navigation menu, click **Policy Monitor**.
- 3 From the Group list box, 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**.

Use Case: Assess Assets with Suspicious Communication

Use Policy Monitor to identify PCI section 10 compliance by tracking, logging, and displaying access to network assets.

Risk Manager can help to identify PCI section 10 compliance by identifying assets in the topology that allow questionable or risky communications. Risk Manager can examine these assets for actual communications or possible communications. Actual communications display assets that used your question criteria to communicate. Possible communications display assets that can use your question criteria to communicate.

PCI section 10 questions can include the following criteria:

- Assets that allow incoming questions to internal networks.
- Assets that communicate from untrusted locations to trusted locations.
- Assets that communicate from a VPN to trusted locations.
- Assets that allow unencrypted out-of-policy protocols within a trusted location.

Finding Assets That Allow Communication

You can find assets that allow communication from the Internet.

Risk Manager evaluates the question and displays the results of any internal assets that allow inbound connections from the Internet. Security professionals, administrators, or auditors in your network can approve communications to assets that are not considered secure or containing customer data. As more events are generated, you can create offenses in SIEM to monitor this type of risky communication.

- 1 Click the **Risks** tab.
- 2 On the navigation menu, click **Policy Monitor**.
- 3 From the Group list box, 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**.

Use Case: Monitor Policies for Violations

Risk Manager can continuously monitor any predefined or user-generated question in Policy Monitor. You can use monitor mode to generate events in Risk Manager.

When you select a question to be monitored, 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 SIEM.

Configuring a Question

You can use Policy Monitor to configure a question to be monitored.

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

- 5 Configure any of the options that you require to monitor your question.
- 6 Click **Save Monitor**.

Monitoring is enabled for the question and events or offenses are generated based on your monitoring criteria.

Use Case: Use Vulnerabilities to Prioritize Risks

Exposed vulnerabilities are a significant risk factor for network assets.

Risk Manager leverages asset information and vulnerability information in Policy Monitor. This information is used to determine if your assets are susceptible to input type attacks, such as; SQL injection, hidden fields, and clickjacking.

Vulnerabilities that are detected on your assets can be prioritized by their network location or a connection to another device that is vulnerable.

Vulnerability asset questions can include the following criteria:

- Assets with new vulnerabilities reported after a specific date.
- Assets with specific vulnerabilities or CVSS score.
- Assets with a specific classification of vulnerability, such as input manipulation, denial of service, OSVDB verified.

Finding Assets That Have Vulnerabilities

You can find assets that have vulnerabilities.

Risk Manager evaluates a question and displays the results of assets that contain your vulnerability. Security professionals, administrators, or auditors can identify assets in your network that contain known SQL injection vulnerabilities. They can promptly patch any assets that are connected to a protected network. As more events are generated, you can create events or offenses in SIEM to monitor assets that contain SQL injection vulnerabilities.

- 1 Click the **Risks** tab.
- 2 On the navigation menu, click **Policy Monitor**.
- 3 From the **Group** list, select **Vulnerability**.
- 4 Select the test question **Assess assets with SQL injection vulnerabilities on specific localnet(s) (that is, protected server network)**.
- 5 Click **Submit Question**.

Use Case: Prioritize Asset Vulnerabilities by Zone or Network Communications

Systems with vulnerabilities in the same network as protected assets are at a greater risk of data loss.

Detecting vulnerabilities on assets by zone or network are key measures to prevent exploits before they occur in your network. PCI section 6.1 and 6.2 stipulate that you review and patch systems within one month of a vulnerability patch release. Risk Manager assists with automating and prioritizing the

patch process. As vulnerabilities are detected on your assets, you can prioritize by the network location or a connection to another device that is vulnerable. Prioritizing is important for secured networks that can be connected to suspicious regions, or assets that contain a CVSS score greater than your internal policy allows.

Vulnerable asset questions can include the following criteria:

- Assets with a client side vulnerability, which communicated with suspicious geographic regions and contain protected assets.
- Assets with denial of service vulnerabilities in a specific network.
- Assets with mail vulnerabilities in a specific network.
- Assets with vulnerabilities and the specific Common Vulnerability Scoring System (CVSS) score.

Finding Assets That Have Vulnerabilities in a Network

You can find assets that have vulnerabilities in a specific network.

Risk Manager evaluates the question and displays the results in the specific location that contains OS-specific vulnerabilities. Security professionals, administrators, or auditors of your network can approve communications to assets that are not considered secure or containing customer data. As more events are generated, you can create offenses to monitor this type of risky communication.

- 1 Click the **Risks** tab.
- 2 On the navigation menu, click **Policy Monitor**.
- 3 From the **Group** list box, select **Vulnerability**.
- 4 Select the test question **Assess assets with OS specific vulnerabilities on a specific localnet(s)**.
- 5 Click **Submit Question**.

6 Use Cases for Simulations

Use Case: Simulate Attacks on Network Assets

Use Case: Simulate the Risk of Network Configuration Changes

Use Case: Simulate Attacks on Network Assets

You can use a simulation to test your network for vulnerabilities from various sources.

You can use attack simulations to audit device configurations in your network.

Simulations provide the following key features:

- Simulations display the theoretical path permutations an attack can take against your network.
- Simulations display how attacks can propagate through your network devices to spread to other assets.
- Simulations allow monitoring to detect new exposure sites.

Creating a Simulation

You can create a simulation for an network attack on an SSH protocol.

- 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 **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 **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 containing SSH vulnerabilities is displayed in the results, allowing 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 and the connections that the attack could take in your network. 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 provided in the attack allows you to strengthen and test your network against thousands of possible attack scenarios.

Use Case: Simulate the Risk of Network Configuration Changes

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

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:

- 1 [Create a topology model.](#)
- 2 [Simulate an attack against the topology model.](#)

Creating a Topology Model

You can create a topology model to test network changes and simulate attacks.

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

You can simulate an attack on ports and protocols.

- 1 Click the **Risks** tab.

- 2 On the navigation menu, select **Simulation > Simulations**.
- 3 From the **Actions** list box, 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 **OK**.
- 11 Click **Save Simulation**.
- 12 From the **Actions** list, select **Run Simulation**.
The results column contains a list box with the date the simulation was run and a link to view the results.
- 13 Click **View Results**.