Extreme Networks Security Risk Manager Installation Guide

9034865

Published May 2015

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

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	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 italicized type	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 Introduction to installing Extreme Networks Security Risk Manager

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

This guide contains instructions for installing Risk Manager and adding Risk Manager as a managed host on Extreme SIEM console.

Risk Manager appliances are preinstalled with software and a Red Hat Enterprise Linux™ operating system. You can also install Risk Manager software on your own hardware.

Intended audience

This guide is intended for network administrators that are responsible for installing and configuring Risk Manager systems in your network.

Administrators need a working knowledge of networking and Linux systems.

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 lawful 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.

Note

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. Extreme Networks Security Analytics may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of Extreme Networks Security Analytics.

2 Prepare to Install Risk Manager

You can install an Risk Manager appliance as a managed host on your SIEM console. Only one Risk Manager can exist on a SIEM Console.

As of version 7.1 of Risk Manager, SIEM Console and Risk Manager use the same installation process and ISO for installation. For this reason, you can use the deployment editor in SIEM console to add Risk Manager to your deployment. A Risk Manager appliance installation includes the Risk Manager software and a Red Hat Enterprise Linux™ operating system.

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.

For information about installing SIEM, including hardware and software requirements, see *SIEM Installation Guide*.

Since Risk Manager is a 64-bit appliance, make sure that you download the correct installation software for your operating system.

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

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)

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

Additional Hardware Requirements

Additional hardware is required before you can install Risk Manager.

Before you install Risk Manager systems, you need access to the following hardware components:

- monitor and keyboard or a serial console
- Uninterrupted Power Supply (UPS)

Risk Manager appliances or systems that are running Risk Manager software that store data must be equipped with an Uninterrupted Power Supply (UPS). Using a UPS ensures that your Risk Manager data, such as consoles, event processors, and Behavioral Flow Collectors, is preserved during a power failure.

Additional Software Requirements

Additional software is required before you can install Risk Manager.

The following software must be installed on the desktop system that you use to access the Risk Manager user interface:

- Java™ runtime environment
- Adobe™ Flash, version 10 or higher

3 Install Risk Manager Appliances

An Risk Manager deployment includes a SIEM Console and Risk Manager appliance as a managed host.

Installing Risk Manager involves the following steps:

1. Preparing your appliance.
2. Installing Risk Manager.
3. Adding Risk Manager to SIEM.

Preparing Your Appliance

You must prepare your appliance before you install an Risk Manager appliance.

You must install all necessary hardware and you need an activation key. The activation key is a 24-digit, four-part, alphanumeric string that you receive from IBM®. You can find the activation key:

- Printed on a sticker and physically placed on your appliance.
- Included with the packing slip; all appliances are listed along with their associated keys.

To avoid typing errors, the letter I and the number 1 (one) are treated the same, as are the letter O and the number 0 (zero).

If you do not have an activation key for your Risk Manager appliance, contact Customer Support (www.extremenetworks.com/support/).

For information about your appliance, see the *Hardware Installation Guide*.

1. Choose one of the following options:
    - Connect a notebook to the serial port on the rear of the appliance.

      If you use a notebook to connect to the system, you must use a terminal program, such as HyperTerminal, to connect to the system. Make sure that you set Connect Using to the appropriate COM port of the serial connector and Bits per second to 9600. You must also set Stop Bits (1), Data bits (8), and Parity (None).
    - Connect a keyboard and monitor to their respective ports.
2. Power on the system and login. The username, which is case-sensitive, is root.
3. Press Enter.
4. Read the information in the window. Press the Spacebar to advance each window until you reach the end of the document.
5. Type `yes` to accept the agreement, and then press Enter.
6. Type your activation key and press Enter.

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 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.

Network Parameter Information for IPv4

Network information for Internet Protocol version 4 (IPv4) network settings is required when you install Risk Manager or when you change network settings.

Network information is required when you install or reinstall Risk Manager, or when you need to change network settings.

The Public IP network setting is optional. This secondary IP address is used to access the server, usually from a different network or the Internet, and is managed by your network administrator. The Public IP address is often configured using the Network Address Translation (NAT) services on your network or firewall settings on your network. NAT translates an IP address in one network to a different IP address in another network.

Installing Risk Manager

You can install Risk Manager after you prepare your appliance.

You must complete the preparation steps before you install Risk Manager.

1. Select normal for the type of setup. Select **Next** and press Enter.
2. Select your time zone continent or area. Select **Next** and press Enter.
3. Select your time zone region. Select **Next** and press Enter.
4. Select an Internet Protocol version. Select **Next** and press Enter.
5. Select the interface that you want to specify as the management interface. Select **Next** and press Enter.
6. Type your hostname, IP address, network mask, gateway, primary DNS, secondary DNS, public IP, and email server.

   For network parameter information, see Network Parameter Information for IPv4 on page 12.
7. Select **Next** and press Enter.
8. Type a password to configure the Risk Manager root password.
9. Select **Next** and press Enter.
10. Retype your new password to confirm. Select **Finish** and press Enter.

    This process typically takes several minutes.

Use the deployment editor to add Risk Manager as a managed host to your SIEM Console.

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 7.7.1 or Risk Manager 7.7.1.

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 *Extreme Networks SIEM Administration Guide*.
Enable Encryption	Creates an SSH encryption tunnel for the host. To enable encryption between two managed hosts, each managed host must be running SIEM console 7.7.1 or Risk Manager 7.7.1.
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 SIEM 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 SIEM Console. The Risks tab is now available.

Clearing Web Browser Cache

You must clear the web browser cache before you can access the Risks tab in SIEM Console.

Ensure that only one web browser is open. If you have multiple browsers open, the cache can fail to clear properly.

If you are using a Mozilla Firefox web browser, you must clear the cache in your Microsoft™ Internet Explorer web browser too.

1 Open your web browser.
2 Clear your web browser cache. For instructions, see your web browser documentation.

Risk Manager User Role

You must assign the Risk Manager user role for users that require access to the Risks tab.

A user account defines the default password, and email address for a user. You need to assign a user role and security profile for each new user account.

Before you can allow access to Risk Manager functionality to other users in your organization, you must assign the appropriate user role permissions. By default, SIEM Console provides a default administrative role, which provides access to all areas of Risk Manager.

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

Assigning the Risk Manager User Role

You can assign the Risk Manager user role to users that need access to the Risk tab.

1 Click the Admin tab.
2 On the navigation menu, click System Configuration.
3 In the User Management pane, click the User Roles icon.
4 Click the Edit icon next to the user role you want to edit.
5 Select the Risk Manager check box.
6 Click Next.

If you add Risk Manager to a user role that has Log Activity permission, then you must define the log sources that the user role can access. You can add an entire log source group by clicking the Add icon in the Log Source Group pane. You can select multiple log sources by holding the Control key while you select each log source you want to add.

7 Click Return.
8 From the Admin tab menu, click Deploy Changes.

Troubleshoot the Risks Tab

You can troubleshoot if the Risks tab does not display properly or is inaccessible.

When the Risks tab is not displaying properly or is inaccessible, you remove and read Risk Manager as a managed host.

Removing a Managed Host

You can remove your Risk Manager managed host from SIEM console to change network settings or if there is a problem with the Risks tab.

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.

   For default login information, see Table 3: Default login information for Risk Manager on page 12.

4 On the Admin tab, click Deployment Editor.

5 Click the System View tab.

6 Right-click the managed host that you want to delete and select Delete. Repeat for each non-Console managed host until all hosts are deleted.

7 Click Save.

8 Close the deployment editor.

9 On the Admin tab, click Deploy Changes.

Reading Risk Manager as a Managed Host

You can read Risk Manager as a managed host after it is removed.

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.

   For default login information, see Table 3: Default login information for Risk Manager on page 12.

4 On the Admin tab, click Deployment Editor.

5 Click the System View tab.

6 From the menu, select Actions > Add a managed host.

7 Click Next.

8 Enter values in the Add new managed host window.

9 Click Next.

10 Click Finish.

   The process of adding Risk Manager can take several minutes to complete.

11 Close the deployment editor.

12 On the Admin tab, click Deploy Changes.

4 USB Flash Drive Installations

You can install Extreme Networks Security Analytics software with a USB flash drive.

USB flash drive installations are full product installations. You cannot use a USB flash drive to upgrade or apply product patches. For information about applying fix packs, see the fix pack Release Notes.

Supported Versions

The following appliances or operating systems can be used to create a bootable USB flash drive:

- A Extreme Security v7.2.1 appliance or later
- A Linux™ system that is installed with Red Hat Enterprise Linux™ 6.4
- Microsoft™ Windows™ Vista
- Microsoft™ Windows™ 7
- Microsoft™ Windows™ 2008
- Microsoft™ Windows™ 2008R2

Installation Overview

Follow this procedure to install Extreme Security software from a USB flash drive:

1. Create the bootable USB flash drive.
2. Install the software for your Extreme Security appliance.
3. Install any product maintenance releases or fix packs.

   See the Release Notes for installation instructions for fix packs and maintenance releases.

Creating a Bootable USB Flash Drive with a Extreme Security Appliance

You can use an Extreme Networks Security Analytics V7.7.2.1 or later appliance to create a bootable USB flash drive that can be used to install Extreme Security software.

Before you can create a bootable USB flash drive from a Extreme Security appliance, you must have access to the following items:

- A 2 GB USB flash drive

- A Extreme Security V7.7.2.1 or later ISO image file
- A physical Extreme Security appliance

If your Extreme Security appliance does not have Internet connectivity, you can download the Extreme Security ISO image file to a desktop computer or another Extreme Security appliance with Internet access. You can then copy the ISO file to the Extreme Security appliance where you install the software.

When you create a bootable USB flash drive, the contents of the flash drive are deleted.

1 Download the Extreme Security ISO image file.

   a Access the Extreme Networks Support Portal.

   b Locate the Extreme Networks Security Analytics ISO file that matches the version of the Extreme Security appliance.

   c Copy the ISO image file to a `/tmp` directory on your Extreme Security appliance.

2 Using SSH, log in to your Extreme Security system as the root user.

3 Insert the USB flash drive in the USB port on your Extreme Security system.

   It might take up to 30 seconds for the system to recognize the USB flash drive.

4 Type the following command to mount the ISO image:

```
mount -o loop /tmp/<name of the ISO image>.iso /media/cdrom
```

5 Type the following commend to copy the USB creation script from the mounted ISO to the `/tmp` directory.

```
cp /media/cdrom/post/create-usb-key.py /tmp/
```

6 Type the following command to start the USB creation script:

```
/tmp/create-usb-key.py
```

7 Press `Enter`.

8 Press `1` and type the path to the ISO file.

   For example,

```
/tmp/<name of the iso image>.iso
```

9 Press **2** and select the drive that contains your USB flash drive.

10 Press **3** to create your USB key.

   The process of writing the ISO image to your USB flash drive takes several minutes to complete. When the ISO is loaded onto the USB flash drive, a confirmation message is displayed.

11 Press `q` to quit the USB key script.

12 Remove the USB flash drive from your Extreme Security system.

13 To free up space, remove the ISO image file from the `/tmp` file system.

If your connection to the appliance is a serial connection, see Configuring a flash drive for serial only appliances.

If your connection to the appliance is keyboard and mouse (VGA), see Installing SIEM with a USB flash drive.

Creating a Bootable USB Flash Drive with Microsoft™ Windows™

You can use a Microsoft™ Windows™ desktop or notebook system to create a bootable USB flash drive that can be used to install Extreme Security software.

Before you can create a bootable USB flash drive with a Microsoft™ Windows™ system, you must have access to the following items:

- A 2 GB USB flash drive
- A desktop or notebook system with one the following operating systems:
    - Windows™ 7
    - Windows™ Vista
    - Windows™ 2008
    - Windows™ 2008R2

You must download the following files from the Extreme Networks Support Portal.

- Extreme Security V7.7.2.1 or later Red Hat 64-bit ISO image file
- Create-USB-Install-Key (CUIK) tool.

You must download the following files from the Internet.

- PeaZip Portable 4.8.1
- SYSLINUX 4.06

Tip
Search the web for **`Peazip Portal v4.8.1`** and **`Syslinux`** to find the download files.

When you create a bootable USB flash drive, the contents of the flash drive are deleted.

1. Extract the Create-USB-Install-Key (CUIK) tool to the `c:\cuik` directory.
2. Copy the `.zip` files for PeaZip Portable 4.8.1 and SYSLINUX 4.06 to the `cuik\deps` folder.

   For example, `c:\cuik\deps\peazip_portable-4.8.1.WINDOWS.zip` and `c:\cuik\deps\syslinux-4.06.zip`.

   You do not need to extract the `.zip` files. The files need only to be available in the `cuik/deps` directory.
3. Insert the USB flash drive into the USB port on your computer.
4. Verify that the USB flash drive is listed by drive letter and that it is accessible in Microsoft™ Windows™.
5. Right-click on `c:\cuik\cuik.exe`, select Run as administrator, and press Enter.
6. Press **1**, select the Extreme Security ISO file, and click Open.
7. Press **2** and select the number that corresponds to the drive letter assigned to your USB flash drive.
8. Press **3** to create the USB flash drive.
9. Press Enter to confirm that you are aware that the contents of the USB flash drive will be deleted.
10. Type **`create`** to create a bootable USB flash drive from the ISO image.

    This process takes several minutes.
11. Press Enter, and then type **q** to exit the Create_USB_Install_Key tool.
12. Safely eject the USB flash drive from your computer.

If your connection to the appliance is a serial connection, see Configuring a flash drive for serial only appliances.

If your connection to the appliance is keyboard and mouse (VGA), see Installing SIEM with a USB flash drive.

Creating a Bootable USB Flash Drive with Red Hat Linux™

You can use a Linux™ desktop or notebook system with Red Hat v6.3 to create a bootable USB flash drive that can be used to install Extreme Networks Security Analytics software.

Before you can create a bootable USB flash drive with a Linux™ system, you must have access to the following items:

- A 2 GB USB flash drive
- A Extreme Security V7.7.2.1 or later ISO image file
- A Linux™ system that has the following software installed:
  - Red Hat 6.4
  - Python 6.2 or later

When you create a bootable USB flash drive, the contents of the flash drive are deleted.

1 Download the Extreme Security ISO image file.

   a Access the Extreme Networks Support Portal.

   b Locate the Extreme Networks Security Analytics ISO file.

   c Copy the ISO image file to a `/tmp` directory on your Extreme Security appliance.

2 Update your Linux- based system to include these packages.

   - syslinux
   - mtools
   - dosfstools
   - parted

   For information about the specific package manager for your Linux™ system, see the vendor documentation.

3 Log in to your Extreme Security system as the root user.

4 Insert the USB flash drive in the front USB port on your system.

   It might take up to 30 seconds for the system to recognize the USB flash drive.

5 Type the following command to mount the ISO image:

```
mount -o loop /tmp/<name of the ISO image>.iso /media/cdrom
```

6 Type the following command to copy the USB creation script from the mounted ISO to the `/tmp` directory.

```
cp /media/cdrom/post/create-usb-key.py /tmp/
```

7 Type the following command to start the USB creation script:

```
/tmp/create-usb-key.py
```

8 Press `Enter`.

9 Press **1** and type the path to the ISO file.

For example,

```
/tmp/Rhe664QRadar7_2_4_<build>.iso
```

10 Press **2** and select the drive that contains your USB flash drive.

11 Press **3** to create your USB key.

The process of writing the ISO image to your USB flash drive takes several minutes to complete. When the ISO is loaded onto the USB flash drive, a confirmation message is displayed.

12 Press **q** to quit the USB key script.

13 Remove the USB flash drive from your system.

If your connection to the appliance is a serial connection, see Configuring a flash drive for serial only appliances.

If your connection to the appliance is keyboard and mouse (VGA), see Installing SIEM with a USB flash drive.

Configuring a USB Flash Drive for Serial-only Appliances

You must complete an extra configuration step before you can use the bootable USB flash drive to install Extreme Security software on serial-only appliances.

This procedure is not required if you have a keyboard and mouse that is connected to your appliance.

1 Insert the bootable USB flash drive into the USB port of your appliance.

2 On your USB flash drive, locate the `syslinux.cfg` file.

3 Edit the syslinux configuration file to change the default installation from `default linux` to `default serial`.

4 Save the changes to the syslinux configuration file.

You are now ready to install Extreme Security with the USB flash drive.

Installing Extreme Security with a USB Flash Drive

Follow this procedure to install Extreme Security from a bootable USB flash drive.

You must create the bootable USB flash drive before you can use it to install Extreme Security software.

This procedure provides general guidance on how to use a bootable USB flash drive to install Extreme Security software.

The complete installation process is documented in the product Installation Guide.

1 Install all necessary hardware.

2 Choose one of the following options:

- Connect a notebook to the serial port at the back of the appliance.
- Connect a keyboard and monitor to their respective ports.

3 Insert the bootable USB flash drive into the USB port of your appliance.

4 Restart the appliance.

   Most appliances can boot from a USB flash drive by default. If you are installing Extreme Security software on your own hardware, you might have to set the device boot order to prioritize USB.

   After the appliance starts, the USB flash drive prepares the appliance for installation. This process can take up to an hour to complete.

5 When the Red Hat Enterprise Linux menu is displayed, select one of the following options:

   - If you connected a keyboard and monitor, select Install or upgrade using VGA console.
   - If you connected a notebook with a serial connection, select Install or upgrade using Serial console.

6 Type `SETUP` to begin the installation.

7 When the login prompt is displayed, type `root` to log in to the system as the root user.

   The user name is case-sensitive.

8 Press Enter and follow the prompts to install Extreme Security.

   The complete installation process is documented in the product Installation Guide.

5 Reinstall Extreme Networks Security Risk Manager from the Recovery Partition

Reinstalling Risk Manager by Using Factory Re-install

When you reinstall Risk Manager from the SIEM Console ISO on the recovery partition, your system is restored back to factory default configuration. This means that your current configuration and data files are overwritten.

This information applies to new Risk Manager installations or upgrades from new Risk Manager installations on Risk Manager appliances. When you install Risk Manager, the installer (SIEM Console ISO) is copied into the recovery partition. From this partition, you can reinstall Risk Manager, which restores Risk Manager to factory defaults.

Note
If you upgrade your software after you install Risk Manager, then the ISO file is replaced with the newer version.

When you reboot your Risk Manager appliance, you are presented with the option to reinstall the software. Since SIEM Console and Risk Manager use the same ISO installation file, the SIEM Console ISO name displays.

If you do not respond to the prompt after 5 seconds, the system reboots as normal, which maintains your configuration and data files. If you choose to reinstall SIEM Console ISO, a warning message is displayed and you must confirm that you want to reinstall the software. After confirmation, the installer runs and you can follow the prompts through the installation process.

After a hard disk failure, you cannot reinstall from the recovery partition because it is no longer available. If you experience a hard disk failure, contact customer support for assistance.

Reinstalling Risk Manager by Using Factory Re-install

You can reboot and reinstall your Risk Manager appliance using the factory reinstall option.

Ensure that you have your activation key, which is a 24-digit, four-part, alphanumeric string that you receive from Extreme Networks. You can find the key:

- Printed on a sticker and physically placed on your appliance.
- Included with the packing slip; appliances are listed along with their associated keys.

To avoid typing errors, the letter I and the number 1 (one) are treated the same, as are the letter O and the number 0 (zero).

If you do not have an activation key for your Risk Manager appliance, contact Customer Support (www.extremenetworks.com/support/).

Software activation keys do not require serial numbers.

1 Reboot your Risk Manager appliance.
2 Select Factory re-install.
3 Type `flatten` to continue.

   The hard disk is partitioned and reformatted, the OS is installed, and then Risk Manager is reinstalled. You must wait for the flatten process to complete. This process can take up to several minutes, depending on your system.
4 Type SETUP.
5 Log in to Risk Manager as the root user.
6 Read the information in the window. Press the Spacebar to advance each window until you reach the end of the document. Type `yes` to accept the agreement, and then press Enter.
7 Type your activation key and press Enter.
8 Select normal for the type of setup. Select Next and press Enter.
9 Select your time zone continent or area. Select Next and press Enter.
10 Select your time zone region. Select Next and press Enter.
11 Select an Internet Protocol version. Select Next and press Enter.
12 Select the interface that you want to specify as the management interface. Select Next and press Enter.
13 Enter information for your hostname, IP address, network mask, gateway, primary DNS, secondary DNS, public IP, and email server.

   For network information, see Network Parameter Information for IPv4 on page 12.
14 Type your password to configure the Risk Manager root password.
15 Select Next and press Enter.
16 Retype your new password to confirm. Select Finish and press Enter.

   This process typically takes several minutes.
17 Press Enter to select OK.
18 Press Enter to select OK.

Use the deployment editor to add Risk Manager as a managed host to your SIEM Console.

6 Change Network Settings

You can change the network settings of an Risk Manager appliance that is attached to an SIEM console.

If you need to change the network settings, then you must complete these tasks in the following order:

1 Remove Risk Manager as a managed host.
2 Change network settings.
3 Read Risk Manager as a managed host.

Removing a Managed Host

You can remove your Risk Manager managed host from SIEM console to change network settings or if there is a problem with the **Risks** tab.

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.

For default login information, see Table 3: Default login information for Risk Manager on page 12.

4 On the **Admin** tab, click **Deployment Editor**.
5 Click the **System View** tab.
6 Right-click the managed host that you want to delete and select **Delete**. Repeat for each non-Console managed host until all hosts are deleted.
7 Click **Save**.
8 Close the deployment editor.
9 On the **Admin** tab, click **Deploy Changes**.

Changing Network Settings

You can change the network settings of an Risk Manager appliance that is attached to an SIEM console.

You must remove the Risk Manager managed host from SIEM Console before you change the network settings.

1 Using SSH, log in to Risk Manager as the root user.
2 Type the command, `qchange_netsetup`.
3 Select an Internet Protocol version. Select **Next** and press Enter. Depending on your hardware configuration, the window displays up to a maximum of four interfaces. Each interface with a physical link is denoted with a plus (+) symbol.

4 Select the interface that you want to specify as the management interface. Select **Next** and press Enter.

5 Enter information for your hostname, IP address, network mask, gateway, primary DNS, secondary DNS, public IP, and email server.

For network information, see Network Parameter Information for IPv4 on page 12.

6 Type your password to configure the Risk Manager root password.

7 Select **Next** and press Enter.

8 Retype your new password to confirm. Select **Finish** and press Enter.

This process typically takes several minutes.

Reading Risk Manager as a Managed Host

You can read Risk Manager as a managed host after it is removed.

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.

For default login information, see Table 3: Default login information for Risk Manager on page 12.

4 On the **Admin** tab, click **Deployment Editor**.

5 Click the **System View** tab.

6 From the menu, select **Actions** > **Add a managed host**.

7 Click **Next**.

8 Enter values in the **Add new managed host** window.

9 Click **Next**.

10 Click **Finish**.

The process of adding Risk Manager can take several minutes to complete.

11 Close the deployment editor.

12 On the **Admin** tab, click **Deploy Changes**.

7 Data Back Up and Restore

You can use a command-line interface (CLI) script to back up data that is stored on SIEM Console managed hosts.

You can use the CLI script to restore Risk Manager after a data failure or hardware failure on the appliance.

A backup script is included in Risk Manager, which can be scheduled by using crontab. The script automatically creates a daily archive of Risk Manager data at 3:00 AM. By default, Risk Manager keeps the last five backups. If you have network or attached storage, you must create a cron job to copy Risk Manager back archives to a network storage location.

The backup archive includes the following data:

- Risk Manager device configurations
- Connection data
- Topology data
- Policy Monitor questions
- Risk Manager database tables

For information about migrating from Risk Manager Maintenance Release 5 to this current release, see the *Risk Manager Migration Guide*.

Prerequisites for Backing Up and Restoring Data

You must understand how data is backed up, stored, and archived before you back up and restore your data.

Data Backup Location

Data is backed up in the `/store/qrm_backups` local directory. Your system might include a mount `/store/backup` from an external SAN or NAS service. External services provide long term offline retention of data. Long-term storage might be required for compliance regulations, such as Payment Card Industry (PCI) standards.

Appliance Version

The version of the appliance that created the backup in the archive is stored. A backup can only be restored in a Risk Manager appliance if it is the same version.

Data Backup Frequency and Archival Information

Daily data backups are created at 3:00 AM. Only the last five backup files are stored. A backup archive is created if there is enough free space on Risk Manager.

Format of Backup Files

Use the following format to save backup files: `backup-<target date>-<timestamp>.tgz`

Where:

`<target date>` is the date that the backup file was created.

The format of the target date is `<day>_<month>_<year>`. `<timestamp>` is the time that the backup file was created. The format of the timestamp is `<hour>_<minute>_<second>`.

Backing Up Your Data

Automatic backup occurs daily, at 3:00 AM, or you can start the backup process manually.

1. Using SSH, log in your SIEM Console as the root user.
2. Using SSH from the SIEM Console, log in to Risk Manager as the root user.
3. Start a Risk Manager backup by typing `/opt/qradar/bin/dbmaint/risk_manager_backup.sh`

The script that is used to start the backup process might take several minutes to start.

After the script completes the backup process, the following message is displayed:

```
Tue Sep 11 10:14:41 EDT 2012
- Risk Manager Backup complete,
wrote /store/qrm_backups/backup-2012-09-11-10-14-39.tgz
```

Restoring Data

You can use a restore script to restore data from a Risk Manager backup.

The Risk Manager appliance and the backup archive must be the same version of Risk Manager. If the script detects a version difference between the archive and the Risk Manager managed host, an error is displayed.

Use the restore script to specify the archive that you are restoring to Risk Manager. This process requires you to stop services on Risk Manager. Stopping services logs off all Risk Manager users and stops multiple processes.

The following table describes the parameters that you can use to restore a backup archive.

Table 4: Parameters used to restore a backup archive to Risk Manager

Option	Description
`-f`	Overwrites any existing Risk Manager data on your system with the data in the restore file. Selecting this parameter allows the script to overwrite any existing device configurations in Configuration Source Management with the device configurations from the backup file.
`-w`	Do not delete directories before you restore Risk Manager data.
`-h`	The help for the restore script.

1 Using SSH, log in your SIEM console as the root user.

2 Using SSH from the SIEM console, log in to Risk Manager as the root user.

3 Stop hostcontext by typing `service hostcontext stop`.

4 Type the following command to restore a backup archive to Risk Manager: `/opt/qradar/bin/risk_manager_restore.sh -r /store/qrm_backups/<backup>`. Where `<backup>` is the Risk Manager archive you want to restore.

For example, backup-2012-09-11-10-14-39.tgz.

5 Start hostcontext by typing `service hostcontext start`.