Extreme Networks Security Risk Manager Installation Guide

9035029

Published August 2016

Legal Notice

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

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

Trademarks

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

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

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks

Support

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

For information, contact:
Extreme Networks, Inc.
145 Rio Robles
San Jose, California 95134
USA

Table of Contents

Preface

Text Conventions

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

Table 1: Notice Icons

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

Providing Feedback to Us

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

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

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

Getting Help

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

- Global Technical Assistance Center (GTAC) for Immediate Support
  - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
  - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal — Manage cases, downloads, service contracts, product licensing, and training and certifications.

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

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

Related Publications

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

ExtremeSecurity Analytics

- *Extreme Security Release Notes*
- *Extreme SIEM Administration Guide*
- *Extreme SIEM Getting Started Guide*
- *Extreme SIEM High Availability Guide*
- *Extreme SIEM User Guide*
- *Extreme SIEM Tuning Guide*

- *ExtremeSecurity API Reference Guide*
- *ExtremeSecurity Ariel Query Language Guide*
- *ExtremeSecurity Application Configuration Guide*
- *ExtremeSecurity DSM Configuration Guide*
- *ExtremeSecurity Hardware Guide*
- *ExtremeSecurity Installation Guide*
- *Extreme Networks Security Juniper NSM Plug-in User Guide*
- *ExtremeSecurity Log Manager Administration Guide*
- *ExtremeSecurity Log Manager Users Guide*
- *Migrating ExtremeSecurity Log Manager to Extreme SIEM*
- *ExtremeSecurity Managing Log Sources Guide*
- *ExtremeSecurity Offboard Storage Guide*
- *ExtremeSecurity Release Notse*
- *ExtremeSecurity Risk Manager Adapter Configuration Guide*
- *ExtremeSecurity Risk Manager Getting Started Guide*
- *ExtremeSecurity Risk Manager Installation Guide*
- *ExtremeSecurity Troubleshooting System Notifications Guide*
- *ExtremeSecurity Upgrade Guide*
- *ExtremeSecurity Vulnerability Manager User Guide*
- *ExtremeSecurity Vulnerability Assessment Configuration Guide*
- *ExtremeSecurity WinCollect User Guide*

1 Prepare to install Extreme Networks Security Risk Manager

USB flash drive installations

Extreme Security Console and Risk Manager use the same installation process and ISO image. After you install the Console and Risk Manager, you add Risk Manager as a managed host by using the **System and License Management** tool on the **Admin** tab. A Risk Manager appliance is preinstalled with the Risk Manager software and a Red Hat Enterprise Linux™ operating system.

USB flash drive installations

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 ExtremeSecurity v7.2.1 appliance or later
- A Linux™ system that is installed with Red Hat Enterprise Linux™ 6.7
- Microsoft™ Windows™ Vista
- Microsoft™ Windows™ 7
- Microsoft™ Windows™ 2008
- Microsoft™ Windows™ 2008R2

Installation overview

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

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

   See the *ExtremeSecurity Release Notse* for installation instructions for fix packs and maintenance releases.

2 Before you install

For information about installing Extreme SIEM, including hardware and software requirements, see *Extreme SIEM Administration 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

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

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

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

Unsupported features in Extreme Networks Security Risk Manager

The following features are not supported in Risk Manager:

- High availability (HA)
- Dynamic Routing for Border Gateway Protocol (BGP)
- IPv6

- Non-contiguous network masks
- Load-balanced routes

3 Additional hardware requirements

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

- Monitor and keyboard
- Uninterrupted Power Supply (UPS)

Protect your Risk Manager installations that store data by using an Uninterrupted Power Supply (UPS). Using a UPS ensures that your Risk Manager data, such as the data that is stored on consoles, event processors, and Extreme Security QFlow Collectors, is preserved during a power failure.

4 Additional software requirements

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

5 Supported web browsers

Enabling document mode and browser mode in Internet Explorer

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

The following table lists the supported versions of web browsers.

Table 3: Supported web browsers for ExtremeSecurity products

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

Enabling document mode and browser mode in Internet Explorer

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

6 Install Extreme Networks Security Risk Manager appliances

Installing Risk Manager involves the following steps:

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

Preparing your appliance

You must install all necessary hardware and you need an activation key. The activation key is a 24-digit, 4-part, alphanumeric string that you receive from Extreme Networks®. You can find the activation key:

- Printed on a sticker that is placed on your appliance.
- Included with the packing slip, where 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 *Extreme Networks Security Hardware Guide*.

1 Connect a keyboard and monitor to their respective ports.
2 Power on the system and log in. The user name, which is case-sensitive, is root.
3 Press **Enter**.
4 Read the information in the window. Press the Space bar 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 then press Enter.

Access the Extreme Networks Security Risk Manager user interface

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

Table 4: Default login information for Risk Manager

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

Network parameter information for IPv4

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 by 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 Extreme Networks Security Risk Manager

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 host name, 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 14.
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.

Adding Extreme Networks Security Risk Manager to Extreme Networks SIEM Console

If you want to enable compression, then the minimum version for each managed host must be Extreme Security Console V7.1 or Risk Manager V7.1.

To add a managed host that is not NATed to your deployment where the Console is NATed, you must change the Extreme Security 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 SIEM Administration Guide*.

1 Open your web browser.
2 Type the URL, `https://<IP Address>`, where <*IP Address*> is the IP address of the Extreme Security Console.
3 Type your user name and password.
4 Click the **Admin** tab.
5 In the System Configuration pane, click **System and License Management**.
6 In the System and License Management window, click **Deployment Actions**, and then select **Add Host**.
7 Click **Next**.
8 Enter values for the following parameters:

Option	Description
Host IP	The IP address of Risk Manager.
Host Password	The root password for the host.
Confirm Host Password	Confirmation for your password.
Encrypt Host Connections	Creates an SSH encryption tunnel for the host. To enable encryption between two managed hosts, each managed host must be running Extreme Security Console V7.1 or Risk Manager V7.1.
Encryption Compression	Enables data compression between 2 managed hosts.
Network Address Translation	To enable NAT for a managed host, the NATed network must be using static NAT translation. For more information, see the *Extreme SIEM Administration Guide*.

9 If you select the **Network Address Translation** check box, then you must enter values for the NAT parameters:

Option	Description
NAT Group	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 Extreme Security Console, select the managed host of the NATed network.
Public IP	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.

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

11 From the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

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

Clearing web browser cache

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.

7 Risk Manager user role

Assigning the Risk Manager user role

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 allow users in your organization to have access to Extreme Networks Security Risk Manager functions, you must assign the appropriate user role permissions. By default, Extreme Security 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 *Extreme SIEM Administration Guide*.

Assigning the Risk Manager user role

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 Ctrl key while you select each log source you want to add.
7. Click **Return**.
8. From the **Admin** tab menu, click **Deploy Changes**.

8 Troubleshoot the Risks tab

Removing a managed host

When the Risks tab is not displaying properly or is inaccessible, you remove and re-add Extreme Networks Security Risk Manager as a managed host.

Removing a managed host

1 Log in to Extreme Security Console as an administrator:

`https://IP_Address_QRadar`

The default user name is **admin**. The password is the password of the root user account that was entered during the installation.

2 Click the **Admin** tab.

3 In the **System Configuration** pane, click **System and License Management**.

4 From the host table, click the Risk Manager host that you want to remove, and click **Deployment Actions** > **Remove Host**.

5 From the **Admin** tab menu bar, click **Deploy Changes**.

6 Refresh your web browser.

9 Re-adding Extreme Networks Security Risk Manager as a managed host

1 On the **Admin** tab, click **System and License Management** > **Deployment Actions** > **Add Host**.
2 Enter the host IP address and password.
3 Click **Add**.

You must wait several minutes while the managed host is added.

4 Close the System and License Management window.
5 On the **Admin** tab toolbar, click **Advanced** > **Deploy Full Configuration**.
6 Click **OK**.

Note

When you remove a Risk Manager managed host and then re-add a Risk Manager managed host by using a different IP address, you must restart the hostcontext and tomcat services.

Use SSH to log in to the Extreme Security Console as the root user and type the following commands to restart these services:

```
service tomcat start
service hostcontext start
```

10 Reinstall Extreme Networks Security Risk Manager from the recovery partition

Reinstalling Extreme Networks Security Risk Manager by using Factory re-install

This information applies to new Risk Manager installations or upgrades from new Risk Manager on Risk Manager appliances. When you install Risk Manager, the installer (Extreme Security 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 Extreme Security Console and Risk Manager use the same ISO installation file, the Extreme Security 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 Extreme Security 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 Extreme Networks Security Risk Manager by using Factory re-install

Ensure that you have your activation key, which is a 24-digit, 4-part, alphanumeric string that you receive from Extreme Networks®. You can find the key in these places:

- Printed on a sticker that is placed on your appliance.
- Included with the packing slip, where 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/).

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 Space bar 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 Follow the instructions in the wizard.

   This process typically takes several minutes.
9 Press `Enter` to select **OK**.
10 Press `Enter` to select **OK**.

11 Change network settings

Removing a managed host
Changing network settings
Re-adding Extreme Networks Security Risk Manager as a managed host

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

1 Remove QRadar® Risk Manager as a managed host.
2 Change network settings.
3 Re-add QRadar® Risk Manager as a managed host.

Removing a managed host

1 Log in to Extreme Security Console as an administrator:

`https://IP_Address_QRadar`

The default user name is **admin**. The password is the password of the root user account that was entered during the installation.

2 Click the **Admin** tab.
3 In the **System Configuration** pane, click **System and License Management**.
4 From the host table, click the Risk Manager host that you want to remove, and click **Deployment Actions** > **Remove Host**.
5 From the **Admin** tab menu bar, click **Deploy Changes**.
6 Refresh your web browser.

Changing network settings

You must remove the Risk Manager managed host from Extreme Security 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 host name, 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 14.

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.

Re-adding Extreme Networks Security Risk Manager as a managed host

1 On the **Admin** tab, click **System and License Management** > **Deployment Actions** > **Add Host**.

2 Enter the host IP address and password.

3 Click **Add**.

You must wait several minutes while the managed host is added.

4 Close the System and License Management window.

5 On the **Admin** tab toolbar, click **Advanced** > **Deploy Full Configuration**.

6 Click **OK**.

Note

When you remove a Risk Manager managed host and then re-add a Risk Manager managed host by using a different IP address, you must restart the hostcontext and tomcat services.

Use SSH to log in to the Extreme Security Console as the root user and type the following commands to restart these services:

```
service tomcat start
service hostcontext start
```

12 Data back up and restore

You can use the CLI script to restore Extreme Networks Security 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 *Extreme Networks Security Risk Manager Migration Guide*.

Prerequisites for backing up and restoring 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 be restored only in an Extreme Networks Security 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 time stamp is `<hour>_<minute>_<second>`.

Backing up your data

1. Using SSH, log in your Extreme Networks SIEM Console as the root user.
2. Using SSH from the Extreme Security Console, log in to Risk Manager as the root user.
3. Start a Risk Manager backup by typing the following command:

   ```
   /opt/qradar/bin/dbmaint/risk_manager_backup.sh
   ```

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

The following message is an example of the output that is displayed, after the script completes the backup process:

```
Fri Sep 11 10:14:41 EDT 2015
- Risk Manager Backup complete,
wrote /store/qrm_backups/backup-2015-09-11-10-14-39.tgz
```

Restoring data

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 5: 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 Extreme Networks SIEM Console as the root user.
2 Using SSH from the Extreme Networks 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 that you want to restore.

   For example, `backup-2012-09-11-10-14-39.tgz`.
5 Start `hostcontext` by typing `service hostcontext start`.