Extreme®
Connect Beyond the Network

Extreme Networks Security Installation Guide

9035027

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

Introduction to ExtremeSecurity installations

Extreme Networks Security Analytics appliances are pre-installed with software and the Red Hat Enterprise Linux™ operating system. You can also install ExtremeSecurity software on your own hardware.

Thank you for ordering your appliance from IBM®! It is strongly recommended that you apply the latest maintenance to you appliance for the best results. Please visit Fix Central to determine the latest recommended patch for your product.

To install or recover a high-availability (HA) system, see the *Extreme SIEM High Availability Guide*.

Intended audience

Network administrators who are responsible for installing and configuring ExtremeSecurity systems must be familiar with network security concepts and the Linux™ operating system.

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.

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	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 ExtremeSecurity deployment overview

For maximum performance and scalability, you must install a high-availability (HA) managed host appliance for each system that requires HA protection. For more information about installing or recovering an HA system, see the *Extreme SIEM High Availability Guide*.

Activation keys and license keys

Activation key

The activation key is a 24-digit, 4-part, alphanumeric string that you receive from IBM®. All installations of ExtremeSecurity products use the same software. However, the activation key specifies which software modules to apply for each appliance type. For example, use the Extreme Networks Security QFlow Collector activation key to install only the QFlow Collector modules.

You can obtain the activation key from the following locations:

- If you purchased an appliance that is pre-installed with ExtremeSecurity software, the activation key is included in a document on the enclosed CD.
- If you purchased ExtremeSecurity software or virtual appliance download, a list of activation keys is included in the *Getting Started* document.

License key

Your system includes a temporary license key that provides you with access to ExtremeSecurity software for five weeks. After you install the software and before the default license key expires, you must add your purchased licenses.

The following table describes the restrictions for the default license key:

Table 3: Restrictions for the default license key for Extreme SIEM installations

Usage	Limit
Active log source limit	750
Events per second threshold	5000
Flows per interval	200000

Table 3: Restrictions for the default license key for Extreme SIEM installations (continued)

Usage	Limit
User limit	10
Network object limit	300

Table 4: Restrictions for the default license key for Log Manager installations

Usage	Limit
Active log source limit	750
Events per second threshold	5000
User limit	10
Network object limit	300

When you purchase a ExtremeSecurity product, an email that contains your permanent license key is sent. These license keys extend the capabilities of your appliance type and define your system operating parameters. You must apply your license keys before your default license expires.

Related Links

Installing a Extreme Security Console or managed host on page 22

Installing RHEL on your own appliance on page 28

You can install the Red Hat Enterprise Linux™ operating system on your own appliance for use with Extreme Networks Security Analytics.

Installing the ExtremeSecurity software on a virtual machine on page 34

After you create your virtual machine, you must install the Extreme Networks Security Analytics software on the virtual machine.

Integrated Management Module

You can configure Integrated Management Module to share an Ethernet port with the Extreme Networks Security Analytics product management interface. However, to reduce the risk of losing the connection when the appliance is restarted, configure Integrated Management Module in dedicated mode.

To configure Integrated Management Module, you must access the system BIOS settings by pressing F1 when the IBM® splash screen is displayed. For more information about configuring Integrated Management Module, see the *Integrated Management Module User's Guide* on the CD that is shipped with your appliance.

Related Links

Prerequisite hardware accessories and desktop software for ExtremeSecurity installations on page 14

Before you install Extreme Networks Security Analytics products, ensure that you have access to the required hardware accessories and desktop software.

ExtremeSecurity components

Extreme Networks Security Analytics consolidates event data from log sources that are used by devices and applications in your network.

Important
Software versions for all Extreme Networks Security Analytics appliances in a deployment must be same version and fix level. Deployments that use different versions of software are not supported.

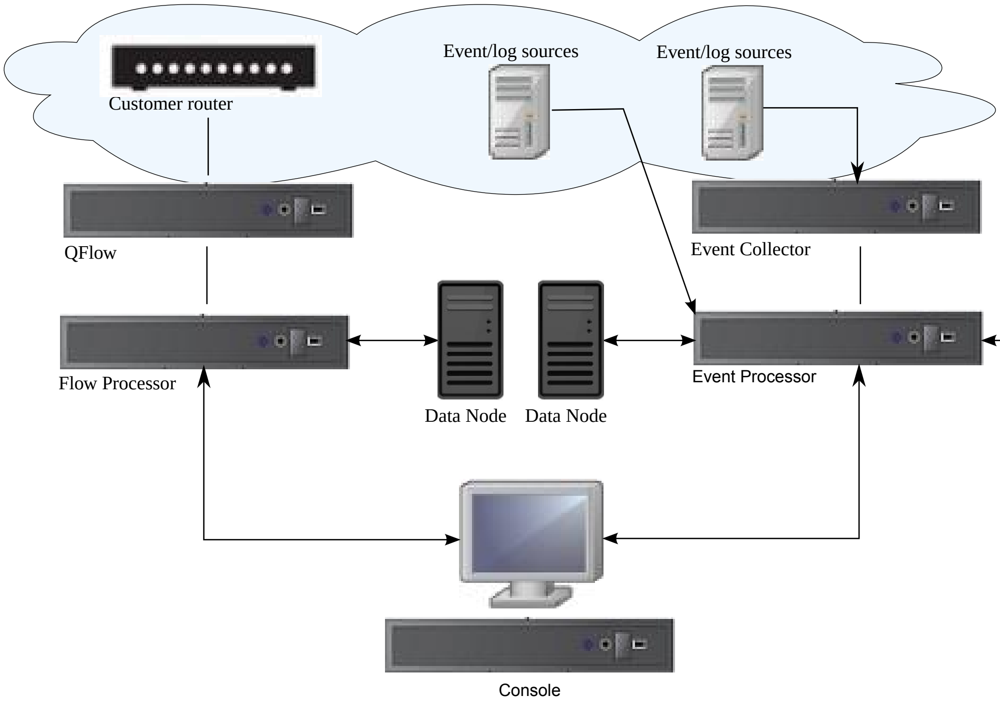

Figure 1: ExtremeSecurity deployment example

ExtremeSecurity deployments can include the following components:

QFlow Collector

Passively collects traffic flows from your network through span ports or network taps. The Extreme Networks Security QFlow Collector also supports the collection of external flow-based data sources, such as NetFlow.

You can install a QFlow Collector on your own hardware or use one of the QFlow Collector appliances.

Restriction
The component is available only for Extreme SIEM deployments.

Extreme Security Console

Provides the ExtremeSecurity product user interface. The interface delivers real-time event and flow views, reports, offenses, asset information, and administrative functions.

In distributed ExtremeSecurity deployments, use the Extreme Security Console to manage hosts that include other components.

Magistrate

A service running on the Extreme Security Console, the Magistrate provides the core processing components. You can add one Magistrate component for each deployment. The Magistrate provides views, reports, alerts, and analysis of network traffic and security events.

The Magistrate component processes events against the custom rules. If an event matches a rule, the Magistrate component generates the response that is configured in the custom rule.

For example, the custom rule might indicate that when an event matches the rule, an offense is created. If there is no match to a custom rule, the Magistrate component uses default rules to process the event. An offense is an alert that is processed by using multiple inputs, individual events, and events that are combined with analyzed behavior and vulnerabilities. The Magistrate component prioritizes the offenses and assigns a magnitude value that is based on several factors, including number of events, severity, relevance, and credibility.

ExtremeSecurity Event Collector

Gathers events from local and remote log sources. Normalizes raw log source events. During this process, the Magistrate component, on the Extreme Security Console, examines the event from the log source and maps the event to a Extreme Security Identifier (QID). Then, the Event Collector bundles identical events to conserve system usage and sends the information to the Event Processor

- Use the Event Collector 1501 in remote locations with slow WAN links. The Event Collector appliances do not store events locally. Instead, the appliances collect and parse events before sending events to an Event Processor appliance for storage.
- The Event Collector can use bandwidth limiters and schedules to send events to the Event Processor to avoid WAN limitations.
- The Event Collector is assigned to an EPS license that matches the Event Processor that it is connected to.

ExtremeSecurity Event Processor

Processes events that are collected from one or more Event Collector components. The Event Processor correlates the information from ExtremeSecurity products and distributes the information to the appropriate area, depending on the type of event.

The Event Processor also includes information that is gathered by ExtremeSecurity products to indicate behavioral changes or policy violations for the event. When complete, the Event Processor sends the events to the Magistrate component.

When to add Event Processors

- If your event rate exceeds the rating for an ExtremeSecurity 3105 (All-in-One), 5000 EPS, you must add a Event Processor 1605 or a Event Processor 1628.
- If you collect and store events in a different country or state, you may need to add Event Processors to comply with local data collection laws.

Data Node

Data Nodes enable new and existing ExtremeSecurity deployments to add storage and processing capacity on demand as required. Data Notes increase the search speed on your deployment by allowing you to keep more of your data uncompressed.

For more information about each component, see the *Administration Guide*.

ExtremeSecurity appliance sizing

The following table provides guidance for when to use specific ExtremeSecurity appliances in your deployment.

Table 5: ExtremeSecurity appliance overview

Appliance	Description
ExtremeSecurity 2100	A non-expandable solution for deployments with 10-200 employees.
ExtremeSecurity 3105 (All-in-One)	Offers increased capacity over the ExtremeSecurity 2100, and offers the ability to add Event Processors and Flow Processors.
ExtremeSecurity 3105 (Console)	If your deployment processes more than 5000 events per second (EPS), you must use a ExtremeSecurity 3105 (Console) with distributed Event Processors. The ExtremeSecurity 3105 (Console) uses offboard event processing and storage to free up resources for serving reports, search results, and faster UI actions.
ExtremeSecurity 3128 (All-in-One)	Offers increased capacity over the ExtremeSecurity 3105 (All-in-One).
ExtremeSecurity 3128 (Console)	Offers increased capacity over the ExtremeSecurity 3105 (Console).
xx05 collectors and processors	12 processors 64 GB of RAM 6.2 TB of usable storage
xx28 collectors and processors	28 processors 128 GB of RAM 40 TB of usable storage Pair xx28 collectors and processors with the ExtremeSecurity 3128 (Console) to increase performance.

When to add Flow Processors

- When your netflow collection rate exceeds the flow rating for your 31xx appliance, you must move to a dedicated Flow Processor.
- If you are adding Extreme Security QFlow Collectors to your deployment, you must add Flow Processors to store and process the QFlow data.
- If you collect and store flows in a different country or state, you may need to add Flow Processors to comply with local data collection laws.

Related Links

Troubleshooting problems on page 61

Data Node Overview on page 53

Understand how to use Data Nodes in your Extreme Networks Security Analytics deployment.

Prerequisite hardware accessories and desktop software for ExtremeSecurity installations

Hardware accessories

Ensure that you have access to the following hardware components:

- Monitor and keyboard, or a serial console
- Uninterrupted Power Supply (UPS) for all systems that store data, such as Extreme Security Console, Event Processor components, or QFlow Collector components
- Null modem cable if you want to connect the system to a serial console

Important
ExtremeSecurity products support hardware-based Redundant Array of Independent Disks (RAID) implementations, but do not support software-based RAID installations.

Desktop software requirements

Ensure that Java™ Runtime Environment (JRE) version 1.7 or 64-bit Runtime Environment for Java™ V7.0 is installed on all desktop systems that you use to access the ExtremeSecurity product user interface.

Related Links

Installing a Extreme Security Console or managed host on page 22

Installing RHEL on your own appliance on page 28
You can install the Red Hat Enterprise Linux™ operating system on your own appliance for use with Extreme Networks Security Analytics.

Installing the ExtremeSecurity software on a virtual machine on page 34
After you create your virtual machine, you must install the Extreme Networks Security Analytics software on the virtual machine.

Firmware update

Update the firmware on Extreme Networks Security Analytics appliances to take advantage of additional features and updates for the internal hardware components of the appliance.

For more information about updating firmware, see Firmware update.

Supported web browsers

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

The following table lists the supported versions of web browsers.

Table 6: 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.

Related Links

Prerequisite hardware accessories and desktop software for ExtremeSecurity installations on page 14

Before you install Extreme Networks Security Analytics products, ensure that you have access to the required hardware accessories and desktop software.

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

Creating a bootable USB flash drive with a ExtremeSecurity appliance

You can use an Extreme Networks Security Analytics V7.2.1 or later appliance to create a bootable USB flash drive that can be used to install ExtremeSecurity software.

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

- A 2 GB USB flash drive
- A ExtremeSecurity V7.2.1 or later ISO image file
- A physical ExtremeSecurity appliance

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

   a Access the IBM® Support website (www.ibm.com/support).

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

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

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

3 Insert the USB flash drive in the USB port on your ExtremeSecurity 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 ExtremeSecurity 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 QRadar® 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 ExtremeSecurity 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 IBM® Support website (www.ibm.com/support).

- ExtremeSecurity V7.2.1 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 ExtremeSecurity 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 QRadar® 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 v6.7 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 ExtremeSecurity V7.2.1 or later ISO image file
- A Linux™ system that has the following software installed:
  - Red Hat 6.7
  - Python 6.2 or later

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

1 Download the ExtremeSecurity ISO image file.

   a Access the IBM® Support website (www.ibm.com/support).

   b Locate the Extreme Networks Security Analytics ISO file.

   c Copy the ISO image file to a `/tmp` directory on your ExtremeSecurity 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 ExtremeSecurity 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 QRadar® with a USB flash drive.

Configuring a USB flash drive for 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 ExtremeSecurity with the USB flash drive.

Installing ExtremeSecurity with a USB flash drive

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

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

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

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

Third-party software on ExtremeSecurity appliances

Extreme Networks Security Analytics is a security appliance that is built on Linux, and is designed to resist attacks. ExtremeSecurity is not intended as a multi-user, general-purpose server. It is designed and developed specifically to support its intended functions. The operating system and the services are designed for secure operation. ExtremeSecurity has a built-in firewall, and allows administrative access only through a secure connection that requires encrypted and authenticated access, and provides controlled upgrades and updates. ExtremeSecurity does not require or support traditional anti-virus or malware agents, or support the installation of third-party packages or programs.

2 Bandwidth for managed hosts

For more information about deploying managed hosts and components after installation, see the *Extreme SIEM Administration Guide*.

3 Installing a Extreme Security Console or managed host

Ensure that the following requirements are met:

- The required hardware is installed.
- A keyboard and monitor are connected by using the VGA connection.
- The activation key is available.
- If you want to configure bonded network interfaces, see www.ibm.com/developerworks (http://www.ibm.com/developerworks/library/se-nic4qradar/).

1 Type `setup` to proceed and log in as root.

2 Accept the Internal Program License Agreement.

> Tip
> Press the Spacebar key to advance through the document.

3 When you are prompted for the activation key, enter the 24-digit, 4-part, alphanumeric string that you received from IBM®.

The letter I and the number 1 (one) are treated the same. The letter O and the number 0 (zero) are also treated the same.

4 For the type of setup, select **normal**, Enterprise model, and set up the time.

5 Select the Internet Protocol version:

- Select **Yes** to auto-configure ExtremeSecurity for IPv6.
- Select **No** to configure an IP address manually ExtremeSecurity for IPv4 or IPv6.

6 Select the bonded interface set up if required.

7 Select the management interface.

8 In the wizard, enter a fully qualified domain name in the **Hostname** field.

9 In the **IP address** field, enter a static IP address, or use the assigned IP address.

> Important
> If you are configuring this host as a primary host for a high availability (HA) cluster, and you selected **Yes** for auto-configure, you must record the automatically-generated IP address. The generated IP address is entered during HA configuration.

For more information, see the *Extreme SIEM High Availability Guide*.

10 If you do not have an email server, enter `localhost` in the **Email server name** field.

11 In the **Root password** field, create a password that meets the following criteria:

- Contains at least 5 characters
- Contains no spaces
- Can include the following special characters: @, #, ^, and *.

12 Click **Finish**.

13 Follow the instructions in the installation wizard to complete the installation.

   The installation process might take several minutes.

14 Apply your license key.

   a Log in to ExtremeSecurity:

   ```
   https://IP_Address_QRadar
   ```

   The default user name is **`admin`**. The password is the password of the root user account.

   b Click **Login To QRadar**.

   c Click the **Admin** tab.

   d In the navigation pane, click **System Configuration**.

   e Click the **System and License Management** icon.

   f From the **Display** list box, select **Licenses**, and upload your license key.

   g Select the unallocated license and click **Allocate System to License**.

   h From the list of systems, select a system, and click **Allocate System to License**.

15 If you want to add managed hosts, see the *Extreme SIEM Administration Guide*.

Go to the IBM Security App Exchange to download *Security applications* for your installation. For more information, see the *Content Management* chapter in the *Extreme SIEM Administration Guide*.

4 ExtremeSecurity software installations on your own appliance

Ensure that your appliance meets the system requirements for ExtremeSecurity deployments.

Important
Install no software other than ExtremeSecurity and Red Hat Enterprise Linux™ on your appliance.

If you are installing ExtremeSecurity software on your own hardware, you can now purchase the RHEL license as part of the ExtremeSecurity software purchase, and use the RHEL that ships with the ExtremeSecurity software ISO image.

Install RHEL separately if your ExtremeSecurity purchase does not include the RHEL operating system. If your QRadar system does include RHEL, you do not need to configure partitions and perform other RHEL preparation. Proceed to Installing a Extreme Security Console or managed host on page 22.

Important
Do not install RPM packages that are not approved by IBM. Unapproved RPM installations can cause dependency errors when you upgrade ExtremeSecurity software and can also cause performance issues in your deployment. Do not use YUM to update your operating system or install unapproved software on ExtremeSecurity systems.

Prerequisites for installing ExtremeSecurity on your own appliance

The following table describes the system requirements:

Table 7: System requirements for RHEL installations on your own appliance

Requirement	Description
Supported software version	Version 6.7
Bit version	64-bit
KickStart disks	Not supported
Network Time Protocol (NTP) package	Optional If you want to use NTP as your time server, ensure that you install the NTP package

Table 7: System requirements for RHEL installations on your own appliance (continued)

Requirement	Description
Memory (RAM) for Console systems	Minimum 32 GB **Note:** You must upgrade your system memory before you install ExtremeSecurity.
Memory (RAM) for Event Processor	24 GB
Memory (RAM) for QFlow Collector	16 GB
Free disk space for Console systems	Minimum 256 GB **Note:** For optimal performance, ensure that an extra 2-3 times of the minimum disk space is available.
QFlow Collector primary drive	Minimum 70 GB
Firewall configuration	WWW (http, https) enabled SSH enabled **Note:** Before you configure the firewall, disable the SELinux option. The ExtremeSecurity installation includes a default firewall template that you can update in the **System Setup** window.

Note
EFI installations are not supported.

Preparing ExtremeSecurity software installations for XFS file systems

As part of configuring high availability (HA), the ExtremeSecurity installer requires a minimal amount of free space in the storage file system, `/store/`, for replication processes. Space must be allocated in advance because XFS file systems cannot be reduced in size after they are formatted.

To prepare the XFS partition, you must do the following tasks:

1 Use the **`mkdir`** command to create the following directories:

- `/media/cdrom`
- `/media/redhat`

2 Mount the ExtremeSecurity software ISO image by typing the following command:

```
mount -o loop <path_to_QRadar_iso> /media/cdrom
```

3 Mount the RedHat Enterprise Linux™ V6.7 software by typing the following command:

```
mount -o loop <path_to_RedHat_6.7_64bit_dvd_iso_1> /media/redhat
```

4 If your system is designated as the primary host in an HA pair, run the following script:

```
/media/cdrom/post/prepare_ha.sh
```

Important
Running this command on an existing stand alone server reformats the /store partition and causes data loss.

5 To begin the installation, type the following command:

```
/media/cdrom/setup
```

Linux™ operating system partition properties for ExtremeSecurity installations on your own appliance

Use the values in following table as a guide when you re-create the partitioning on your Red Hat Enterprise Linux™ operating system.

Restriction
Resizing logical volumes by using a logical volume manager (LVM) is not supported.

Table 8: Partition guide for RHEL

Partition	Description	Mount point	File system type	Size	Forced to be primary	SDA or SDB
/boot	System boot files	/boot	EXT4	200 MB	Yes	SDA
swap	Used as memory when RAM is full.	empty	swap	Systems with 4 to 8 GB of RAM, the size of the swap partition must match the amount of RAM Systems with 8 to 24 GB of RAM, configure the swap partition size to be 75% of RAM, with a minimum value of 8 GB and a maximum value of 24 GB.	No	SDA

Table 8: Partition guide for RHEL (continued)

Partition	Description	Mount point	File system type	Size	Forced to be primary	SDA or SDB
`/`	Installation area for ExtremeSecurity, the operating system, and associated files.	`/`	EXT4	20000 MB	No	SDA
`/store/tmp`	Storage area for ExtremeSecurity temporary files	`/store/tmp`	EXT4	20000 MB	No	SDA
`/var/log`	Storage area for ExtremeSecurity and system log files	`/var/log`	EXT4	20000 MB	No	SDA
`/store`	Storage area for ExtremeSecurity data and configuration files	`/store`	XFS	[1]On Console appliances: approximately 80% of the available storage. On managed hosts other than QFlow Collectors and Store and Forward Event Collectors: approximately 90% of the available storage.	No	SDA If 2 disks, SDB

Table 8: Partition guide for RHEL (continued)

Partition	Description	Mount point	File system type	Size	Forced to be primary	SDA or SDB
`/store/transient`	Storage area for ariel database cursor	`/store/transient`	XFS on Consoles EXT4 on managed hosts	[1]On Console appliances: 20% of the available storage. On managed hosts other than QFlow Collectors and Store and Forward Event Collectors: 10% of the available storage.	No	SDA If 2 disks, SDB
[1]The `/store` and `/store/transient` together take 100% of the disk space that remains after you create the first 5 partitions.						

Restrictions

Future software upgrades might fail if you reformat any of the following partitions or their sub-partitions:

- `/store`
- `/store/tmp`
- `/store/ariel`
- `/store/transient`

Installing RHEL on your own appliance

Install RHEL separately if your ExtremeSecurity installation does not include the RHEL operating system. If your QRadar system does include RHEL, proceed to ExtremeSecurity software installations on your own appliance on page 24.

1 Copy the Red Hat Enterprise Linux™ 6.7 operating system DVD ISO to one of the following portable storage devices:

- Digital Versatile Disk (DVD)
- Bootable USB flash drive

2 Insert the portable storage device into your appliance and restart your appliance.

3 From the starting menu, select one of the following options:

- Select the **USB** or **DVD** drive as the boot option.
- To install on a system that supports Extensible Firmware Interface (EFI), you must start the system in **legacy** mode.

4 When prompted, log in to the system as the root user.

5 To prevent an issue with Ethernet interface address naming, on the Welcome page, press the Tab key and at the end of the `Vmlinuz initrd=initrd.image` line add `biosdevname=0`.

6 Follow the instructions in the installation wizard to complete the installation:

   a Select the **Basic Storage Devices** option.

   b When you configure the host name, the **Hostname** property can include letters, numbers, and hyphens.

   c When you configure the network, in the Network Connections window, select **System eth0** and then click **Edit** and select **Connect automatically**.

   d On the **IPv4 Settings** tab, from the **Method** list, select **Manual**.

   e In the **DNS servers** field, type a comma-separated list.

   f Select **Create Custom Layout** option.

   g Configure **`EXT4`** for the file system type for the `/`, `/boot`, `store/tmp`, and `/var/log` partitions.

   For more information about file system types based on appliance types, see Linux operating system partition properties for ExtremeSecurity installations on your own appliance on page 26.

   h Reformat the swap partition with a file system type of swap.

   i Select **Basic Server**.

7 When the installation is complete, click **Reboot**.

After installation, if your onboard network interfaces are named anything other than `eth0`, `eth1`, `eth2`, and `eth3`, you must rename the network interfaces.

Related Links

Linux operating system partition properties for ExtremeSecurity installations on your own appliance on page 26

If you use your own appliance, you can delete and re-create partitions on your Red Hat Enterprise Linux™ operating system rather than modify the default partitions.

5 Virtual appliance installations for Extreme SIEM and Log Manager

Restriction
Resizing logical volumes by using a logical volume manager (LVM), and EFI installations are not supported.

To install a virtual appliance, complete the following tasks in sequence:

- Create a virtual machine.
- Install ExtremeSecurity software on the virtual machine.
- Add your virtual appliance to the deployment.

Important
Install no software other than ExtremeSecurity and Red Hat Enterprise Linux™ on the virtual machine.

Overview of supported virtual appliances

A virtual appliance provides the same visibility and function in your virtual network infrastructure that ExtremeSecurity appliances provide in your physical environment.

After you install your virtual appliances, use the deployment editor to add your virtual appliances to your deployment. For more information on how to connect appliances, see the *Administration Guide*.

The following virtual appliances are available:

Extreme SIEM All-in-One Virtual 3199

This virtual appliance is a Extreme SIEM system that can profile network behavior and identify network security threats. The Extreme SIEM All-in-One Virtual 3199 virtual appliance includes an on-board Event Collector and internal storage for events.

The Extreme SIEM All-in-One Virtual 3199 virtual appliance supports the following items:

- Up to 1,000 network objects
- 200,000 flows per interval, depending on your license

- 5,000 Events Per Second (EPS), depending on your license
- 750 event feeds (more devices can be added to your licensing)
- External flow data sources for NetFlow, sFlow, J-Flow, Packeteer, and Flowlog files
- QFlow Collector and Layer 7 network activity monitoring

To expand the capacity of the Extreme SIEM All-in-One Virtual 3199 beyond the license-based upgrade options, you can add one or more of the Extreme SIEM Event Processor Virtual 1699 or Extreme SIEM Flow Processor Virtual 1799 virtual appliances:

Extreme SIEM Flow Processor Virtual 1799

This virtual appliance is deployed with any Extreme SIEM 3105 or Extreme SIEM 3124 series appliance. The virtual appliance is used to increase storage and includes an on-board Event Processor, and internal storage.

Extreme SIEM Flow Processor Virtual 1799 appliance supports the following items:

- 600,000 flows per interval, depending on traffic types
- 2 TB or larger dedicated flow storage
- 1,000 network objects
- QFlow Collector and Layer 7 network activity monitoring

You can add Extreme SIEM Flow Processor Virtual 1799 appliances to any Extreme SIEM 3105 or Extreme SIEM 3124 series appliance to increase the storage and performance of your deployment.

Extreme SIEM Event Processor Virtual 1699

This virtual appliance is a dedicated Event Processor that allows you to scale your Extreme SIEM deployment to manage higher EPS rates. The Extreme SIEM Event Processor Virtual 1699 includes an on-board Event Collector, Event Processor, and internal storage for events.

The Extreme SIEM Event Processor Virtual 1699 appliance supports the following items:

- Up to 20,000 events per second
- 2 TB or larger dedicated event storage

The Extreme SIEM Event Processor Virtual 1699 virtual appliance is a distributed Event Processor appliance and requires a connection to any Extreme SIEM 3105 or Extreme SIEM 3124 series appliance.

Data Node Virtual 1400

This virtual appliance provides retention and storage for events and flows. The virtual appliance expands the available data storage of Event Processors and Flow Processors, and also improves search performance.

Size your Data Node Virtual 1400 appliance appropriately, based on the EPS rate and data retention rules of the deployment.

Data retention policies are applied to a Data Node Virtual 1400 appliance in the same way that they are applied to stand-alone Event Processors and Flow Processors. The data retention policies are evaluated on a node-by-node basis. Criteria, such as free space, is based on the individual Data Node Virtual 1400 appliance and not the cluster as a whole.

Data Nodes can be added to the following appliances:

- Event Processor (16XX)
- Flow Processor (17XX)
- Event/Flow Processor (18XX)
- All-In-One (2100 and 31XX)

To enable all features included in the Data Node Virtual 1400 appliance, install using the 1400 activation key.

VFlow Collector 1299

This virtual appliance provides the same visibility and function in your virtual network infrastructure that a QFlow Collector offers in your physical environment. The QFlow Collector virtual appliance analyzes network behavior and provides Layer 7 visibility within your virtual infrastructure. Network visibility is derived from a direct connection to the virtual switch.

The VFlow Collector 1299 virtual appliance supports a maximum of the following items:

- 10,000 flows per minute
- Three virtual switches, with one more switch that is designated as the management interface.

The VFlow Collector 1299 virtual appliance does not support NetFlow.

System requirements for virtual appliances

Before you install your virtual appliance, ensure that the following minimum requirements are met:

Table 9: Requirements for virtual appliances

Requirement	Description
VMware client	VMWare ESX 5.0 VMWare ESX 5.1 VMWare ESX 5.5 For more information about VMWare clients, see the VMware website (www.vmware.com)
Virtual disk size on appliances	Minimum: 256 GB to install ExtremeSecurity

The following table describes the minimum memory requirements for virtual appliances.

Table 10: Minimum and optional memory requirements for ExtremeSecurity virtual appliances

Appliance	Minimum memory requirement	Suggested memory requirement
VFlow Collector 1299	6 GB	6 GB
Event Collector Virtual 1599	12 GB	16 GB

Table 10: Minimum and optional memory requirements for ExtremeSecurity virtual appliances (continued)

Appliance	Minimum memory requirement	Suggested memory requirement
Extreme SIEM Event Processor Virtual 1699	12 GB	48 GB
Extreme SIEM Flow Processor Virtual 1799	12 GB	48 GB
Extreme SIEM All-in-One Virtual 3199	24 GB	48 GB
Log Manager Virtual 3190	24 GB	48 GB
Risk Manager	24 GB	48 GB
Extreme Security Vulnerability Manager Processor	8 GB	16 GB
Extreme Security Vulnerability Manager Scanner	2 GB	4 GB

Table 11: Sample CPU page settings

Number of processors	Performance based on ExtremeSecurity appliances
4	Log manager 3190: 2500 events per second or less. Log manager Event Processor 1690, or SIEM Event Processor 1690: 2500 events per second or less. All-in-One 3190: 25000 flows per minute or less, 500 events per second or less. Flow Processor 1790: 150,000 flows per minute. Dedicated Console 3190
8	Log manager 3190: 5000 events per second or less. Log manager Event Processor 1690, or SIEM Event Processor 1690: 5000 events per second or less. All-in-One 3190: 50000 flows per minute or less, 1000 events per second or less. Flow Processor 1790: 300,000 flows per minute.
12	All-in-One 3190: 100,000 flows per minute or less, 1000 events per second or less.
16	Log manager Event Processor 1690, or SIEM Event Processor 1690: 20,000 events per second or less. All-in-One 3190: 200,000 flows per minute or less, 5000 events per second or less.

Related Links

Creating your virtual machine on page 33

To install a virtual appliance, you must first use VMWare ESX to create a virtual machine.

Creating your virtual machine

1. From the VMware vSphere Client, click **File** > **New** > **Virtual Machine**.
2. Add the **Name and Location**, and select the **Datastore** for the new virtual machine.

3 Use the following steps to guide you through the choices:

a In the **Configuration** pane of the Create New Virtual Machine window, select **Custom**.

b In the **Virtual Machine Version** pane, select **Virtual Machine Version: 7**.

c For the **Operating System (OS)**, select **Linux**, and select **Red Hat Enterprise Linux 6 (64-bit)**.

d On the **CPUs** page, configure the number of virtual processors that you want for the virtual machine. For more information about CPU settings, see System requirements for virtual appliances.

e In the **Memory Size** field, type or select the RAM required for your deployment. For more information about memory requirements, see System requirements for virtual appliances.

f Use the following table to configure you network connections.

Table 12: Descriptions for network configuration parameters

Parameter	Description
How many NICs do you want to connect	You must add at least one Network Interface Controller (NIC)
Adapter	**VMXNET3**

g In the **SCSI controller** pane, select **VMware Paravirtual**.

h In the **Disk** pane, select **Create a new virtual disk** and use the following table to configure the virtual disk parameters.

Table 13: Settings for the virtual disk size and provisioning policy parameters

Property	Option
Capacity	256 or higher (GB) for the installation. Your storage capacity depends on your event rate, the average size of your events, and your retention requirements.
Disk Provisioning	Thin provision
Advanced options	Do not configure

4 On the **Ready to Complete** page, review the settings and click **Finish**.

Install the ExtremeSecurity software on your virtual machine.

Installing the ExtremeSecurity software on a virtual machine

Ensure that the activation key is readily available.

1 In the left navigation pane of your VMware vSphere Client, select your virtual machine.

2 In the right pane, click the **Summary** tab.

3 In the **Commands** pane, click **Edit Settings**.

4 In the left pane of the **Virtual Machine Properties** window, click **CD/DVD Drive 1**.

5 In the **Device Type** pane, select **DataStore ISO File**.

6 In the **Device Status** pane, select the **Connect at power on** check box.

7 In the **Device Type** pane, click **Browse**.

8 In the Browse Datastores window, locate and select the ExtremeSecurity product ISO file, click **Open** and then click **OK**.

9 After the ExtremeSecurity product ISO image is installed, right-click your virtual machine and click **Power** > **Power On.**

10 Log in to the virtual machine by typing `root` for the user name.

The user name is case-sensitive.

11 Ensure that the End User License Agreement (EULA) is displayed.

> Tip
> Press the Spacebar key to advance through the document.

12 When you are prompted for the activation key, enter the 24-digit, 4-part, alphanumeric string that you received from IBM®.

The letter I and the number 1 (one) are treated the same. The letter O and the number 0 (zero) are also treated the same.

13 For the type of setup, select **normal**, Enterprise model, and set up the time.

14 Select the Internet Protocol version:

- Select **Yes** to auto-configure ExtremeSecurity for IPv6.
- Select **No** to configure an IP address manually ExtremeSecurity for IPv4 or IPv6.

15 Select the bonded interface set up if required.

16 Select the management interface.

17 In the wizard, enter a fully qualified domain name in the **Hostname** field.

18 In the **IP address** field, enter a static IP address, or use the assigned IP address.

> Important
> If you are configuring this host as a primary host for a high availability (HA) cluster, and you selected **Yes** for auto-configure, you must record the automatically-generated IP address. The generated IP address is entered during HA configuration.

For more information, see the *IBM Security QRadar High Availability Guide*.

19 If you do not have an email server, enter `localhost` in the **Email server name** field.

20 In the **Root password** field, create a password that meets the following criteria:

- Contains at least 5 characters
- Contains no spaces
- Can include the following special characters: @, #, ^, and *.

21 Click **Finish**.

22 Follow the instructions in the installation wizard to complete the installation.

The installation process might take several minutes.

23 Apply your license key.

   a Log in to ExtremeSecurity:

```
https://IP_Address_QRadar
```

   The default user name is **admin**. The password is the password of the root user account.

   b Click **Login To QRadar**.

   c Click the **Admin** tab.

   d In the navigation pane, click **System Configuration**.

   e Click the **System and License Management** icon.

   f From the **Display** list box, select **Licenses**, and upload your license key.

   g Select the unallocated license and click **Allocate System to License**.

   h From the list of systems, select a system, and click **Allocate System to License**.

Go to the IBM Security App Exchange to download *Security applications* for your installation. For more information, see the *Content Management* chapter in the *Extreme SIEM Administration Guide*.

Related Links

Creating your virtual machine on page 33

To install a virtual appliance, you must first use VMWare ESX to create a virtual machine.

Adding your virtual appliance to your deployment

1 Log in to the Extreme Security Console.

2 On the **Admin** tab, click the **Deployment Editor** icon.

3 In the **Event Components** pane on the **Event View** page, select the virtual appliance component that you want to add.

4 On the first page of the **Adding a New Component** task assistant, type a unique name for the virtual appliance.

   The name that you assign to the virtual appliance can be up to 20 characters in length and can include underscores or hyphens.

5 Complete the steps in the task assistant.

6 From the **Deployment Editor** menu, click **File** > **Save to staging**.

7 On the **Admin** tab menu, click **Deploy Changes**.

8 Apply your license key.

   a Log in to ExtremeSecurity:

```
https://IP_Address_QRadar
```

   The default user name is **admin**. The password is the password of the root user account.

   b Click **Login To QRadar**.

   c Click the **Admin** tab.

   d In the navigation pane, click **System Configuration**.

   e Click the **System and License Management** icon.

   f From the **Display** list box, select **Licenses**, and upload your license key.

   g Select the unallocated license and click **Allocate System to License**.

   h From the list of systems, select a system, and click **Allocate System to License**.

Related Links

Creating your virtual machine on page 33

To install a virtual appliance, you must first use VMWare ESX to create a virtual machine.

6 Installations from the recovery partition

Reinstalling from the recovery partition

When you restart your ExtremeSecurity appliance, an option to reinstall the software is displayed. If you do not respond to the prompt within 5 seconds, the system continues to start as normal. Your configuration and data files are maintained. If you choose the reinstall option, a warning message is displayed and you must confirm that you want to reinstall.

The warning message states that you can retain the data on the appliance. This data includes events and flows. Selecting the retain option backs up the data before the reinstallation, and restores the data after installation completes. If the retain option is not available, the partition where the data resides may not be available, and it is not possible to back up and restore the data. The absence of the retain option can indicate a hard disk failure. Contact Customer Support if the retain option is not available.

Important

The retain option is not available on High-Availability systems. See the *Extreme SIEM High Availability Guide* for information on recovering High-Availability appliances.

Any software upgrades of ExtremeSecurity version 7.2.0 replaces the existing ISO file with the newer version.

These guidelines apply to new ExtremeSecurity version 7.2.0 installations or upgrades from new ExtremeSecurity version 7.0 installations on ExtremeSecurity version 7.0 appliances.

Reinstalling from the recovery partition

Locate your activation key. The activation key is a 24-digit, four-part, alphanumeric string that you receive from IBM®. You can find the activation key in one of the following locations:

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

If you do not have your activation key, go to the Extreme Networks Support Portal to obtain your activation key. You must provide the serial number of the ExtremeSecurity appliance. Software activation keys do not require serial numbers.

If your deployment includes offboard storage solutions, you must disconnect your offboard storage before you reinstall ExtremeSecurity. After you reinstall, you can remount your external storage solutions. For more information on configuring offboard storage, see the *ExtremeSecurity Offboard Storage Guide*.

1 Restart your ExtremeSecurity appliance and select **Factory re-install**.

2 Type `flatten` or `retain`.

The installer partitions and reformats the hard disk, installs the OS, and then re-installs the ExtremeSecurity product. You must wait for the flatten `or retain` process to complete. This process can take up to several minutes. When the process is complete, a confirmation is displayed.

3 Type SETUP.

4 Log in as the root user.

5 Ensure that the End User License Agreement (EULA) is displayed.

> Tip
> Press the Spacebar key to advance through the document.

6 For Extreme Security Console installations, select the **Enterprise** tuning template.

7 Follow the instructions in the installation wizard to complete the installation.

8 Apply your license key.

a Log in to ExtremeSecurity:

```
https://IP_Address_QRadar
```

The default user name is **`admin`**. The password is the password of the root user account.

b Click **Login To QRadar**.

c Click the **Admin** tab.

d In the navigation pane, click **System Configuration**.

e Click the **System and License Management** icon.

f From the **Display** list box, select **Licenses**, and upload your license key.

g Select the unallocated license and click **Allocate System to License**.

h From the list of systems, select a system, and click **Allocate System to License**.

7 Setting up silent installations for ExtremeSecurity

This installation requires the Red Hat Enterprise Linux operating system, and the ExtremeSecurity V7.7.2.7 ISO. For information about version numbers and requirements, see ExtremeSecurity software installations on your own appliance on page 24.

1 Install RHEL on the host where you want to install ExtremeSecurity to set up the necessary partitions. For more information, see Installing RHEL on your own appliance on page 28.

2 As the root user, use SSH to log on to the host where you want to install ExtremeSecurity.

3 On the host where you want to install ExtremeSecurity, go to the root directory and create a file that is named `AUTO_INSTALL_INSTRUCTIONS` and that contains the following information:

Example
The following AUTO_INSTALL_INSTRUCTIONS file example shows the correct parameters for silently installing ExtremeSecurity in the America/Moncton timezone.

```
timezone=America/Moncton
sectempl=Enterprise
date=2015/05/19
ntpserver=q1dc04.canlab.ibm.com
ntpsync=1
timechoice=manual
nicid=eth0
box_ip=1.2.3.4
ip_v6=
netmask=255.255.255.255
ipverchoice=ipv4
gateway_v6=
hostname=name
pdns=1.2.3.4
bdns=5.6.7.8
newkey=######-######-######-######
defpass=password
isconsole=yes
setuptypechoice=normal
is_ha_appl=0
isconstandby=yes
smtpname=localhost
bonding_interfaces=
bonding_options=
bonding_enabled=false
```

Important
The `AUTO_INSTALL_INSTRUCTIONS` file must have no extension.

Learn more about silent installations

Table 14: Silent Install File parameters

Parameter	Required?	Description	Permitted values
`setuptypechoice`	Required	Specifies the type of installation for this host	`normal`- A standard ExtremeSecurity managed host or console deployment. `recovery` - A High Availability (HA) recovery installation on this host.

`timezone`	Required	The timezone from the TZ database. For more information, see http://timezonedb.com/.	`Europe/London`
			`America/Montreal`
			`America/New_York`
			`America/Los_Angeles`
			`Asia/Tokyo`, and so on.

`date`	Required	The current date for this host. Use the following format: `YYYY/MM/DD` format	
`timechoice`	Required	Specifies how this host obtains the current time	`manual` - The time that you manually enter in the `time parameter`. `server` - Use a Network Time Protocol (NTP) server that is specified by the ntpserver parameter
`time`	If `timechoice` is set to `manual`, then required.	The time for the host in the 24 hour format `HH:MM:SS`.	
`ntpserver`	If `timechoice` is set to `server`, then required.	The FQHN or IP address of the network time protocol (NTP) server.	
`ntpsync`	If `timechoice` is set to `server`, then required.	Enter 1 to sync with the NTP server, otherwise, enter 0.	
`nicid`	Required	The identifier for the network interface card	Values: `eth0`, `eth1`, `ethx`
`management_iface`	Required	The identifier for the management interface	Values: `eth0`, `eth1`, `ethx`
`hostname`	Optional	The fully qualified host name for your ExtremeSecurity system.	

Table 14: Silent Install File parameters (continued)

Parameter	Required?	Description	Permitted values
ipverchoice	Required	Specify the IP standard protocol for this host	IPv4, IPv6
box_ip	If ipverchoice is set to IPv4, then required	The IP address of the host that you are installing the software on	A valid IPv4 address
ip_v6	If ipverchoice is set to IPv6, then required	Enter the IPv6 address of the ExtremeSecurity installation if required.	A valid IPv6 address
netmask	If ipverchoice is set to IPv4, then required	The netmask for this host	
gateway	If ipverchoice is set to IPv4, then required	The network gateway for this host	A valid IPv4 address
gateway_v6	If ipverchoice is set to IPv6, then required	The network gateway for this host	A valid IPv6 address
ip_v6_nocidr	Optional	The IPv6 address with no Classless Inter-Domain Routing (CIDR).	A valid IPv6 address
pdns	If ipverchoice is set to IPv4, then required	The primary DNS server.	A valid IPv4 address
bdns	If ipverchoice is set to IPv4, then required	The secondary DNS server.	A valid IPv4 address
newkey	Required	The activation key for the ExtremeSecurity installation.	
defpass	Required	The default root password to use for this host.	

Table 14: Silent Install File parameters (continued)

Parameter	Required?	Description	Permitted values
`isconsole`	Required	Specify whether this host is the console within the deployment	`Y` - This host is the console in the deployment `N` - This is not the console and is another type of managed host (Event or Flow Processor, and so on)
`sectempl`	If `isconsole` is set to `Y`, then required	The security template.	`Enterprise` - for all SIEM-based hosts `Logger` - for Log Manager
`is_ha_appl`	Required	Specifies whether this host is a HA pair or companion host	`0` - This host is not an HA appliance/installation `1` - This host is an HA appliance/installation
`isconstandby`	If `isconsole` is set to `Y`, then required.	Specifies whether this host is an HA console standby	`0` - This host is not a standby HA console `1` - This host is a standby HA console
`clusterip`	Optional	Specifies the IP address for the HA cluster.	`ip_address`
`smtpname`	Required	Enter the mail server or SMTP name, such as localhost.	
`bonding _interfaces`	If using bonded interfaces, then required.	The MAC addresses for the interfaces that you are bonding, separated by commas.	`mac_addresses`
`bonding_options`	If using bonded interfaces, then required.	The Linux options for bonded interfaces.	Note: `miimon=100 mode=4 lacp_rate=1`
`bonding enabled`	If using bonded interfaces, then required.	Specifies whether you are using bonded interfaces.	`true` or `false`

4 Using an Secure File Transfer Protocol (SFTP) program, such as WinSCP, copy the ExtremeSecurity ISO to the host where you want to install ExtremeSecurity.

5 Using a program such as WinSCP, copy the RHEL ISO to the host where you want to install ExtremeSecurity.

6 Create a `/media/cdrom` directory by using the following command:

```
mkdir /media/cdrom
```

7 Create a `/media/redhat` directory by using the following command:

```
mkdir /media/redhat
```

8 Mount the ExtremeSecurity ISO by using the following command:

```
mount -o loop <qradar.iso> /media/cdrom
```

9 Mount the RHEL ISO by using the following command:

```
mount -o loop <RHEL.iso> /media/redhat
```

10 Run the ExtremeSecurity setup by using the following command:

```
/media/cdrom/setup
```

8 Overview of ExtremeSecurity deployment in a cloud environment

Important

Ensure that the following requirements are met to avoid compromised security data:

- Set a strong root password.
- Allow only specific connections to ports 443 (https), 22 (ssh), 10000 (webmin), and 1194 (UDP, TCP for OpenVPN).

Configure ExtremeSecurity for the cloud in the following order:

1 Install ExtremeSecurity on Amazon Web Service (AWS) or SoftLayer.
2 For cloud and on-premises hosts, define the role:
  - The server endpoint of a VPN tunnel.
  - The client endpoint of a VPN tunnel.
  - The member host that routes traffic that is destined for the VPN tunnel through the local VPN endpoint.
  - None, if a host that has no need to communicate with hosts on the other side of the VPN tunnel.
3 Confirm that the ExtremeSecurity firewall settings protect your network security.

Configuring an ExtremeSecurity host on a SoftLayer Virtual Machine

To avoid losing access to the ExtremeSecurity SSH login session, ensure that a second SoftLayer instance can access the ExtremeSecurity instance through the private IP address. If no private IP addresses are available, configure an hourly SoftLayer instance.

If you are not installing ExtremeSecurity behind a Vyatta firewall, you must provide the following IP addresses when you configure firewall protection:

- Your company's public IP address
- The network address of your private cloud subnet
- The network address of your local lab, or on-premises network

SoftLayer offers a number of networking options, but it is common for a SoftLayer instance to be provisioned with two interfaces that use these options:

- An IP address on the private SoftLayer network
- A public IP address

You can install ExtremeSecurity on the SoftLayer public IP address, then use ExtremeSecurity network address translation (NAT). NAT uses the IP address that is assigned to the host by the VPN as the ExtremeSecurity public IP address. However, it is simpler and more secure to install ExtremeSecurity on the SoftLayer private IP address, and this type of installation does not require NAT support.

Configuring a ExtremeSecurity host on SoftLayer bare metal servers

Get ready

To avoid losing access to the ExtremeSecurity SSH login session, ensure that a second SoftLayer instance can access the ExtremeSecurity instance through the private IP address. If no private IP addresses are available, configure an hourly SoftLayer instance.

If you are not installing ExtremeSecurity behind a Vyatta firewall, you must provide the following IP addresses when you configure firewall protection:

- Your company's public IP address
- The network address of your private cloud subnet
- The network address of your local lab, or on-premises network

SoftLayer offers a number of networking options, but it is common for a SoftLayer instance to be provisioned with two interfaces that use these options:

- An IP address on the private SoftLayer network
- A public IP address

You can install ExtremeSecurity on the SoftLayer public IP address, then use ExtremeSecurity network address translation (NAT). NAT uses the IP address that is assigned to the host by the VPN as the ExtremeSecurity public IP address. However, it is simpler and more secure to install ExtremeSecurity on the SoftLayer private IP address, and this type of installation does not require NAT support.

Configuring a ExtremeSecurity host on Amazon Web Service

1. Configure a key pair on AWS.
2. Create an Amazon EC2 instance that meets the following requirements:

Table 15: AWS Instance Requirements

Requirement	Value
Image	`RHEL-6.7_HVM_Beta_20150714-x86_64-1-Hourly-GP2`
Instance type	m4.2xlarge

Table 15: AWS Instance Requirements (continued)

Requirement	Value
Storage	1 x 100 GB volume 2 x 2 TB volumes
Security Group	Your IP addresses from the list, with ports 22 and 443 open.

Important
Commands in this procedure are examples. Values in commands can vary between deployments.

The AWS instance key is required to log in to the instance with SSH.

XFS is not supported on the RedHat Enterprise Linux™ (RHEL) v6.7 loads that are provided by AWS. Use ext4.

Important
High availability (HA) is not supported on AWS ExtremeSecurity installations.

1 To log in to the AWS instance by using the key pair that you created when you configured the instance, type the following command:

```
ssh -i <your_key>.pem ec2-user@<public_IP_address>
```

2 Enter the root shell of the AWS instance by using the following command:

```
sudo su -
```

To return to the root shell, you must enter the `sudo su -` command any time you log back in to the AWS instance to return to the root shell.

3 Determine the device that you want to configure:

a Type the `lsblk` command to list device details.

```
# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda
      202:0 0 100G 0 disk
xvda1 202:1 0 100G 0 part /
xvdc 202:32 0 100G 0 disk
xvdb 202:16 0 100G 0 disk
```

b Find the device that has no partitions and has the required storage.

After you find the block devices, export the device name and device data as environment variables for use in subsequent steps. For the preceding example, you type the following commands:

```
export device_name=/dev/xvdc

export device_data=/dev/xvdb
```

4 To create the partition type for the disk (label), type the following commands:

```
parted -a optimal --script ${device_name} -- mklabel gpt

parted -a optimal --script ${device_data} -- mklabel gpt
```

5 To create these partitions on the device, type the following commands:

> Note
> The following allocations are examples. For information about partitions, see the *IBM® Security QRadar® Installation Guide*.

```
parted -a optimal --script ${device_name} -- mkpart swap 0% 30%
parted -a optimal --script ${device_name} -- mkpart ext4 30% 60%
parted -a optimal --script ${device_name} -- mkpart ext4 60% 100%
parted -a optimal --script ${device_data} -- mkpart ext4 0% 80%
parted -a optimal --script ${device_data} -- mkpart ext4 80% 100%
```

6 To create the following file systems on the partitioned device, type the following commands:

```
mkswap -L swap1 ${device_name}1
mkfs.ext4 ${device_name}2
mkfs.ext4 ${device_name}3
mkfs.ext4 ${device_data}1
mkfs.ext4 ${device_data}2
```

7 Label the partitions with the following names:

```
e2label ${device_name}2 /var/log
e2label ${device_name}3 /store/tmp
e2label ${device_data}2 /store/transient
e2label ${device_data}1 /store
```

8 In the `/etc/fstab` file, comment out the `/dev/<device_name> /mnt`, or `/dev/<device_data> /mnt` lines if they are present.

9 Type the following commands to add the required entries to `/etc/fstab` file:

> Important
> Paste the commands into a text editor and remove the line breaks before you copy the commands to the command prompt.

```
eval `blkid -t LABEL=/store -o export` ; echo UUID=$UUID $LABEL $TYPE
 defaults,noatime 1 1 >> /etc/fstab

eval `blkid -t LABEL=/transient -o export` ; echo
      UUID=$UUID /store/transient $TYPE defaults,noatime 1 1 >> /etc/fstab

eval `blkid -t LABEL=/var/log -o export` ; echo UUID=$UUID $LABEL $TYPE
 defaults,noatime 1 1 >> /etc/fstab

eval `blkid -t LABEL=/transient -o export` ; echo UUID=$UUID /store/tmp
 $TYPE defaults.noatime 1 1 >> /etc/fstab

echo "${device_name}1 swap swap defaults 0 0" >> /etc/fstab
```

10 To create and mount the `/store` directory, type the following commands:

```
mkdir /store
mount /store
mkdir /store/tmp
mount /store/tmp
mkdir /store/transient
mount /store/transient
cd /var; mv log oldlog; mkdir log; mount /var/log; mv oldlog/* log
```

11 To enable the swap between devices, type the following command:

```
swapon -a
```

12 Confirm that the `/etc/sysconfig/i18n` line contains the following string, including the quotation marks:

```
LANG="en_US.UTF-8"
```

13 To copy the ISO image to the device, type the following command:

```
scp -i <key.pem qradar.iso> ec2-user@<Public_DNS>:qradar.iso
```

Where:

14 To mount the ISO image, type the following commands:

```
mkdir /media/cdrom
mount -o loop /home/ec2-user/qradar.iso /media/cdrom
```

15 Configure missing dependencies by using the following commands:

Important
Paste the commands into a text editor and remove the line breaks before you copy the commands in to the command prompt.

```
yum  install -y libxml2 libxml2.i686 audit-libs audit-libs.i686 glibc
glibc.i686 device-mapper-multipath zlib zlib.i686 libcom_err
libcom_err.i686 nspr nspr.i686 nss nss.i686 nss-util nss-util.i686
krb5-libs krb5-libs.i686 keyutils-libs keyutils-libs.i686
openssl   openssl.i686 httpd-tools httpd-devel httpd mod_ssl keyutils
keyutils.i686 keyutils-libs keyutils-libs.i686 openldap openldap.i686
openldap-clients cyrus-sasl-lib cyrus-sasl-lib.i686 pam pam.i686 libgcc
libgcc.i686 elfutils-libelf  elfutils-libelf.i686
libstdc++   libstdc++.i686

yum remove php.x86_64 php-cli.x86_64 php-common.x86_64
php-devel.x86_64 php-imap.x86_64 samba-common samba-winbind-clients
samba-client samba-winbind
httpd httpd-tools mod_ssl

sed -i -e "s/plugins=1/plugins=0/" /etc/yum.conf
```

16 To start the setup program, type the following command:

```
/media/cdrom/setup
```

17 Type **Y** when prompted to accept an installation on unsupported hardware.

Configuring server endpoints for cloud installations

A server endpoint requires the following items:

- A main OpenVPN configuration file.
- Routing instructions for each client in the server configuration file.
- A configuration file for each client that records routing instructions for each client that can connect.
- Additional iptables rules that allow forwarding across the tunnel.
- IP forwarding enabled in the kernel.
- A custom certificate authority (CA) to issue the certificates that are used to authenticate servers and clients.
- A server certificate that is issued by the local CA.

For more information about the OpenVPN tool options, enter `-h`.

1 To specify the server endpoint, type the following command to define the server endpoint in the cloud.

```
/opt/qradar/bin/vpntool server server_host_IP_address
network_address_behind_VPN
```

Example

```
/opt/qradar/bin/vpntool server 1.2.3.4 5.6.7.8/24
```

If your network requires TCP rather than UDP mode on your clients and servers, type the following command with your required IP addresses:

```
/opt/qradar/bin/vpntool server server_host_IP_address
 network_address_behind_VPN --tcp
```

After you define the server endpoint, VPNtool Server completes the following tasks:

- If the local certificate authority is not established, the CA is initialized and the CA key and certificate created.
- The local CA creates a key and certificate for use by this server endpoint.
- Configuration properties are written to the VPN configuration file.

2 To build and deploy the configuration, type the following command:

```
/opt/qradar/bin/vpntool deploy
```

After you build and deploy the configuration, VPNtool Server completes the following tasks::

- The OpenVPN server configuration is generated and copied into the `/etc/openvpn` directory.
- The CA certificate, and the server key and certificate, are copied into the standard location in `/etc/openvpn/pki`.
- IPtables rules are constructed and reloaded.
- IP forwarding is enabled and made persistent by updating the `/etc/sysctl.conf` file.

3 To start the server, type the following command:

```
/opt/qradar/bin/enable --now
```

Entering `/opt/qradar/bin/enable --now` creates the persistent enabled state, and automatically starts OpenVPN on system restart.

Configuring client networks for cloud installations

A client requires the following items:

- A main OpenVPN configuration file.
- Extra iptables rules to allow forwarding across the tunnel.
- IP forwarding is enabled in the kernel.
- A client certificate that is issued by the local CA.

1 On the server, inform the server of the new client, type the following command:

```
/opt/qradar/bin/vpntool addclient Console name, role,
 or IP  1.2.3.4/24
```

Informing the server of the client includes the following tasks:

- The CA certificate is copied to a known location.
- The client key and certificate from the PKCS#12 file are extracted and copied to known locations.
- Client configuration properties are written to the VPN configuration file.

2 Deploy and restart the server by using the following command:

```
/opt/qradar/bin/vpntool deploy
service openvpn restart
```

3 Copy the generated client credentials file and the CA file to the ExtremeSecurity host that is used for this client endpoint.

Example

```
scp root@ server_IP_address :/opt/qradar/conf
/vpn/pki/ca.crt /root/ca.crtscp root@ server_IP_address
:/opt/qradar/conf/vpn/pki/Console.p12 /root/Console.p12
```

4 On the client, configure the host as a VPN client:

```
/opt/qradar/bin/vpntool client server_IP_address
ca.crt client.pk12
```

If your network requires that you not configure UDP mode on your clients and servers, you can use TCP.

```
/opt/qradar/bin/vpntool client server_IP_address
/root/ca.crt /root/Console.p12 --tcp
```

5 To build and deploy the configuration, type the following command:

```
/opt/qradar/bin/vpntool deploy
```

Building and deploying the configuration includes the following steps:

- The client OpenVPN configuration file is generated and copied into place in `/etc/openvpn`.
- The CA certificate, and client key and certificate, are copied into the standard locations within `/etc/openvpn/pki`.
- Iptables rules are generated and loaded.
- IP forwarding is enabled and made persistent by updating the `/etc/sysctl.conf` file.

6 To start the client, enter the following command:

```
/opt/qradar/bin/enable --now
```

Entering `/opt/qradar/bin/enable --now` creates the persistent enabled state, and automatically starts OpenVPN on system restart.

7 To connect the client through an HTTP proxy, enter the following command:

```
/opt/qradar/bin/vpntool client IP Address  /root/ca.crt
 /root/Console.p12 --http-proxy= IP Address:port
```

- Proxy configuration is always in TCP mode, even if you do not enter TCP in the command.
- See the OpenVPN documentation for configuration options for proxy authentication. Add these configuration options to the following file:

```
/etc/openvpn/client.conf
```

Configuring a member for cloud installations

To join a Extreme SIEM host to the local VPN, so that it communicates directly with hosts on the other side of the tunnel, by using the following command:

```
/opt/qradar/bin/vpntool join local_host_IP_address remote host IP address
/opt/qradar/bin/vpntool deploy
```

9 Data Node Overview

Data Nodes enable new and existing ExtremeSecurity deployments to add storage and processing capacity on demand as required.

Users can scale storage and processing power independently of data collection, which results in a deployment that has the appropriate storage and processing capacity. Data Nodes are plug-n-play and can be added to a deployment at any time. Data Nodes seamlessly integrate with the existing deployment.

Increasing data volumes in deployments require data compression sooner. Data compression slows down system performance as the system must decompress queried data before analysis is possible. Adding Data Node appliances to a deployment allows you to keep data uncompressed longer.

The ExtremeSecurity deployment distributes all new data across the Event and Flow processors and the attached Data Nodes.

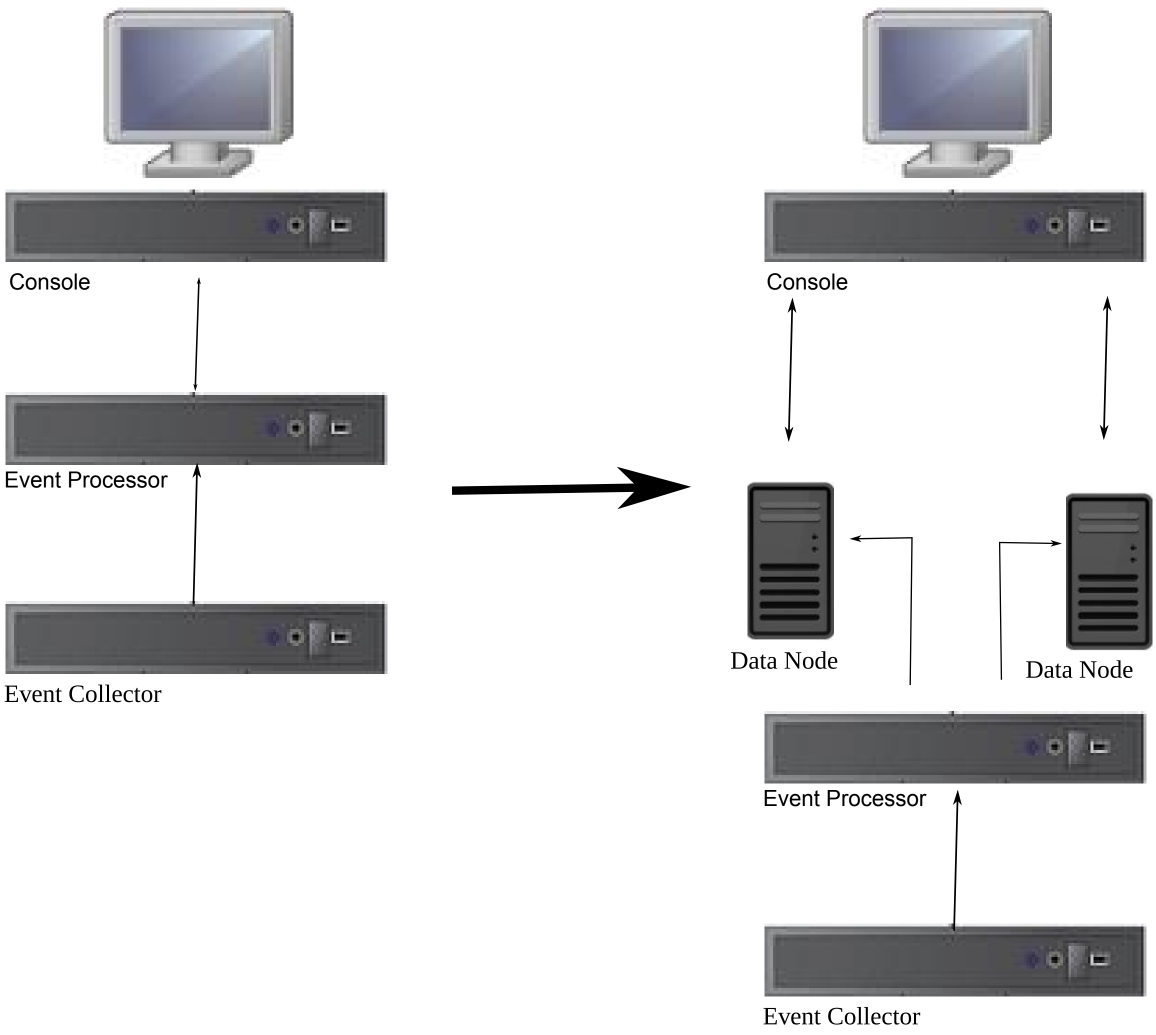

Figure 2: ExtremeSecurity deployment before and after adding Data Node appliances

Clustering

Data Nodes add storage capacity to a deployment, and also improve performance by distributing data collected on a processor across multiple storage volumes. When the data is searched, multiple hosts, or a "cluster", do the search. The cluster can greatly improve search performance, but don't require the addition of multiple event processors. Data Nodes multiply the storage for each processor.

Note
You can connect a Data Node to only one processor at a time, but a processor can support multiple data nodes.

Deployment Considerations

- Data Nodes are available on ExtremeSecurity 7.2.2 and later
- Data Nodes perform similar search and analytic functions as Event and Flow processors in a ExtremeSecurity deployment. Operations on a cluster are affected by the slowest member of a

cluster. Data Node system performance improves if Data Nodes are sized similarly to the event and flow processors in a deployment. To facilitate similar sizing between Data Nodes and event and flow processors, Data Nodes are available on both XX05 and XX28 core appliances.

- Data Nodes are available in three formats: Software (on your own hardware), Physical and Appliances. You can mix the formats in a single cluster.

Bandwidth and latency

Ensure a 1 Gbps link and less than 10 ms between hosts in the cluster. Searches that yield many results require more bandwidth.

Compatibility

Data Nodes are compatible with all existing ExtremeSecurity appliances that have an Event or Flow Processor component, including All-In-One appliances. Data Nodes are not compatible with ExtremeSecurity Incident Forensics PCAP appliances.

Data Nodes support high-availability (HA).

Installation

Data Nodes use standard TCP/IP networking, and do not require proprietary or specialized interconnect hardware. Install each Data Node that you want to add to your deployment as you would install any other ExtremeSecurity appliance. Associate Data Nodes with event or flow processors in the ExtremeSecurity Deployment Editor. See *IBM Security QRadar Administration Guide*.

You can attach multiple Data Nodes to a single Event or Flow Processor, in a many-to-one configuration.

When you deploy HA pairs with Data Node appliances, install, deploy and rebalance data with the High Availability appliances before you synchronize the HA pair. The combined effect of the data rebalancing and the replication process utilized for HA results in significant performance degradation. If High Availability is present on the existing appliances to which Data Nodes are being introduced, it is also preferable that the HA connection be broken and reestablished once the rebalance of the cluster is completed.

Decommissioning

Remove Data Nodes from your deployment with the Deployment Editor, as with any other ExtremeSecurity appliance. Decommissioning does not erase balanced data on the host. The data is not available in the user interface. You can retrieve the data for archiving and redistribution.

Data Rebalancing

Adding a Data Node to a cluster distributes data to each Data Node. Each Data Node appliance maintains the same percentage of available space. New Data Nodes added to a cluster initiate additional rebalancing from cluster event and flow processors to achieve efficient disk usage on the newly added Data Node appliances.

Starting in ExtremeSecurity 7.2.3, data rebalancing is automatic and concurrent with other cluster activity, such as queries and data collection. No downtime is experienced during data rebalancing.

Data Nodes offer no performance improvement in the cluster until data rebalancing is complete. Rebalancing can cause minor performance degradation during search operations, but data collection and processing continue unaffected.

Management and Operations

Data Nodes are self-managed and require no regular user intervention to maintain normal operation. ExtremeSecurity manages activities, such as data backups, high-availability and retention policies, for all hosts, including Data Node appliances.

Failures

If a Data Node fails, the remaining members of the cluster continue to process data.

When the failed Data Node returns to service, data rebalancing can occur to maintain proper data distribution in the cluster, and then normal processing resumes. During the downtime, data on the failed Data Node is unavailable.

For catastrophic failures requiring appliance replacement or the reinstallation of ExtremeSecurity, decommission Data Nodes from the deployment and replace them using standard installation steps. Copy any data not lost in the failure to the new Data Node before deploying. The rebalancing algorithm accounts for data existing on a data node, and shuffles only data collected during the failure.

For Data Nodes deployed with an HA pair, a hardware failure causes a failover, and operations continue to function normally.

Related Links

ExtremeSecurity components on page 11

10 Network settings management

Changing the network settings in an all-in-one system

- You must have a local connection to your Extreme Security Console
- Confirm that there are no undeployed changes.
- If you are changing the IP address host name of a box in the deployment you must remove it from the deployment.
- If this system is part of an HA pair you must disable HA first before you change any network settings.
- If the system that you want to change is the console, you must remove all hosts in the deployment before proceeding.

1 Log in to as the root user.
2 Type the following command:

```
qchange_netsetup
```

3 Follow the instructions in the wizard to complete the configuration.

The following table contains descriptions and notes to help you configure the network settings.

Table 16: Description of network settings for an all-in-one Extreme Security Console

Network Setting	Description
Host name	Fully qualified domain name
Secondary DNS server address	Optional
Public IP address for networks that use Network Address Translation (NAT)	Optional Used to access the server, usually from a different network or the Internet. Configured by using 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).
Email server name	If you do not have an email server, use `localhost`.

A series of messages are displayed as ExtremeSecurity processes the requested changes. After the requested changes are processed, the ExtremeSecurity system is automatically shutdown and restarted.

Changing the network settings of a Extreme Security Console in a multi-system deployment

- You must have a local connection to your Extreme Security Console

1 To remove managed hosts, log in to ExtremeSecurity:

`https://IP_Address_QRadar`

The **Username** is **`admin`**.

a Click the **Admin** tab.

b Click the **System and License Management** icon.

c Select the managed host that you want to remove.

d Select **Deployment Actions** > **Remove Host**.

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

2 Type the following command: `qchange_netsetup`.

3 Follow the instructions in the wizard to complete the configuration.

The following table contains descriptions and notes to help you configure the network settings.

Table 17: Description of network settings for a multi-system Extreme Security Console deployment

Network Setting	Description
Host name	Fully qualified domain name
Secondary DNS server address	Optional
Public IP address for networks that use Network Address Translation (NAT)	Optional Used to access the server, usually from a different network or the Internet. Configured by using 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).
Email server name	If you do not have an email server, use `localhost`.

After you configure the installation parameters, a series of messages are displayed. The installation process might take several minutes.

4 To re-add and reassign the managed hosts, log in to ExtremeSecurity.

   `https://IP_Address_QRadar`

   The **Username** is **`admin`**.

   a Click the **Admin** tab.
   b Click the **System and License Management** icon.
   c Click **Deployment Actions** > **Add Host**.
   d Follow the instructions in the wizard to add a host.

      Select the **Network Address Translation** option to configure a public IP address for the server. This IP address is a secondary IP address that is used to access the server, usually from a different network or the Internet. The Public IP address is often configured by using 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

5 Reassign all components that are not your Extreme Security Console to your managed hosts .

   a Click the **Admin** tab.
   b Click the **System and License Management** icon.
   c Select the host that you want to reassign.
   d Click **Deployment Actions** > **Edit Host Connection**.
   e Enter the IP address of the source host in the **Modify Connection** window.

Updating network settings after a NIC replacement

The network settings file contains one pair of lines for each NIC that is installed and one pair of lines for each NIC that was removed. You must remove the lines for the NIC that you removed and then rename the NIC that you installed.

Your network settings file might resemble the following example, where *`NAME="eth0"`* is the NIC that was replaced and *`NAME="eth4"`* is the NIC that was installed.

```
# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"

# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"

# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth4"

# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth4"
```

1 Use SSH to log in to the Extreme Networks Security Analytics product as the root user.

   The user name is `root`.

2 Type the following command:

   ```
   cd /etc/udev/rules.d/
   ```

3 To edit the network settings file, type the following command:

   ```
   vi 70-persistent-net.rules
   ```

4 Remove the pair of lines for the NIC that was replaced: `NAME=”eth0”`.

5 Rename the `Name=<eth>` values for the newly installed NIC.

   Example
   Rename `NAME="eth4"` to `NAME="eth0"`.

6 Save and close the file.

7 Type the following command: `reboot`.

11 Troubleshooting problems

Review the following table to help you or customer support resolve a problem.

Table 18: Troubleshooting actions to prevent problems

Action	Description
Apply all known fix packs, service levels, or program temporary fixes (PTF).	A product fix might be available to fix the problem.
Ensure that the configuration is supported.	Review the software and hardware requirements.
Look up error message codes by selecting the product from the IBM® Support Portal (http://www.ibm.com/support/entry/portal) and then typing the error message code into the **Search support** box.	Error messages give important information to help you identify the component that is causing the problem.
Reproduce the problem to ensure that it is not just a simple error.	If samples are available with the product, you might try to reproduce the problem by using the sample data.
Check the installation directory structure and file permissions.	The installation location must contain the appropriate file structure and the file permissions. For example, if the product requires write access to log files, ensure that the directory has the correct permission.
Review relevant documentation, such as release notes, tech notes, and proven practices documentation.	Search the IBM® knowledge bases to determine whether your problem is known, has a workaround, or if it is already resolved and documented.
Review recent changes in your computing environment.	Sometimes installing new software might cause compatibility issues.

If you still need to resolve problems, you must collect diagnostic data. This data is necessary for an IBM® technical-support representative to effectively troubleshoot and assist you in resolving the problem. You can also collect diagnostic data and analyze it yourself.

Related Links

ExtremeSecurity components on page 11

Troubleshooting resources

To view the video version, search for "troubleshooting" through either Google search engine or YouTube video community.

Related Links

ExtremeSecurity log files on page 62

Use the Extreme Networks Security Analytics log files to help you troubleshoot problems.

Support Portal

Use IBM® Support Portal to access all the IBM® support resources from one place. You can adjust the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM® Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos).

Find the Extreme Networks Security Analytics content that you need by selecting your products from the IBM® Support Portal (http://www.ibm.com/support/entry/portal).

Service requests

To open a service request, or to exchange information with technical support, view the IBM® Software Support Exchanging information with Technical Support page (http://www.ibm.com/software/support/exchangeinfo.html). Service requests can also be submitted directly by using the Service requests (PMRs) tool (http://www.ibm.com/support/entry/portal/Open_service_request) or one of the other supported methods that are detailed on the exchanging information page.

Fix Central

Use the pull-down menu to go to your product fixes on Fix Central (http://www.ibm.com/support/fixcentral). You might also want to view Getting started with Fix Central (http://www.ibm.com/systems/support/fixes/en/fixcentral/help/getstarted.html).

ExtremeSecurity log files

You can review the log files for the current session individually or you can collect them to review later.

Follow these steps to review the ExtremeSecurity log files.

1. To help you troubleshoot errors or exceptions, review the following log files.
   - `/var/log/qradar.log`
   - `/var/log/qradar.error`
2. If you require more information, review the following log files:
   - /var/log/qradar-sql.log
   - /opt/tomcat6/logs/catalina.out
   - /var/log/qflow.debug
3. Review all logs by selecting **Admin** > **System & License Mgmt** > **Actions** > **Collect Log Files**.

Related Links

Troubleshooting resources on page 61

Troubleshooting resources are sources of information that can help you resolve a problem that you have with a product. Many of the resource links provided can also be viewed in a short video demonstration.

Common ports and servers used by ExtremeSecurity

SSH communication on port 22

All the ports that are used by the ExtremeSecurity console to communicate with managed hosts can be tunneled, by encryption, through port 22 over SSH.

The console connects to the managed hosts using an encrypted SSH session to communicate securely. These SSH sessions are initiated from the console to provide data to the managed host. For example, the Extreme Security Console can initiate multiple SSH sessions to the Event Processor appliances for secure communication. This communication can include tunneled ports over SSH, such as HTTPS data for port 443 and Ariel query data for port 32006. Extreme Networks Security QFlow Collector that use encryption can initiate SSH sessions to Flow Processor appliances that require data.

Open ports that are not required by ExtremeSecurity

Installing additional software on your system may open ports that are not required by ExtremeSecurity. For example, you might find additional ports open in the following situations:

- When you install ExtremeSecurity on your own hardware, you may see open ports that are used by services, daemons, and programs included in Red Hat Enterprise Linux™.
- When you mount or export a network file share, you might see dynamically assigned ports that are required for RPC services, such as `rpc.mountd` and `rpc.rquotad`.
- When you install third-party backup and recovery software, such as Veritas NetBackup, you might see open ports that are required for processes such as `bpcd` and `pbx_exchange`.

If you see open ports on your system that are not listed in ExtremeSecurity documentation, refer to the vendor documentation for the other software that is installed on your system.

ExtremeSecurity port usage

WinCollect remote polling

WinCollect agents that remotely poll other Microsoft™ Windows™ operating systems might require additional port assignments.

For more information, see the Extreme Networks Security Analytics WinCollect *User Guide*.

ExtremeSecurity listening ports

The following table shows the ExtremeSecurity ports that are open in a `LISTEN` state. The `LISTEN` ports are valid only when iptables is enabled on your system. Unless otherwise noted, information about the assigned port number applies to all ExtremeSecurity products.

Table 19: Listening ports that are used by ExtremeSecurity services and components

Port	Description	Protocol	Direction	Requirement
22	SSH	TCP	Bidirectional from the Extreme Security Console to all other components.	Remote management access. Adding a remote system as a managed host. Log source protocols to retrieve files from external devices, for example the log file protocol. Users who use the command-line interface to communicate from desktops to the Console. High-availability (HA).
25	SMTP	TCP	From all managed hosts to the SMTP gateway.	Emails from ExtremeSecurity to an SMTP gateway. Delivery of error and warning email messages to an administrative email contact.
37	rdate (time)	UDP/TCP	All systems to the Extreme Security Console. Extreme Security Console to the NTP or rdate server.	Time synchronization between the Extreme Security Console and managed hosts.
111	Port mapper	TCP/UDP	Managed hosts that communicate with the Extreme Security Console. Users that connect to the Extreme Security Console.	Remote Procedure Calls (RPC) for required services, such as Network File System (NFS).
135 and dynamically allocated ports above 1024 for RPC calls.	DCOM	TCP	Bidirectional traffic between WinCollect agents and Windows™ operating systems that are remotely polled for events. Bidirectional traffic between Extreme Security Console components or Extreme Networks Security Analytics event collectors that use either Microsoft™ Security Event Log Protocol or Adaptive Log Exporter agents and Windows™ operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft™ Security Event Log Protocol, or Adaptive Log Exporter. Note: DCOM typically allocates a random port range for communication. You can configure Microsoft™ Windows™ products to use a specific port. For more information, see your Microsoft™ Windows™ documentation.

Table 19: Listening ports that are used by ExtremeSecurity services and components (continued)

Port	Description	Protocol	Direction	Requirement
137	Windows™ NetBIOS name service	UDP	Bidirectional traffic between WinCollect agents and Windows™ operating systems that are remotely polled for events. Bidirectional traffic between Extreme Security Console components or Extreme Security Event Collectors that use either Microsoft™ Security Event Log Protocol or Adaptive Log Exporter agents and Windows™ operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft™ Security Event Log Protocol, or Adaptive Log Exporter.
138	Windows™ NetBIOS datagram service	UDP	Bidirectional traffic between WinCollect agents and Windows™ operating systems that are remotely polled for events. Bidirectional traffic between Extreme Security Console components or Extreme Security Event Collectors that use either Microsoft™ Security Event Log Protocol or Adaptive Log Exporter agents and Windows™ operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft™ Security Event Log Protocol, or Adaptive Log Exporter.
139	Windows™ NetBIOS session service	TCP	Bidirectional traffic between WinCollect agents and Windows™ operating systems that are remotely polled for events. Bidirectional traffic between Extreme Security Console components or Extreme Security Event Collectors that use either Microsoft™ Security Event Log Protocol or Adaptive Log Exporter agents and Windows™ operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft™ Security Event Log Protocol, or Adaptive Log Exporter.

Table 19: Listening ports that are used by ExtremeSecurity services and components (continued)

Port	Description	Protocol	Direction	Requirement
162	NetSNMP	UDP	ExtremeSecurity managed hosts that connect to the Extreme Security Console. External log sources to Extreme Security Event Collectors.	UDP port for the NetSNMP daemon that listens for communications (v1, v2c, and v3) from external log sources. The port is open only when the SNMP agent is enabled.
199	NetSNMP	TCP	ExtremeSecurity managed hosts that connect to the Extreme Security Console. External log sources to Extreme Security Event Collectors.	TCP port for the NetSNMP daemon that listens for communications (v1, v2c, and v3) from external log sources. The port is open only when the SNMP agent is enabled.
427	Service Location Protocol (SLP)	UDP/TCP		The Integrated Management Module uses the port to find services on a LAN.
443	Apache/HTTPS	TCP	Bidirectional traffic for secure communications from all products to the Extreme Security Console.	Configuration downloads to managed hosts from the Extreme Security Console. ExtremeSecurity managed hosts that connect to the Extreme Security Console. Users to have log in access to ExtremeSecurity. Extreme Security Console that manage and provide configuration updates for WinCollect agents.

Table 19: Listening ports that are used by ExtremeSecurity services and components (continued)

Port	Description	Protocol	Direction	Requirement
445	Microsoft™ Directory Service	TCP	Bidirectional traffic between WinCollect agents and Windows™ operating systems that are remotely polled for events. Bidirectional traffic between Extreme Security Console components or Extreme Security Event Collectors that use the Microsoft™ Security Event Log Protocol and Windows™ operating systems that are remotely polled for events. Bidirectional traffic between Adaptive Log Exporter agents and Windows™ operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft™ Security Event Log Protocol, or Adaptive Log Exporter.
514	Syslog	UDP/TCP	External network appliances that provide TCP syslog events use bidirectional traffic. External network appliances that provide UDP syslog events use uni-directional traffic. Internal syslog traffic from ExtremeSecurity hosts to the Extreme Security Console.	External log sources to send event data to ExtremeSecurity components. Syslog traffic includes WinCollect agents, event collectors, and Adaptive Log Exporter agents capable of sending either UDP or TCP events to ExtremeSecurity.
762	Network File System (NFS) mount daemon (mountd)	TCP/UDP	Connections between the Extreme Security Console and NFS server.	The Network File System (NFS) mount daemon, which processes requests to mount a file system at a specified location.
1514	Syslog-ng	TCP/UDP	Connection between the local Event Collector component and local Event Processor component to the syslog-ng daemon for logging.	Internal logging port for syslog-ng.
2049	NFS	TCP	Connections between the Extreme Security Console and NFS server.	The Network File System (NFS) protocol to share files or data between components.
2055	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the Extreme Networks Security QFlow Collector.	NetFlow datagram from components, such as routers.

Table 19: Listening ports that are used by ExtremeSecurity services and components (continued)

Port	Description	Protocol	Direction	Requirement
2375	Docker command port	TCP	Internal communications. This port is not available externally.	Used to manage ExtremeSecurity application framework resources.
3389	Remote Desktop Protocol (RDP) and Ethernet over USB is enabled	TCP/UDP		If the Microsoft™ Windows™ operating system is configured to support RDP and Ethernet over USB, a user can initiate a session to the server over the management network. This means the default port for RDP, 3389 must be open.
3900	Integrated Management Module remote presence port	TCP/UDP		Use this port to interact with the ExtremeSecurity console through the Integrated Management Module.
4333	Redirect port	TCP		This port is assigned as a redirect port for Address Resolution Protocol (ARP) requests in ExtremeSecurity offense resolution.
5432	Postgres	TCP	Communication for the managed host that is used to access the local database instance.	Required for provisioning managed hosts from the **Admin** tab.
6514	Syslog	TCP	External network appliances that provide encrypted TCP syslog events use bidirectional traffic.	External log sources to send encrypted event data to ExtremeSecurity components.
6543	High-availability heartbeat	TCP/UDP	Bidirectional between the secondary host and primary host in an HA cluster.	Heartbeat ping from a secondary host to a primary host in an HA cluster to detect hardware or network failure.

Table 19: Listening ports that are used by ExtremeSecurity services and components (continued)

Port	Description	Protocol	Direction	Requirement
7676, 7677, and four randomly bound ports above 32000.	Messaging connections (IMQ)	TCP	Message queue communications between components on a managed host.	Message queue broker for communications between components on a managed host. Ports 7676 and 7677 are static TCP ports, and four extra connections are created on random ports. For more information about finding randomly bound ports, see Viewing IMQ port associations on page 72.
7777, 7778, 7779, 7780, 7781, 7782, 7783, 7788, 7790, 7791, 7792, 7793, 7795, 7799, and 8989.	JMX server ports	TCP	Internal communications. These ports are not available externally.	JMX server (Java™ Management Beans) monitoring for all internal QRadar® processes to expose supportability metrics. These ports are used by ExtremeSecurity support.
7789	HA Distributed Replicated Block Device (DRBD)	TCP/UDP	Bidirectional between the secondary host and primary host in an HA cluster.	Distributed Replicated Block Device (DRBD) used to keep drives synchronized between the primary and secondary hosts in HA configurations.
7800	Apache Tomcat	TCP	From the Event Collector to the Extreme Security Console.	Real-time (streaming) for events.
7801	Apache Tomcat	TCP	From the Event Collector to the Extreme Security Console.	Real-time (streaming) for flows.
7803	Apache Tomcat	TCP	From the Event Collector to the Extreme Security Console.	Anomaly detection engine port.
7804	QRM Arc builder	TCP	Internal control communications between ExtremeSecurity processes and ARC builder.	This port is used for Risk Manager only. It is not available externally.
8000	Event Collection service (ECS)	TCP	From the Event Collector to the Extreme Security Console.	Listening port for specific Event Collection Service (ECS).
8001	SNMP daemon port	UDP	External SNMP systems that request SNMP trap information from the Extreme Security Console.	UDP listening port for external SNMP data requests.
8005	Apache Tomcat	TCP	Internal communications. Not available externally.	Open to control tomcat. This port is bound and only accepts connections from the local host.

Table 19: Listening ports that are used by ExtremeSecurity services and components (continued)

Port	Description	Protocol	Direction	Requirement
8009	Apache Tomcat	TCP	From the HTTP daemon (HTTPd) process to Tomcat.	Tomcat connector, where the request is used and proxied for the web service.
8080	Apache Tomcat	TCP	From the HTTP daemon (HTTPd) process to Tomcat.	Tomcat connector, where the request is used and proxied for the web service.
8413	WinCollect agents	TCP	Bidirectional traffic between WinCollect agent and Extreme Security Console.	This traffic is generated by the WinCollect agent and communication is encrypted. It is required to provide configuration updates to the WinCollect agent and to use WinCollect in connected mode.
9090	XForce IP Reputation database and server	TCP	Internal communications. Not available externally.	Communications between ExtremeSecurity processes and the XForce Reputation IP database.
9913 plus one dynamically assigned port	Web application container	TCP	Bidirectional Java™ Remote Method Invocation (RMI) communication between Java™ Virtual Machines	When the web application is registered, one additional port is dynamically assigned.
9995	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the QFlow Collector.	NetFlow datagram from components, such as routers.
9999	Extreme Networks Security Vulnerability Manager processor	TCP	Unidirectional from the scanner to the appliance running the Extreme Security Vulnerability Manager processor	Used for Extreme Security Vulnerability Manager (QVM) command information. This port is only used when QVM is enabled.
10000	ExtremeSecurity web-based, system administration interface	TCP/UDP	User desktop systems to all ExtremeSecurity hosts.	In ExtremeSecurity V7.2.5 and earlier, this port is used for server changes, such as the hosts root password and firewall access. Port 10000 is disabled in V7.7.2.6.
10101, 10102	Heartbeat command	TCP	Bidirectional traffic between the primary and secondary HA nodes.	Required to ensure that the HA nodes are still active.

Table 19: Listening ports that are used by ExtremeSecurity services and components (continued)

Port	Description	Protocol	Direction	Requirement
15433	Postgres	TCP	Communication for the managed host that is used to access the local database instance.	Used for Extreme Security Vulnerability Manager (QVM) configuration and storage. This port is only used when QVM is enabled.
23111	SOAP web server	TCP		SOAP web server port for the Event Collection Service (ECS).
23333	Emulex Fibre Channel	TCP	User desktop systems that connect to ExtremeSecurity appliances with a Fibre Channel card.	Emulex Fibre Channel HBAnywhere Remote Management service (elxmgmt).
32004	Normalized event forwarding	TCP	Bidirectional between ExtremeSecurity components.	Normalized event data that is communicated from an off-site source or between Extreme Security Event Collectors.
32005	Data flow	TCP	Bidirectional between ExtremeSecurity components.	Data flow communication port between Extreme Security Event Collectors when on separate managed hosts.
32006	Ariel queries	TCP	Bidirectional between ExtremeSecurity components.	Communication port between the Ariel proxy server and the Ariel query server.
32007	Offense data	TCP	Bidirectional between ExtremeSecurity components.	Events and flows contributing to an offense or involved in global correlation.
32009	Identity data	TCP	Bidirectional between ExtremeSecurity components.	Identity data that is communicated between the passive Vulnerability Information Service (VIS) and the Event Collection Service (ECS).
32010	Flow listening source port	TCP	Bidirectional between ExtremeSecurity components.	Flow listening port to collect data from Extreme Security QFlow Collectors.
32011	Ariel listening port	TCP	Bidirectional between ExtremeSecurity components.	Ariel listening port for database searches, progress information, and other associated commands.

Table 19: Listening ports that are used by ExtremeSecurity services and components (continued)

Port	Description	Protocol	Direction	Requirement
32000-33999	Data flow (flows, events, flow context)	TCP	Bidirectional between ExtremeSecurity components.	Data flows, such as events, flows, flow context, and event search queries.
40799	PCAP data	UDP	From Juniper Networks SRX Series appliances to ExtremeSecurity.	Collecting incoming packet capture (PCAP) data from Juniper Networks SRX Series appliances. Note: The packet capture on your device can use a different port. For more information about configuring packet capture, see your Juniper Networks SRX Series appliance documentation.
ICMP	ICMP		Bidirectional traffic between the secondary host and primary host in an HA cluster.	Testing the network connection between the secondary host and primary host in an HA cluster by using Internet Control Message Protocol (ICMP).

Viewing IMQ port associations

Several ports used by Extreme Networks Security Analytics allocate additional random port numbers. For example, Message Queues (IMQ) open random ports for communication between components on a managed host. You can view the random port assignments for IMQ using telnet to connect to the local host and doing a look up on the port number.

Random port associations are not static port numbers. If a service is restarted, the ports generated for the service are reallocated and the service is provided with a new set of port numbers.

1 Using SSH, log in to the Extreme Security Console as the root user.
2 To display a list of associated ports for the IMQ messaging connection, type the following command:

```
telnet localhost 7676
```

```
telnet localhost 7677
```

3 If no information is displayed, press the Enter key to close the connection.

Searching for ports in use by ExtremeSecurity

1. Using SSH, log in to your Extreme Security Console, as the root user.
2. To display all active connections and the TCP and UDP ports on which the computer is listening, type the following command:

   ```
   netstat -nap
   ```

3. To search for specific information from the netstat port list, type the following command:

   ```
   netstat -nap | grep port
   ```

   Examples

   - To display all ports that match 199, type the following command:

     ```
     netstat -nap | grep 199
     ```

   - To display information on all listening ports, type the following command:

     ```
     netstat -nap | grep LISTEN
     ```

ExtremeSecurity public servers

Public servers

This table lists descriptions for the IP addresses or host names that ExtremeSecurity accesses.

Table 20: Public servers that ExtremeSecurity must access

IP address or hostname	Description
194.153.113.31	Extreme Networks Security Vulnerability Manager DMZ scanner
194.153.113.32	Extreme Security Vulnerability Manager DMZ scanner
qmmunity.q1labs.com	ExtremeSecurity auto-update server. For more information about auto-update servers, see www.ibm.com/support (http://www-01.ibm.com/support/docview.wss?uid=swg21958881).
www.iss.net	Extreme Security X-Force Threat Intelligence Threat Information Center dashboard item
update.xforce-security.com	X-Force Threat Feed update server
license.xforce-security.com	X-Force Threat Feed licensing server

RSS feeds for ExtremeSecurity products

The following list describes the requirements for RSS feeds that ExtremeSecurity uses. Copy URLs into a text editor and remove page breaks before pasting into a browser.

Table 21: RSS feeds

Title	URL	Requirements
Security Intelligence	http://feeds.feedburner.com/SecurityIntelligence	ExtremeSecurity and an Internet connection
Security Intelligence Vulns / Threats	http://securityintelligence.com/topics/vulnerabilities-threats/feed	ExtremeSecurity and an Internet connection
IBM® My Notifications	http://www-945.events.ibm.com/systems/support/myfeed/xmlfeeder.wss?feeder.requid=feeder.create_feed&feeder.feedtype=RSS&feeder.uid=270006EH0R&feeder.subscrid=S14b5f284d32&feeder.subdefkey=swgother&feeder.maxfeed=25	ExtremeSecurity and an Internet connection
Security News	http://*IP_address_of_QVM_processor*:8844/rss/research/news.rss	Extreme Networks Security Vulnerability Manager processor is deployed
Security Advisories	http://*IP_address_of_QVM_processor*:8844/rss/research/advisories.rss	Vulnerability Manager processor is deployed
Latest Published Vulnerabilities	http://*IP_address_of_QVM_processor*:8844/rss/research/vulnerabilities.rss	Vulnerability Manager processor deployed
Scans Completed	http://*IP_address_of_QVM_processor*:8844/rss/scanresults/completedScans.rss	Vulnerability Manager processor is deployed
Scans In Progress	http://*IP_address_of_QVM_processor*:8844/rss/scanresults/runningScans.rss	Vulnerability Manager processor is deployed

Index