



Extreme Networks Security Upgrade Guide

Copyright © 2016 All rights reserved.

Legal Notice

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

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

Trademarks

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

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

For additional information on Extreme Networks trademarks, please see:

www.extremenetworks.com/company/legal/trademarks

Support

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

For information, contact:

Extreme Networks, Inc.

145 Rio Robles

San Jose, California 95134

USA

Table of Contents

Introduction to Upgrading ExtremeSecurity Software.....	4
Text Conventions.....	4
Providing Feedback to Us.....	5
Getting Help.....	5
Related Publications.....	6
Chapter 1: Preparation for the upgrade	8
Firmware update.....	8
Software version requirements for upgrades.....	8
Memory and disk space requirements.....	9
Supported web browsers	11
Upgrade priority order in distributed deployments.....	12
Upgrades in HA deployments.....	12
Chapter 2: Upgrading ExtremeSecurity products.....	13
Clearing the Java™ cache and web browser cache after upgrades.....	14
Index.....	15



Introduction to Upgrading ExtremeSecurity Software

Information about upgrading Extreme Networks Security Analytics applies to Extreme SIEM, Extreme Networks Security Log Manager products.

Intended audience

System administrators who are responsible for upgrading Extreme Networks Security Analytics systems must be familiar with network security concepts and device configurations.

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.



Table 1: Notice Icons (continued)




Icon	Notice Type	Alerts you to...
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
	New	This command or section is new for this release.

Table 2: Text Conventions

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

Providing Feedback to Us

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

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

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

Getting Help

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

- **Global Technical Assistance Center (GTAC) for Immediate Support**
 - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

- **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- **GTAC Knowledge** — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- **The Hub** — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- **Support Portal** — Manage cases, downloads, service contracts, product licensing, and training and certifications.

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

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

Related Publications

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

ExtremeSecurity Analytics

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

- *ExtremeSecurity Managing Log Sources Guide*
- *ExtremeSecurity Offboard Storage Guide*
- *ExtremeSecurity Release Note*
- *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 Preparation for the upgrade

Firmware update

Software version requirements for upgrades

Memory and disk space requirements

Supported web browsers

Upgrade priority order in distributed deployments

Upgrades in HA deployments

Important



When you upgrade to ExtremeSecurity V7.7.2.6 and later releases, the SSH keys on every managed host are replaced. If you are connecting to or from a ExtremeSecurity managed host and you are using key-based authentication, do not remove or alter the SSH keys. Removing or altering the keys might disrupt communication between the ExtremeSecurity Console and the managed hosts, which can result in lost data.

Firmware update

For more information about updating firmware, see [Firmware update](#).

Software version requirements for upgrades

Ensure that the following software requirements are met:

- ExtremeSecurity version 7.2.4983526 or later must be installed.

You can check the software version in the software by clicking **Help > About**.

Important



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

Upgrade paths

Applying fix packs before you upgrade

Before you upgrade, you can apply fixes (fix pack) to your existing software. Download the fix pack from [IBM® Fix Central](http://www.ibm.com/support/fixcentral) (www.ibm.com/support/fixcentral) and follow the instructions in the release notes document to install it.

ExtremeSecurity is pre-configured for automatic, weekly updates. You can view the pending updates in the **Updates** window on the **Admin tab**.

Single step and multiple step upgrade paths

For some ExtremeSecurity software versions, you can upgrade directly to the most current ExtremeSecurity version. To upgrade to ExtremeSecurity version V7.7.2.7 in one step, you must have ExtremeSecurity version 7.2.4.983526 or later installed. When you upgrade from ExtremeSecurity version 7.2.4.983526 or later, pre-tests identify any potential upgrade issues, and you are returned to the software level that you started from if you encounter upgrade errors. Also, in high-availability deployments, the secondary host upgrades before the primary to maximize up-time.

For older versions of ExtremeSecurity, you might be required to upgrade to an interim version before you upgrade to the most current version of ExtremeSecurity.

Use the following table to help you determine your upgrade path and note any special considerations.

Table 3: Supported upgrade paths for ExtremeSecurity products

Current* version	Step 1	Step 2	Step 3
7.1 (MR2) (7.1.0.501605) or later	7.2.4 (SFS)		
7.1 GA to 7.1 (MR1) Patch 3 (7.1.0.380596 to 7.1.0.495292)	7.1 MR2 Patch 2 (7.1.0.599086) (SFS)	7.2.4 (SFS)	
7.0 (MR5) to 7.0 (MR5) Patch 7 (7.0.0.301503 to 7.0.0.672904)	7.1 MR2 Patch 2 (7.1.0.599086) (ISO)	7.2.4 (SFS)	
7.0 GA to 7.0 MR4 Patch 2 (7.0.0.167618 to 7.0.0.276729)	7.0 MR5 (7.0.0.301503) (SFS)	7.1 MR2, (7.1.0.599086) (ISO)	7.2.4 (SFS)

Memory and disk space requirements

ExtremeSecurity memory requirements

The following table describes the minimum and suggested memory requirements for ExtremeSecurity appliances. The minimum memory requirement defines the amount of memory that is required by the software features. The suggested memory requirements include the amount of memory that is required by the current software features and extra memory for possible future capabilities. Appliances that have less than the suggested appliance memory might experience performance issues during periods of excessive event and flow traffic.

Table 4: Minimum and optional memory requirements for ExtremeSecurity appliances

Appliance	Minimum memory requirement	Suggested memory requirement
QFlow Collector 1201	6 GB	6 GB
QFlow Collector 1202	6 GB	6 GB
QFlow Collector Virtual 1299 without ExtremeSecurity Vulnerability Scanner	2 GB	2 GB

Table 4: Minimum and optional memory requirements for ExtremeSecurity appliances (continued)

Appliance	Minimum memory requirement	Suggested memory requirement
QFlow Collector Virtual 1299 with ExtremeSecurity Vulnerability Scanner	6 GB	6 GB
QFlow Collector 1301	6 GB	6 GB
QFlow Collector 1310	6 GB	6 GB
ExtremeSecurity Event Collector 1501	12 GB	16 GB
ExtremeSecurity Event Collector Virtual 1599	12 GB	16 GB
ExtremeSecurity Event Processor 1601	12 GB	48 GB
ExtremeSecurity Event Processor 1605	12 GB	48 GB
ExtremeSecurity Event Processor 1624	64 GB	64 GB
ExtremeSecurity Event Processor 1628	128 GB	128 GB
ExtremeSecurity Event Processor Virtual 1699	12 GB	48 GB
ExtremeSecurity Flow Processor 1701	12 GB	48 GB
ExtremeSecurity Flow Processor 1705	12 GB	48 GB
ExtremeSecurity Flow Processor 1724	64 GB	64 GB
ExtremeSecurity Flow Processor 1728	128 GB	128 GB
ExtremeSecurity Flow Processor Virtual 1799	12 GB	48 GB
ExtremeSecurity Event and Flow Processor 1805	12 GB	48 GB
ExtremeSecurity Event and Flow Processor 1824	64 GB	64 GB
ExtremeSecurity Event and Flow Processor 1828	128 GB	128 GB
ExtremeSecurity SIEM 2100	24 GB	24 GB
ExtremeSecurity SIEM 2100 Light	24 GB	24 GB
ExtremeSecurity SIEM 3100	24 GB	48 GB
ExtremeSecurity SIEM 3105	24 GB	48 GB
ExtremeSecurity SIEM 3124	64 GB	64 GB
ExtremeSecurity SIEM 3128	128 GB	128 GB
ExtremeSecurity SIEM Virtual 3199	24 GB	48 GB
Log Manager 1605	12 GB	48 GB
Log Manager 1624	64 GB	64 GB
Log Manager 1628	128 GB	128 GB
Log Manager 2100	24 GB	24 GB
Log Manager 3105	24 GB	48 GB

Table 4: Minimum and optional memory requirements for ExtremeSecurity appliances (continued)

Appliance	Minimum memory requirement	Suggested memory requirement
Log Manager 3124	64 GB	64 GB
Log Manager 3128	128 GB	128 GB
Log Manager 3199	24 GB	48 GB

Other memory requirements

If the following conditions are met, extra memory requirements might be required:

- If you plan to enable payload indexing, your system requires a minimum of 24 GB of memory. However, 48 GB of memory is suggested.
- If you install ExtremeSecurity software on your own hardware, your system requires a minimum of 24 GB of memory.

Disk space requirements

The following table describes the minimum requirements for free disk space:

Table 5: Disk space requirements for ExtremeSecurity

Partition	Free space requirement
/	3 GB or 10 GB ¹
/store	4 GB
/var/log	500 MB
/store/tmp	800 MB

¹If your appliance has less than 8 GB of available swap space or 5 GB of memory, the root (/) partition requires 10 GB of drive space. Otherwise, appliances require a minimum of 3 GB of disk space on the root partition.

Restriction



If your Extreme Networks Security QFlow Collector appliances have less than an 80 GB of available disk space, you must install the most current software version. For more information, see the *Installation Guide* for your product.

The upgrade pretest determines whether a partition includes enough free space to complete an upgrade. Before you can upgrade, you must free up sufficient disk space on the partition that is defined in the pretest error message.

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

Upgrade priority order in distributed deployments

Upgrade your ExtremeSecurity systems in the following order:

- 1 Console
- 2 The following ExtremeSecurity systems can be upgrade concurrently:
 - Event Processors
 - Extreme Security Event Collectors
 - Flow Processors
 - QFlow Collectors

Upgrades in HA deployments

If the HA cluster is disconnected, or you want to add a new secondary HA host, you must reinstall ExtremeSecurity on the secondary HA. For more information about reinstalling software, see the *Installation Guide* for your system. After you reinstall the secondary HA host, log in to the user interface to reconnect or to create a new HA cluster.



Important

Disk replication and failover are disabled until the primary and secondary hosts synchronize and the `needs_upgrade` or `failed` status is cleared from the secondary host.

After you upgrade the secondary host, you might be required to restore the configuration of the secondary host. For more information about restoring a failed host, see the *Administration Guide* for your product.

2 Upgrading ExtremeSecurity products

Clearing the Java cache and web browser cache after upgrades

Ensure that you take the following precautions:

- Back up your data, and confirm that backups are complete before you begin the upgrade.

For more information about backup and recovery, see the *Administration Guide* for your product.

- To avoid access errors in your log file, close all open ExtremeSecurity product sessions.
- Ensure that you have sufficient RAM.

During the upgrade from versions 7.1.x to 7.2.x, a system pretest checks that the minimum amount of RAM is available. If there is not enough RAM, the upgrade stops.

- If your deployment includes offboard storage solutions, you must disconnect your offboard storage.

After you complete the upgrade, you can remount your external storage solutions. For more information, see the *ExtremeSecurity Offboard Storage Guide*.

- 1 Download the `<QRadar_patchupdate>.sfs` file from the [Extreme Networks Support Portal](#).
- 2 Use SSH to log in to your system as the root user.
- 3 Copy the patch file to the `/tmp` directory or to another location that has sufficient disk space.



Important

Do not copy the file to an existing ExtremeSecurity system directory, such as `/store` or `/root`.

- 4 To create the `/media/updates` directory, type the following command:

```
mkdir -p /media/updates
```

- 5 Change to the directory where you copied the patch file.

- 6 To mount the patch file to the `/media/updates` directory, type the following command:

```
mount -o loop -t squashfs <QRadar_patchupdate>.sfs /media/updates/
```

- 7 To run the patch installer, type the following command:

```
/media/updates/installer
```

The first time that you run the patch installer script, there might be a delay before the first patch installer menu is displayed.

- 8 Provide answers to the pre-patch questions based on your ExtremeSecurity deployment.

- 9 Using the patch installer, apply the software fix to all systems in your deployment.

The patch installer menu lists the following options.

- Console
- All

If you select **All**, the software fix is applied to the ExtremeSecurity Console first, and then to all managed hosts. If you select **Console**, the software fix is applied only to the ExtremeSecurity Console. After the software fix is applied to the ExtremeSecurity Console, the menu lists the remaining managed hosts, and the **All** option.

If your SSH session is disconnected while the upgrade is in progress, the upgrade continues. When you reopen your SSH session and rerun the installer, the installation resumes.

- 10 After the upgrade is complete, unmount the software update by using the following command:

```
umount /media/updates
```

- 1 Perform an automatic update to ensure that your configuration files contain the latest network security information. For more information, see the *Extreme SIEM Administration Guide*.
- 2 Clear your Java™ cache and your web browser cache. After you upgrade ExtremeSecurity, the **Vulnerabilities** tab might not be displayed. To use Vulnerability Manager after you upgrade, you must upload and allocate a valid license key. For more information, see the *Administration Guide* for your product.

Clearing the Java™ cache and web browser cache after upgrades

The Java™ Runtime Environment version 1.7 must be installed on the desktop system that you use to view the user interface.

- 1 To clear the Java™ cache, open the Windows™ **Control Panel** search and enter `Java Control Panel`.
 - a View the **Temporary Internet Files**.
 - b Delete all of the ExtremeSecurity Deployment Editor entries.
- 2 To clear you web browser cache, ensure that you have only one instance of your web browser open, and then clear the cache.
- 3 Log in to ExtremeSecurity by typing the IP address of the ExtremeSecurity system into a web browser:

```
https://IP Address
```

The default user name is **admin**.

Index

C

- cache
 - clearing after upgrade 14
- clusters
 - upgrading 12
- Conventions
 - notice icons 4
 - text 4
- customer support
 - contact information 4

D

- distributed deployments
 - upgrade sequence 12
- documentation 4
- Documentation feedback 5
- Documentation, related 6

F

- Fix Central
 - installing fix packs 8, 9
- fix packs
 - installing before upgrade 8, 9

H

- HA, see high availability
- high availability
 - upgrading systems 12

J

- Java cache
 - clearing after upgrade 14

M

- memory and disk space requirements for upgrades
 - hardware 9, 11

N

- network administrator
 - description 4

P

- patches
 - installing before upgrade 8, 9
- primary systems
 - upgrading 12

S

- software versions
 - requirements 8
- Support 5

T

- technical library
 - documentation 4
- Technical support
 - contacting 5

U

- updates
 - configuring 8, 9
- upgrade paths
 - supported 8, 9
- upgrades
 - disk space requirements 9, 11
 - memory requirements 9, 11
- upgrading
 - overview 8
 - priority order 12
 - steps 13

W

- web browser
 - clearing the cache after upgrade 14
- web browser cache
 - clearing after upgrade 14