Extreme Networks SIEM Release Notes

V7.7.1.2 Patch 12

9038355-17

Published March 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: www.extremenetworks.com/documentation/

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

Table of Contents

Preface

Text Conventions

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

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
☞	General Notice	Helpful tips and notices for using the product.
📝	Note	Important features or instructions.
⚠	Caution	Risk of personal injury, system damage, or loss of data.
⚡	Warning	Risk of severe personal injury.
New	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 theExtreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at internalinfodev@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks Global Technical Assistance Center using one of the following methods:

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

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

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

Related Publications

The Extreme Security & Threat Protection product documentation listed below can be downloaded from http://documentation.extremenetworks.com.

Extreme Security Analytics

- *Extreme Security Release Notes*
- *Extreme Networks SIEM Administration Guide*
- *Extreme Networks SIEM Getting Started Guide*
- *Extreme Networks SIEM High Availability Guide*
- *Extreme Networks SIEM Users Guide*
- *Extreme Networks SIEM Tuning Guide*
- *Extreme Networks Security API Reference Guide*
- *Extreme Networks Security Ariel Query Language Guide*
- *Extreme Networks Security Application Configuration Guide*

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

Extreme Security Threat Protection

- *Extreme Security Intrusion Prevention System Hardware Replacement Guide*
- *Extreme Security Threat Protection Downloads & Release Notes*
- *Extreme Security Threat Protection Installation and Configuration Guide*

1 Extreme SIEM V7.7.1.2 Patch 12 Release Notes

Extreme Networks is pleased to introduce the Extreme Networks Security Information and Event Manager (SIEM) 7.7.1.

Note
We recommend that you review this document prior to installing or upgrading this product.

If your deployment is installed with Extreme SIEM 7.7.1, you can install fix pack 7.7.1 Build 1104434.

Product Firmware Support

Status	Firmware Version	Product Type	Release Date
Current Version	7.7.1 Build 1104434	Customer Software	2/16/2016
Previous Version	7.7.1 Build 1098887	Customer Software	8/14/2015
Previous Version	7.7.1 Build 1036373	Customer Software	2/17/2015
Previous Version	7.7.1 Build 989724	Customer Software	1/7/2015
Previous Version	7.7.1 Build 962104	Customer Software	10/24/2014
Previous Version	7.7.1 Build 880308	Customer Software	7/11/2014
Previous Version	7.7.1 Build 809045	Customer Software	4/21/2014
Previous Version	7.7.1 Build 770365	Customer Software	3/6/2014
Previous Version	7.7.1 Build 682020	Customer Software	11/22/2013
Previous Version	7.7.1 Build 599086	Customer Software	7/29/2013
Previous Version	7.7.1 Build 581477	Customer Software	6/27/2013
Previous Version	7.7.1 MR2	Customer Software	5/7/2013
Previous Version	7.7.1 Build 495292	Customer Software	3/15/2013
Previous Version	7.7.1 Build 457882	Customer Software	2/8/2013
Previous Version	7.7.1 Build 449508	Customer Software	2/8/2013
Previous Version	7.7.1 MR1	Customer Software	2/8/2013
Previous Version	7.7.1	Customer Software	12/17/2012

Installation Notes

To install this patch, refer to Patch Installation Instructions on page 9.

You must wait for the Console to upgrade, reboot, and complete starting up prior to upgrading your other Extreme SIEM systems. If not, you may receive a “connection refused” error when upgrading the other systems, as they attempt to contact the Console prior to starting the upgrade. To check that your

Console is online, try to log in to the web interface. Once you can log in to the web interface, you can begin the upgrade of the other systems.

For complete software installation instructions, refer the *Extreme Networks Security Installation Guide*.

Issues Resolved in V7.7.1.2 Patch 12

Number	Description
Security Bulletin	Cookie missing HTTPOnly Flag.
Security Bulletin	Apache Commons Java object deserialization.
Security Bulletin	Session Expiry not enforced by default.
Security Bulletin	Remote Code Execution in Extreme SIEM Web User Interface.
Security Bulletin	Cross Site Scripting in Extreme SIEM Web User Interface.
Security Bulletin	SSH Private Key Exposure.
Security Bulletin	Cross Site Scripting in Extreme SIEM Web User Interface.

Known Issues

In this version, administrators who attempt to add a Flow Source from a flowlog file without typing a directory path might receive an Application Error in the user interface. All flowlog configurations that reference a flowlog file must include a path to a file that references the location of the flowlog file on the Extreme SIEM appliance.

To resolve this issue, the administrator can close the Flow Source Management window and add the Flow Sources a second time from the Admin tab. In the Add Flow Source configuration, the administrator must specify a valid path to either the flowlog file or a list of Flowlog Files before attempting to Save, such as `@/store/flowlogs/flowloglist`.

2 Patch Installation Instructions

Before you begin, ensure that you take the following precautions:

- Back up your data before you begin any software upgrade. For more information about backup and recovery, see the *Extreme Networks SIEM Administration Guide*.
- To avoid access errors in your log file, close all open SIEM sessions.
- The fix pack for cannot install on a managed host that is at a different software version from the Console. All appliances in the deployment must be at the same software revision to patch the entire deployment.
- Verify that all changes are deployed on your appliances.
- The patch cannot install on appliances that have changes that are not deployed.

Fix packs are cumulative software updates to fix known software issues in your SIEM deployment. SIEM fix packs are installed by using an SFS file. The fix pack can update any appliance attached to the SIEM Console that is at the same software version as the Console.

1 Download the 771_patchupdate-7.7.1.<build_number>.sfs patch from the Extreme Networks Support Portal (http://support.extremenetworks.com/).

2 Using SSH, log in to your system as `root`.

3 Copy the patch file to the `/tmp` directory on the SIEM Console.

   Note
   If space in `/tmp` is limited, copy the patch file to another location with sufficient space.

4 Create the /media/updates directory:

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

5 Change to the directory where you copied the patch file: `cd <directory>`

   For example: `cd /tmp`

6 Mount the patch file to the /media/updates directory:

```
mount -o loop -t squashfs 771_patchupdate-7.7.1. <build_number>.sfs /
media/updates/
```

7 Run the patch installer:

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

   Note
   The first time you use the patch installer script, expect a delay before the first patch installer menu is displayed.

8 Using the patch installer, select **all**.

The **all** option updates the software on all systems in your deployment. In HA deployments, primary HA appliances are patched and replicate the patch update to the secondary HA appliance.

If you do not select the **all** option, you copy the fix to each appliance in your deployment and install the fix pack. If you manually install fix packs in your deployment, you must update your appliances in the following order:

1 Console
2 Event Processors
3 Event Collectors
4 Flow Processors
5 Flow Collectors

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

9 Clear the browser cache before logging in to the Console.

A summary of the fix pack installation advises you of any managed host that were not updated. If the fix pack fails to update a managed host, you can copy the fix pack to the host and run the installation locally.

3 System Requirements

SIEM v7.7.1 is supported on the following appliances:

SIEM Appliances

DSIMBA7-CON	SIEM Console Manager, requires a minimum of at least one processor appliance (Event and/or Flow processor).
DSIMBA7-GB SIEM	Small Office appliance supporting 200 EPS, 15,000 flows per minute (upgradable to 30,000 flows per minute), 750 log sources.
DSIMBA7-LU SIEM	Large Enterprise appliance supporting 2500 EPS, 100K flows, and 750 log sources. Upgradeable to support a maximum of 5,000 EPS and 200K flows.
DSIMBA7-LX SIEM	Enterprise appliance supporting 1000 EPS, 25,000 flows, and 750 log sources. Upgradeable to support a maximum of 50,000 flows.
DSIMBA7-EVP	SIEM Event Processor and Storage Appliance with 5000 EPS. Upgradeable to support a maximum of 10,000 EPS.
DSIMBA7-EVP2500	SIEM Event Processor and Storage Appliance with 2500 EPS. Upgradeable to support a maximum of 10,000 EPS.
DSIMBA7-EVP-FAP	SIEM Combined Event Processor and Flow Processor
DSIMBA7-FAP	SIEM Flow Processor and Storage Appliance with 200K flows. Upgradeable to support a maximum of 600K flows.
DSIMBA7-FAP100K	SIEM Flow Processor and Storage Appliance with 100K flows. Upgradeable to support a maximum of 600K flows.
DSIMBA7-SE	SIEM Integrated Flow Sensor, supporting 1000 EPS, 25,000 flows per minute (upgradable to 50,000 flows per minute), 750 log sources.

SIEM High Availabilty Appliances

DSIMBA7-CON-HA	Provides High Availability to the DSIMBA7-CON appliance.
DSIMBA7-GB-HA	Provides High Availability to the DSIMBA7-GB appliance.
DSIMBA7-LU-HA	Provides High Availability to the DSIMBA7-LU appliance.
DSIMBA7-LX-HA	Provides High Availability to the DSIMBA7-LX appliance.
DSIMBA7-EVP-HA	Provides High Availability to the DSIMBA7-EVP appliance.
DSIMBA7-EVP2500-HA	Provides High Availability to the DSIMBA7-EVP2500 appliance.
DSIMBA7-FAP-HA	Provides High Availability to the DSIMBA7-FAP appliance.
DSIMBA7-FAP100K-HA	Provides High Availability to the DSIMBA7-FAP100K appliance.
DSIMBA7-SE-HA	Provides High Availability to the DSIMBA7-SE appliance.

SIEM Network Behavioral Flow Sensors

DSNBA7-50-TX	Behavioral Flow Sensor – 50Mbps Copper
DSNBA7-250-TX	Behavioral Flow Sensor – GE250 Copper
DSNBA7-250-SX	Behavioral Flow Sensor – GE250 Fiber
DSNBA7-1G-TX	Behavioral Flow Sensor – 1 Gb Copper
DSNBA7-1G-SX	Behavioral Flow Sensor – 1 Gb Fiber
DSNBA7-10GSR	Behavioral Flow Sensor – 10 Gb Fiber
DSNBA7-10GLR	Behavioral Flow Sensor – 10 Gb Fiber

SIEM Network Behavioral Flow High Availabilty Sensors:

DSNBA7-50TX-HA	Provides High Availability to the DSNBA7-50-TX appliance.
DSNBA7-250TX-HA	Provides High Availability to the DSNBA7-250-TX appliance.
DSNBA7-1G-TX-HA	Provides High Availability to the DSNBA7-1G-TX appliance.
DSNBA7-1G-SX-HA	Provides High Availability to the DSNBA7-1G-SX appliance.
DSNBA7-250SX-HA	Provides High Availability to the DSNBA7-250-SX appliance.
DSNBA7-10GSR-HA	Provides High Availability to the DSNBA7-10GSR appliance.
DSNBA7-10GLR-HA	Provides High Availability to the DSNBA7-10GLR appliance.

SIEM Virtual Appliances

DVSIEM	All-in-one appliance supporting 100 EPS, 15,000 flows
DVSIEM-CON	Dedicated console for distributed system
DVSIEM-EVP	Event Processor Base with 100 EPS
DVSIEM-FAP	Flow Processor Base supporting 15,000 flows
DSIMBS7-VFLOW	VFlow Collector supporting up to 10,000 flows

SIEM v7.7.1 is not supported on the following SIEM appliances:

- DSIMBA7-BFS-ME
- DSIMBA7-ME
- DSIMBA7-LE