Extreme Networks Security Analytics Release Notes

For Software Version 7.7.2.4

9035005

Published June 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

Related Publications

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

ExtremeSecurity 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*

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: 1-800-872-8440 (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

1 About these Release Notes

These release notes cover ExtremeSecurity for release V7.7.2.4, including patches. These notes cover:

- Firmware support
- Fixes
- Known Issues

For the patch upgrade procedure, see Patch Installation Instructions on page 11.

Product Firmware Support

Status	Firmware Version	Product Type	Release Date
Current Version	7.7.2.4 Build 1104465	Customer Software	6/29/2016
Previous Version	7.7.2.4 Build 1040318	Customer Software	2/23/2015
Prevous Version	7.7.2.4 Build 1012120	Customer Software	2/3/2015
Previous Version	7.7.2.4 Build 988458	Customer Software	1/8/2015

System Requirements

ExtremeSecurity V7.7.2.4 is supported on the following appliances:

SIEM Appliances

SIMBA7-CONSIEM	Console Manager, requires a minimum of at least one processor appliance (Event and/or Flow processor)
DSIMBA7-GBSIEM	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, 25,000flows, 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	SIEMIntegrated Flow Sensor, supporting 1000 EPS, 25,000 flows per minute (upgradable to 50,000 flows per minute), 750 log sources.

SIEM High Availability 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 – 50 Mbps 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 Behavior Flow High Availablity 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-VFLOWV	Flow Collector supporting up to 10,000 flows.

ExtremeSecurity V7.7.2.4 is not supported on the following appliances:

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

Known Restrictions and Limitations

- These error messages may appear in qradar.log for SIEM console associated EVP and FAP:

  Error processing configuration for database events

  Feb 9 14:58:50 ::ffff:10.54.117.204 [ariel.ariel_proxy_server] [ariel_query_1:422ac1a2-5bca-4352-b298-d4da497862c5] java.lang.NullPointerException

  Error processing configuration for database flows

  Feb 9 14:58:50 ::ffff:10.54.117.204 [ariel.ariel_proxy_server] [ariel_query_1:422ac1a2-5bca-4352-b298-d4da497862c5]

  java.lang.NullPointerException
- After reaching 300K assets, SIEM will not process/update additional assets. The following benign error messages appear in qradar.log:

  [ERROR] [NOT:0000003000][10.54.117.222/- -] [-/- -]UpdateResolutionWorker.run(): Unable to apply update 'AssetProfileUpdate FROM: IDENTITY - Interfaces: [Interface 00:01:03:97:01:1B: [Primary IP: 1.3.151.28 (17012508), Secondary IP: <None>]], Usernames: [Username: peap, Group: null, Type: OBSERVED], Properties: [Asset Property [Property Type: EXTENDED, Property Value: Switch: 10.54.25.252 SwitchPortId: ge.1.8]]]' to profile from source IDENTITY/215 .....

  com.q1labs.assetprofile.updateresolution.AssetProfileCeilingException: Unable to create new asset profile because max number of profiles (300000) has been reached.
- After creating and deploying a user, the message below appears:
  `[WARN] Got output '/opt/qradar/init/prepare_io_scheduler: line 33 : echo: write error: Invalid argument' for /sys/block/sda/queue/max_sectors_kb`
- When logged into the SIEM Console, the follow message may display:

  `TypeError: Cannot read property ‘appendChild’ of null` or

  `“Type Error: arg.parent is null”.`
- The following warning message may appear in System Notification or qradar.log:

Raid Controller Misconfiguration - Hardware Monitoring has determined that a virtual drive is misconfigured and local storage performance may be negatively impacted - WriteThrough cache policy detected on Adapter:0 Virtual Drive:0

The message may indicate that either the battery backup is dead or "Write Back" policy should be configured in the hardware RAID BIOS.

- The support contact info on the top right corner of the System Management/Administration still shows the old support email (support@enterasys.com). The new support email address is support@extremenetworks.com.
- Generating the Obsolete Environments report triggers the following java exceptions in qradar.log:

  [report_runner] [main] java.lang.IllegalStateException

  Jan 29 13:54:36 ::ffff:10.54.117.203 [report_runner] [main] at com.q1labs.frameworks.session.JPASessionDelegate.checkTX(JPASessionDelegate.java:290)

  Jan 29 13:54:36 ::ffff:10.54.117.203 [report_runner] [main] at com.q1labs.frameworks.session.JPASessionDelegate.checkTX(JPASessionDelegate.java:277)

  Jan 29 13:54:36 ::ffff:10.54.117.203 [report_runner] [main] at com.q1labs.frameworks.session.JPASessionDelegate.connection(JPASessionDelegate.java:154)

  Jan 29 13:54:36 ::ffff:10.54.117.203 [report_runner] [main] at com.q1labs.core.assetprofile.services.search.QuickSearchValidation.validateTsQuery(QuickSearchValidation.java:89).....
- For syslog events from Enterasys HiPath, you must add the Log Source manually. The received events are displayed as “Stored” status in the Low Level Category of Log Activity.
- Some error messages may appear in qradar.log when upgrading the installed patch from 7.7.1.2 to SIEM 7.7.2.4 Patch 3:

  For example:

  Jan 28 12:37:21 lu11 []: WARNING: Unexpected error forwarding to login page

  Jan 28 12:37:21 lu11 []: org.apache.jasper.JasperException: Failed to load or instantiate TagExtraInfo class: org.apache.struts.taglib.logic.IterateTeiJan 28 12:37:21 lu11 []: at org.apache.jasper.compiler.DefaultErrorHandler.jspError(DefaultErrorHandler.java:51)

  Jan 28 12:37:21 lu11 []: at org.apache.jasper.compiler.ErrorDispatcher.dispatch(ErrorDispatcher.java:409)

  Jan 28 12:37:21 lu11 []: at org.apache.jasper.compiler.ErrorDispatcher.jspError(ErrorDispatcher.java:281)

  Jan 28 12:37:21 lu11 []: at org.apache.jasper.compiler.TagLibraryInfoImpl.createTagInfo(TagLibraryInfoImpl.java:434)

  Jan 28 12:37:21 lu11 []: at org.apache.jasper.compiler.TagLibraryInfoImpl.parseTLD(TagLibraryInfoImpl.java:265

  Jan 28 12:37:21 lu11 []: WARNING: Unexpected error forwarding to login page

Jan 28 12:37:21 lu11 []: org.apache.jasper.JasperException: org.apache.jasper.JasperException: Unable to load class for JSP

Jan 28 12:37:21 lu11 []: at org.apache.jasper.servlet.JspServletWrapper.getServlet(JspServletWrapper.java:161)

Jan 28 12:37:21 lu11 []: at org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:340)

Jan 28 12:37:21 lu11 []: at org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:313)

Jan 28 12:37:21 lu11 []: at org.apache.jasper.servlet.JspServlet.service(JspServlet.java:260)

Jan 28 12:37:21 lu11 []: at javax.servlet.http.HttpServlet.service(HttpServlet.java:723)

Jan 28 12:37:21 lu11 []: at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)

Jan 28 12:38:23 ::ffff:10.54.150.11 [ariel.ariel_proxy_server] [main] com.q1labs.frameworks.core.JMXHelper: [ERROR] [NOT:0000003000][10.54.150.11/- -] [-/- -]Failed to stop connection server: service:jmx:rmi://10.54.150.11:7782/jndi/rmi://10.54.150.11:7782/jmxrmi

Jan 28 12:38:23 ::ffff:10.54.150.11 [ariel.ariel_proxy_server] [main] java.lang.IllegalStateException: Request already cancelled Jan 28 12:38:23 ::ffff:10.54.150.11 [ariel.ariel_proxy_server] [main] at sun.misc.GC$LatencyRequest.cancel(GC.java:243)

Jan 28 12:44:02 lu11 []: Jan 28, 2015 12:44:02 PM org.apache.catalina.startup.ClassLoaderFactory validateFile

Jan 28 12:44:02 lu11 []: WARNING: Problem with directory [/opt/qradar/jars/jaxb2], exists: [false], isDirectory: [false], canRead: [false] .....

- Some events are displayed as “Stored” status in the Log Activity window. For example:

  A2/A4/B2/: (Same events type) Radius packet<189>DEC 17 16:19:13 20.1.0.4-1 USER_MGR[1]: 3856 % % Radius Session-Timeout period expired for user :admin

  B3: SEC_LOG<190>Dec 17 15:45:50 20.1.2.1-1 SEC_LOG[1] User:escsu:su; Source:console; Action:"show logging default"; Status:OK

  C2: dhcp packet<190>Dec 17 16:38:06 20.1.3.2-1 DHCP_SNP[205221584]: ds_main.c(584) 2109 % %dsPacketIntercept : creating a ds binding for vlan 4093 in interface 59

  I3: SNTP packet<187>Dec 17 17:07:54 192.168.81.33-1 SNTP[151777376]: sntp_client.c(1241) 54128 %% SNTP Socket close -1
- In Log source from Enterasys or Extreme Networks products, the username field displays “N/A” and thesource and destination ports are displayed as “0”.
- If you are using Firefox version above Firefox EST 24 for the SIEM Console, error messages such as `Parse Error` and `Type Error` appear occasionally. These errors are benign. The officially supported version of Firefox for SIEM 7.7.2.4 is FF 24 ESR.

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.

You must wait for the Console to upgrade, reboot, and complete starting up prior to upgrading your other 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 login to the web interface, you can begin the upgrade of the other systems.

1 Download the 724_patchupdate-7.2.4.<build_number>.sfs patch from the **Software** tab of the Extreme SIEM downloads page (https://extranet.extremenetworks.com/downloads/Pages/SIEM.aspx).

Note
You must have a user account to access this page.

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 725_patchupdate-7.2.5. <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 displays.

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 After the patch completes and you have exited the installer, type the following command:

```
umount /media/updates
```

10 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.

2 Release Notes for ExtremeSecurity V7.7.2.4 Patch 6

If your deployment is installed with ExtremeSecurity 7.7.1.2 any patch level, you can install fix pack `7.2.4-QRADAR-QRSIEM-1104465` to update your deployment to ExtremeSecurity V7.7.2.4 Patch 6. This fix pack is the only approved software version to upgrade from ExtremeSecurity 7.7.1.2 (any patch) to the V7.7.2.4 software stream.

To install this fix pack, see Patch Installation Instructions on page 11.

This release note does not cover all of the installation messages and requirements. For information on upgrading to V7.7.2.4, see the *Extreme Networks Security Upgrade Guide*.

Resolved Issues

This is a cumulative release, meaning that installing the latest version includes all of the resolved issues identified in previous releases.

Note
Some APAR links in the table below might take 24 hours to display properly after a software release.

Table 1: Issues Resolved in V7.7.2.4 Patch 6

Number	Description
IV79451	PATCHING FROM EXTREME SECURITY 7.1.2 PATCH 11 (BUILD 1098887) OR NEWER TO EXTREME SECURITY 7.2.X FAILS DUE TO AN RPM DEPENDENCY

3 Release Notes for ExtremeSecurity V7.7.2.4 Patch 5

If your deployment is installed with ExtremeSecurity 7.7.1.2 or later, you can install fix pack `7.2.4-QRADAR-QRSIEM-1078277` and above to the latest software version. This release note does not cover all of the installation messages and requirements. For information on upgrading to V7.7.2.4, see the *Extreme Networks Security Upgrade Guide*.

To install this fix pack, see Patch Installation Instructions on page 11.

Resolved Issues

This is a cumulative release, meaning that installing the latest version includes all of the resolved issues identified in previous releases.

Note
Some APAR links in the table below might take 24 hours to display properly after a software release.

Table 2: Issues Resolved in V7.7.2.4 Patch 5

Number	Description
IV66404	QRM - ZIPTIE SERVER LOGS ARE NOT ROTATING AND MAY CAUSE THE '/' PARTITION TO RUN OUT OF DISK SPACE
IV67045	SSHAUDIT.LOG FILE IS NOT ROTATING
IV67046	THE SYSLOG-NG SERVICE IS RESTARTED DAILY ON HIGH AVAILABILITY STANDBY SYSTEMS
IV67328	**`REMOTE METHOD ERROR`** POP-UP WHEN PERFORMING AN EVENT SEARCH
IV67691	EXTREME SYSTEM LOAD DUE TO MULTIPLE DF -TP PROCESSES
IV68100	EXTREME SECURITY SYSTEM NOTIFICATION MESSAGES **SAR `MONITORING REPORT: PERCENTAGE OF SWAP USED...`** ON SYSTEMS WITH LESS THAN 24GB
IV68151	THE USER ROLE **VIEW VA DATA** RADIO BUTTON DOES NOT WORK AS EXPECTED
IV68403	DEPLOY PROCESS FAILS FOR A NEWLY ADDED MANAGED HOST WITH **ENABLE ENCRYPTION** SELECTED
IV68437	ANOMALY DETECTION ENGINE RULES CAN CAUSE SYSTEM NOTIFICATIONS: **`DISCOVERED OUT-OF-MEMORY ERROR FOR ACCUMULATOR.ACCUMULATOR`**
IV68545	DASHBOARD GRAPH LEGEND ITEMS THAT ARE DESELECTED IN A UI LOGIN SESSION APPEAR SELECTED ON SUBSEQUENT LOGINS

Table 2: Issues Resolved in V7.7.2.4 Patch 5 (continued)

Number	Description
IV68594	MANAGED SEARCH RESULTS `EXPIRES ON` DISPLAYED DATE AND TIME IS INCORRECT
IV68685	LOG SOURCES DISPLAYING `ERROR` STATUS AND `LAST EVENT TIME` UNCHANGED AFTER PATCHING EXTREME SECURITY
IV68778	EXTREME SECURITY SYSTEM NOTIFICATION `FAILED TO RESET TRAFFIC ANALYSIS ENGINE ON A CONFIG CHANGE. REASON: NULL`
IV68851	QRADAR..LOG REPORTS A NULLPOINTEREXCEPTION RELATING TO DISK MAINTENANCE
IV68853	AQL SEARCH 'RIGHT CLICK FILTER' RETURNS ERROR `UNABLE TO PARSE EXPRESSION`
IV68885	CONTENT MANAGEMENT EXPORTS AND IMPORTS CAN FAIL WHEN USING A LARGE REFERENCE SET
IV68973	SFLOW TRAFFIC CONTAINING VLAN TAGS WITH SUBSEQUENT VLAN TAGS ARENOT PARSED BY QFLOW
IV69080	DETECTED LANGUAGE FOR MICROSOFT WINDOWS EVENT LOG SOURCE MAY DISPLAY INCORRECT LANGUAGE
IV69090	PAGING IS NOT WORKING IN REFERENCE SET MANAGEMENT OR THE QVM SCAN POLICY EDIT SCREEN
IV69135	QVM: INSUFFICIENT DISK SPACE ERROR WHEN TRYING TO EXPORT SCAN RESULTS TO EITHER XML OR CSV
IV69179	NON-CONSOLE HA PRIMARY DOES NOT TIME SYNCHRONIZE WITH THE TIME SERVER, RESULTING IN DRIFT
IV69367	QVM - EXTREME SECURITY AUTOUPDATE CAN RETURN AN `INSTALLED WITH ERRORS` MESSAGE CAUSED BY MISSING QVM SQL RPMS
IV69397	EXTREME SECURITY DOES NOT LOG SIM AUDIT MESSAGES FOR FAILED AD LOGIN ATTEMPTS FOR USERIDS THAT DO NOT HAVE ACCESS TO EXTREME SECURITY
IV69494	QVM - BENIGN AUTOUPDATE FAILURE MESSAGES
IV69508	NULLPOINTEREXCEPTION ERRORS AROUND REFERENCE SET CACHES
IV69660	REPORTS AND GRAPHS MIGHT APPEAR EMPTY AFTER PATCHING TO EXTREME SECURITY V7.7.2.4
IV69729	TOMCAT OUT OF MEMORY ERROR CAN OCCUR WHEN USING REST API TO GET ALL ASSETS
IV69745	THE ECS-EP SERVICE CAN SOMETIMES BE SLOW TO RESTART CAUSING EVENT PARSING AND PERFORMANCE ISSUES
IV69749	UNABLE TO CREATE REPORT WHEN USING ADVANCED SEARCH
IV69800	APPLICATION ERROR OCCURS AND UNABLE TO VIEW TOPOLOGY IN QRM WHEN DEVICE IN TOPOLOGY CONTAINS INTERFACE WITH NO IP ADDRES

Table 2: Issues Resolved in V7.7.2.4 Patch 5 (continued)

Number	Description
IV69818	CANNOT ACCESS CONFIGURATION SOURCES MANAGEMENT SCREEN WHEN USING THE HOSTNAME
IV69819	LOGIN FAILURE WARNING ICON DISPLAYS INCORRECTLY IN SCAN RESULTS
IV69827	SHELL SHOCK SCAN TOOL NOT ADDED TO AUTHENTICATIONSCANJOBANOINT SPRING BEAN FOR CENTRALIZED CREDENTIALS
IV69899	TOP DESTINATION IPS ASSET REPORT PERFORMANCE PROBLEM
IV69942	UNEXPECTED HIGH AVAILABILITY (HA) RESYNC OCCURS AFTER PATCHING TO EXTREME SECURITY V7.7.2.4
IV69943	QUERY ERRORS WHEN USING THE UTF8 FUNCTION ON THE PAYLOAD FIELD FOR AN AQL QUERY.
IV69948	MANAGED HOSTS CAN NOT DEPLOY IF THEY ARE IN THE SAME NAT GROUP AS THE CONSOLE.
IV70492	EXTREME SECURITY DATA NODE NO LONGER BALANCES DATA LOAD AFTER A PROCESS OUT OF MEMORY OCCURANCE
IV70519	'ALPHANUMERIC IGNORE CASE' REFERENCE SET TYPE IS BROKEN IN EXTREME SECURITY V7.7.2.4 PATCH 4
IV70554	APPLICATION ERROR WHILE CREATING TOPOLOGY
IV70556	CLEAN UP AGENT MESSAGING IN THE LOGS ON `CANNOT RETRIEVE JMX PORT NUMBER FOR PROCESS`
IV70599	REFERENCE SET FILTERS ARE NOT FUNCTIONING IN V7.7.2.4 PATCH 4
IV70715	MISSPELLED WORD IN RISK SCORE ON MANAGE VULNS SCREEN
IV70816	PERFORMANCE IMPROVEMENTS ON BUILDREPORT_WINDOWS_PATCHES
IV70826	TOMCAT INSTABILITY MAY OCCUR IN AN ENVIRONMENTS WITH A LARGE NUMBER OF MANAGED HOSTS OR OTHER INBOUND CONNECTIONS
IV70882	BUFFEROVERFLOWEXCEPTION FOR COMPLEX DEVICE CONFIGURATION
IV71346	/STORE/TRANSIENT CAN FILL UP AS IT IS NOT SETUP FOR AUTOMATIC FILE CLEANUP AND MAINTENANCE
IV71523	PAYLOAD EVENT FORWARDING WITH 'PREFIX A SYSLOG HEADER IF IT IS MISSING OR INVALID' ENABLED ADDS A CORRUPTED HEADER
IV71934	MESSAGE IN QRADAR.LOG `ERROR FETCHING HOSTNAME OF DEVICE FOR ID XXXX` WHEN USING DEVICE STOPPED SENDING RULE

4 Release Notes for ExtremeSecurity V7.7.2.4 Patch 4

If your deployment is installed with ExtremeSecurity 7.7.1.2 or later, you can install fix pack `7.2.4-QRADAR-QRSIEM-1040138` and above to the latest software version. This release note does not cover all of the installation messages and requirements. For information on upgrading to V7.7.2.4, see the *Extreme Networks Security Upgrade Guide*.

To install this fix pack, see Patch Installation Instructions on page 11.

Resolved Issues

This is a cumulative release, meaning that installing the latest version includes all of the resolved issues identified in previous releases.

Note
Some APAR links in the table below might take 24 hours to display properly after a software release.

Table 3: Issues Resolved in V7.7.2.4 Patch 4

Number	Description
IV69233	REPLICATION PROCESS NO LONGER FUNCTIONING AFTER PATCHING TO EXTREME SECURITY 7.2.4.4
n/a	GLIBC VERSION UPDATE
IV66445	QVM - `QRADAR VULNERABILITY MANAGER IS IN THE PROCESS OF BEING DEPLOYED` MESSAGE ON THE VULNERABILITIES TAB
IV67112	QVM - UNABLE TO CHANGE RUN SCHEDULE TO 'MANUAL' FOR SCAN PROFILES ASSOCIATED TO AN OPERATIONAL WINDOW
IV67166	QVM - TOMCAT SERVICE RESTARTS EVERY TEN MINUTES
IV67458	RULES THAT COMPARE A NUMERICALLY FORMATTED CUSTOM PROPERTY TO A NUMERICAL REFERENCE SET FAIL TO MATCH
IV67499	SERVER DISCOVERY DOES NOT RETURN ANY RESULTS
IV67502	SECURITY APAR - USER ROLE CAPABILITIES CAN BE CHANGED WITHOUT CORRECT PERMISSION SET
IV67724	TOMCAT 'OUT OF MEMORY' OCCURENCES IN EXTREME SECURITY ENVIRONMENTS THAT CONTAIN A LARGE QUANTITY OF LOG SOURCES
IV67726	NO LONGER RECEIVING FLOWS FROM QFLOW COLLECTOR AFTER PATCHING TO EXTREME SECURITY 7.2.4.X
IV67812	UNABLE TO USE MULTIPLE WORD 'SEARCH PARAMETER' DESCRIPTIONS FOR OFFENSE 'AVAILABLE SAVED SEARCHES'

Table 3: Issues Resolved in V7.7.2.4 Patch 4 (continued)

Number	Description
IV68141	INDEXED CUSTOM EVENT PROPERTIES MIGHT CAUSE PERFORMANCE ISSUES
IV68153	WHEN EXTREMELY EXPENSIVE CUSTOM EVENT PROPERTIES ARE SET TO 'OPTIMIZE', THE PROCESSING QUEUE CAN FILL UP AND FAIL
IV68154	QVM - REMOVING AND RE-ADDING, OR MOVING A QVM PROCESSOR CAN CAUSE EXTREME SECURITY CONFIG BACKUPS TO FAIL
IV68185	PERFORMANCE DEGRADATION CAUSED BY INDEXED AND OPTIMIZED CUSTOM EVENT PROPERTIES BEING PARSED MULTIPLE TIMES
IV68189	QRM - NO DROP-DOWN MENU APPEARS WHEN CLICKING THE **NEW JOB** BUTTON IN CONFIGURATION SOURCE MANAGEMENT
IV68190	QVM - EXTREME SECURITY USER INTERFACE UNRESPONSIVE CAUSED BY VULNERABILITY IMPORT PROCESS
IV68203	HOURLY EXTREME SECURITY SYSTEM NOTIFICATIONS **`RAID CONTROLLER MISCONFIGURATION...`**
IV68510	EXTREME SECURITY PATCH CAN STALL AT MESSAGE **`APPLYING MAIN SCRIPT (45/114)`** FOR MULTIPLE HOURS
IV68562	PATCH SCANS THAT USE CENTRALISED CREDENTIALS MAY SPAWN MULTIPLE COPIES OF THE SAME COMMANDS
IV68567	APPLICATION ERROR OCCURS WHEN CREATING OR EDITING AN ANOMALY RULE
IV68592	PARSING ISSUES CAN OCCUR WITH INDEXED CUSTOM EVENT PROPERTIES THAT ARE OPTIMIZED THEN UNOPTIMIZED

5 Release Notes for ExtremeSecurity V7.7.2.4 Patch 3 Interim Fix 01

Interim fixes are intended to resolve specific APAR issues in the latest version of ExtremeSecurity products. If your deployment is installed with ExtremeSecurity V7.7.2.4 Patch 3 (7.2.4.1012120), then this interim fix can be applied to your system. This fix addresses an issue where multiple scans are started when centralized credentials are used.

Note
This interim fix corrects a scan issue in Extreme Security Vulnerability Manager. If you do not have this activated or installed in your deployment, then this interim fix is not required

To install this fix pack, see Patch Installation Instructions on page 11. The build number for this interim fix is `7.2.4-QRADAR-QRSIEM-1017100INT`.

Resolved Issues

This is a cumulative release, meaning that installing the latest version includes all of the resolved issues identified in previous releases.

Note
Some APAR links in the table below might take 24 hours to display properly after a software release.

Table 4: Issues Resolved in V7.7.2.4 Patch 3 Interim Fix 01

Number	Description
IV68562	PATCH SCANS WHICH USE CENTRALIZED CREDENTIALS MAY SPAWN MULTIPLE COPIES OF THE SAME COMMANDS

6 Release Notes for ExtremeSecurity V7.7.2.4 Patch 3

If your deployment is installed with ExtremeSecurity 7.7.1.2 or later, you can install fix pack `7.2.4-QRADAR-QRSIEM-1012120` and above to the latest software version. This release note does not cover all of the installation messages and requirements. For information on upgrading to V7.7.2.4, see the *Extreme Networks Security Upgrade Guide*.

To install this fix pack, see Patch Installation Instructions on page 11.

Resolved Issues

This is a cumulative release, meaning that installing the latest version includes all of the resolved issues identified in previous releases.

Note
Some APAR links in the table below might take 24 hours to display properly after a software release.

Table 5: Issues Resolved in V7.7.2.4 Patch 3

Number	Description
IV68365	EXTREME SECURITY V7.7.2.4 PATCH 4 FAILS WITH ERROR `AT LEAST <#>MB MORE SPACE NEEDED ON THE /BOOT FILESYSTEM`

7 Release Notes for ExtremeSecurity V7.7.2.4 Patch 2

If your deployment is installed with ExtremeSecurity 7.7.1.2 or later, you can install fix pack `7.2.4-QRADAR-QRSIEM-1002626` and above to the latest software version. This release note does not cover all of the installation messages and requirements. For information on upgrading to V7.7.2.4, see the *Extreme Networks Security Upgrade Guide*.

To install this fix pack, see Patch Installation Instructions on page 11.

Resolved Issues

This is a cumulative release, meaning that installing the latest version includes all of the resolved issues identified in previous releases.

Note
Some APAR links in the table below might take 24 hours to display properly after a software release.

Table 6: Issues Resolved in V7.7.2.4 Patch 2

Number	Description
IV40431	TOMCAT RESTARTED BY TXSENTRY
IV55305	LOG SOURCES DISAPPEAR FROM THE UI
IV60753	DASHBOARD REFRESH INTERVAL MAY GENERATE AN INVALID RESULT SET FOR A CUSTOM QUERY
IV63833	IF A 'SYSTEM' OFFENSE RULE IS EDITED, THE RULE RESPONSES WILL BEGIN TO FIRE TWICE WHEN THE OFFENSE IS TRIGGERED
IV64158	SOME FIELDS WITHIN IN THE EXTREME SECURITY UI WILL NOT ACCEPT A LOWER-CASE **T** WHEN USING SOME WEB BROWSERS
IV64857	TOMCAT SERVICE MAY RUN OUT OF MEMORY AND CAUSE THE EXTREME SECURITY USER INTERFACE TO BECOME TEMPORARILY UNRESPONSIVE
IV64997	EXTREME SECURITY TXSENTRY SYSTEM NOTIFICATIONS MAY OCCUR DURING LARGE ARIEL SEARCHES
IV65467	CUSTOM PROPERTY NAMES THAT CONTAIN A LEADING OR TRAILING WHITE SPACE WILL BREAK CUSTOM RULES
IV65668	EXPORTING CSV DATA OF AN OFFENSE USING SPECIFIED SEARCH CRITERIA DOES NOT WORK AS EXPECTED
IV65933	USING THE OFFENSE SEARCH **SAVE CRITERIA** OPTION THAT CONTAINS A CIDR RANGE DOES NOT RETAIN THE CIDR INFORMATION

Table 6: Issues Resolved in V7.7.2.4 Patch 2 (continued)

Number	Description
IV65938	EXTREME SECURITY SQL TRANSACTIONS MAY TIME OUT DURING A PATCH INSTALLATION CAUSING UNEXPECTED RESULTS OR PATCH ERROR MESSAGES
IV65959	ASSETS ARE DISPLAYED MULTIPLE TIMES IN THE USER INTERFACE AND IN ASSET EXPORTS
IV65976	ERROR GENERATED WHEN ADDING A SEARCH FILTER VALUE WITH A CIDR RANGE ON A CUSTOM PROPERTY CREATED AS `FIELD TYPE: IP`
IV66082	ASSETPROFILER RELATED TXSENTRY SYSTEM NOTIFICATIONS DURING VULNERABILITY SCAN IMPORTS
IV66384	OFFENSES, RULES PAGE LOADS BLANK AND BECOMES UNRESPONSIVE IN CERTAIN CONDITIONS
IV66390	REPORTS THAT CONTAIN A SEARCH WITH `DESTINATION PAYLOAD CONTAINS IS NOT N/A` FILTER FAIL
IV66391	A REPORT RUN ON ALL LOG SOURCES COMPLETES AS AN EMPTY REPORT
IV66396	MANAGEMENT INTERFACE CHANGES FROM ETH0 TO ETH2 AFTER EXTREME SECURITY INSTALLATION ON M4 X3550 HARDWARE
IV66402	TIME SYNC MAY FAIL BETWEEN HA PAIR IN EXTREME SECURITY SIEM 7.2.3
IV66434	EXTREME SECURITY UI SYSTEM NOTIFICATION `PROCESS ECS-EP HAS FAILED TO START` FOR A EXTREME SECURITY COLLECTOR
IV66647	Vulnerability Manager - VULNERABILITY SCAN APPEARS TO HANG OR NEVER COMPLETE
IV66759	UNABLE TO GENERATE TIMES SERIES DATA OR EDIT A SEARCH THAT CONTAINS MULTIPLE 'GROUP BY'
IV67007	CLASSCASTEXCEPTION THROWN WHEN CREATING TIME SERIES FOR SEARCHES THAT HAVE GROUP BYS THAT ARE SUBSETS OF OTHER SEARCHES
IV67093	CHANGES MADE TO 'MAX NUMBER OF TCP SYSLOG CONNECTIONS' DO NOT GET REPLICATED TO MANAGED HOSTS
IV67171	CUSTOMERS USING THE REST API MAY EXPERIENCE TOMCAT 'OUT OF MEMORY' INSTANCES
IV67175	ERROR WHEN TRYING TO ADD HA SECONDARY 'KEY NOT FOUND: SYSTEMMANAGEMENT.HA.WIZARD.ERROR.1'
IV67201	EXTREME SECURITY USER INTERFACE BECOMES UNRESPONSIVE WHEN ATTEMPTING A SEARCH USING `LOG SOURCE GROUP`
IV67492	Vulnerability Manager - RUNNING THE Vulnerability Manager ASSET UPDATE TOOL WILL GENERATE EMAILS EVERY HOUR IF EXTREME SECURITY SYSTEM MAIL IS ENABLED
IV67495	EXTREME SECURITY LOGS FILLING WITH LARGE AMOUNTS OF ARIEL FLOW ERRORS

8 Release Notes for ExtremeSecurity V7.7.2.4 Patch 1

If your deployment is installed with ExtremeSecurity 7.7.1.2 or later, you can install fix pack `7.2.4-QRADAR-QRSIEM-988458` and above to the latest software version. This release note does not cover all of the installation messages and requirements. For information on upgrading to V7.7.2.4, see the *Extreme Networks Security Upgrade Guide*.

To install this fix pack, see Patch Installation Instructions on page 11.

Resolved Issues

This is a cumulative release, meaning that installing the latest version includes all of the resolved issues identified in previous releases.

Note
Some APAR links in the table below might take 24 hours to display properly after a software release.

Table 7: Issues Resolved in V7.7.2.4 Patch 1

Number	Description
IV66977	V7.7.2.4 - SOME USERS ARE UNABLE TO MAKE UI CUSTOMIZATION CHANGES
IV67009	QUICK FILTER CANNOT START WITH THE ' * ' CHARACTER
IV67010	V7.7.2.4 - `MINIMUM SYSTEM MEMORY CHECK ON SECONDARY IS FAILED` MESSAGE WHEN TRYING TO CREATE A HIGH AVAILABILITY PAIR
IV67012	V7.7.2.4 - SYSTEM LICENSE EXPORT AND OFFENSE EXPORT TO CSV OR XML FAILS

9 Release Notes for ExtremeSecurity V7.7.2.4

If your deployment is installed with ExtremeSecurity 7.7.1.2 or later, you can install fix pack `7.2.4-QRADAR-QRSIEM-983526` and above to the latest software version. This release note does not cover all of the installation messages and requirements. For information on upgrading to V7.7.2.4, see the *Extreme Networks Security Upgrade Guide*.

To install this fix pack, see Patch Installation Instructions on page 11.

Resolved Issues

This is a cumulative release, meaning that installing the latest version includes all of the resolved issues identified in previous releases.

Note
Some APAR links in the table below might take 24 hours to display properly after a software release.

Table 8: Issues Resolved in V7.7.2.4

Number	Description
IV46355	RAPID7 NEXPOSE SCANNER DISPLAYS AN ERROR WHEN THE SITE NAME PATTERN FIELD CONTAINS AN AMPERSAND (&) CHARACTER
IV46461	THE TEST FIELD IN THE CUSTOM PROPERTIES WINDOW MIGHT NOT DISPLAY SPECIAL CHARACTERS AS INTENDED
IV47857	NO NOTIFICATION THAT EVENTS ARE DROPPED BY A ROUTING RULE
IV50577	THE LICENSE DETAILS SCREEN MAY SHOW LICENSE DETAILS FOR ANOTHER HOST IN THE DEPLOYMENT
IV50730	BACKUP ARCHIVES FAIL TO GENERATE DUE TO A MISSING RPM DEPENDANCY CAUSED BY AUTOMATIC UPDATES
IV54191	ASSET SEARCH WITH OS INFORMATION IS SLOW
IV54564	USER PROFILES WITH ONLY ACCESS TO REPORTS WILL THROW 404 WHEN ACCESSING REPORTS IN INTERNET EXPLORER
IV54606	AFTER AN UPGRADE TO EXTREME SECURITY 7.7.2.1 Patch 4, A LOG SOURCE EXTENSION MIGHT DISPLAY INVALID CHARACTER SYMBOLS
IV54655	DEPLOYS MAY FAIL WHEN AN ENCRYPTED CONNECTION EXISTS FOR AN UNASSIGNED COMPONENT
IV54675	DASHBOARD TIME SERIES GRAPHS FOR EVENT RATES (EPS) MIGHT DISPLAY A DECREASE IN AN EVENT RATE WHERE NONE EXISTS
IV54720	MANAGED HOSTS WITH AN HA SECONDARY MIGHT EXPERIENCE A POSTGRES RPM OR DISKMAINT ERROR AFTER A HOSTSERVICES RESTART

Table 8: Issues Resolved in V7.7.2.4 (continued)

Number	Description
IV54734	RULE RESPONSES THAT SEND AN OFFENSE SUMMARY EMAIL NOTIFICATION MIGHT INCLUDE AN UNRESOLVABLE ADDRESS IN THE URL
IV59270	RISK SCORE FILTER NOT FILTERING - RETURNING ALL ASSETS
IV59284	NETWORK HIERARCHY TREE SHOWS "UNDEFINED" WHEN NETWORK GROUP HAS DEPTH GREATER THAN 9 LEVELS
IV59345	IMPROPERLY FORMATTED SYSTEM EVENTS ARE BEING PICKED UP BY THE CRE LOG SOURCE
IV60520	OFFENSE RULE CONDITION "LOG SOURCE TYPE(S) THAT DETECTED THE OFFENSE" DOES NOT FIRE DUE TO LOG SOURCE MISMATCH
IV60570	NON-ADMIN USERS UNABLE TO VIEW FULL RULE DETAILS
IV60575	NOTIFICATION QID VALUE IS INCORRECT
IV60576	IMPROVE CRE PERFORMANCE AGAINST PORTS AND LARGE DATABASE TABLES
IV60644	EXCESSIVE SIM AUDIT EVENTS FOR HA SSH ACTIVITY
IV60760	ROUTING RULES FILTER RETURNING UNEXPECTED RESULTS
IV60765	FILTERING PAYLOAD BY REGEX ENDING WITH "\ " INTERFERES WITH THE LOG ACTIVITY VIEW
IV61200	SORTING IN ASSET DETAILS - USER LIST DOES NOT WORK
IV61255	EXTREME SECURITY SHOWS A TIMESTAMP FOR 'LAST SEEN PASSIVE' EVEN IF ALL FLOW SOURCES ARE DISABLED
IV61260	RULE TEST TO NOT CREATE OFFENSE IF TWO RULES ARE MATCHED IS CREATING AN OFFENSE
IV61456	COLUMN SORTING NOT SORTING IN THE LOG SOURCE WINDOW
IV61687	RULE INFORMATION IS MISSING FROM THE AUDIT LOG WHEN RULES ARE MODIFIED
IV62203	MANUAL CARRIAGE RETURNS USED IN THE TEXT FIELD OF AN OFFENSE NOTE CAUSE INCOMPLETE NOTE OUTPUT IN THE AUDIT LOGS
IV62349	WINCOLLECT LOG SOURCE DISPLAY SORTING RETURNS NO RESULTS IN 7.1.0
IV62439	UI PROBLEM IN FIREFOX 30 - UNABLE TO SELECT LEVEL ON SOURCE NETWORK GROUP
IV62441	ASSET TABLE EXPORT SHOWS 0.0.0.0 FOR THE IP AT TIMES WHEN THE GUI DISPLAYS A REAL IP
IV62476	VULNERABILITY DETAILS NOT SHOWN FOR NON-ADMIN USER
IV62587	RULE COUNTING IS NOT WORKING USING SPECIFIC PALO ALTO CONFIGURATION
IV63048	MEMORY LEAK IN BANDWIDTH MANAGER
IV63122	WHEN SHARING A SAVED SEARCH, **INCLUDE IN MY DASHBOARD** IS SELECTED BY DEFAULT AND SHOULD NOT BE

Table 8: Issues Resolved in V7.7.2.4 (continued)

Number	Description
IV63346	HAVING AN EQUAL SIGN ("=") IN A RULE NAME CAN CAUSE EVENTS TO BE DROPPED AND OTHER EVENT PIPELINE FAILURES
IV63375	LARGE INCREASE IN EVENTS GENERATED BY THE SYSTEM NOTIFICATION LOG SOURCE
IV63416	GROUPED EVENT SEARCHES CONTAINING NUMERIC CUSTOM PROPERTIES MAY RETURN INCORRECT SUM CALCULATIONS
IV63452	WHEN AN HA FAILOVER OCCURS, ADDITIONAL BONDED INTERFACES WILL BE REMOVED
IV63457	ACTIVE DIRECTORY LOGIN FAILS WHEN TRYING TO AUTHENTICATE TO THE API
IV63462	PDF REPORT FILENAMES WITH CHINESE CHARACTERS THAT ARE MAILED DO NOT RETAIN CORRECT CHINESE CHARACTERS IN THE ATTACHMENT NAME
IV63610	THE **WRAP TEXT** CHECKBOX DOES NOT WORK WHEN SELECTED FOR VIEWING CISCO IDS EVENT PAYLOADS
IV63733	TUNNELRDATE WARNING MESSAGES GENERATED EVEN WHEN NOT USING ENCRYPTION BETWEEN CONSOLE AND MANAGED HOST
IV63742	'BB:CATEGORYDEFINITION: COUNTRIES/REGIONS WITH NO REMOTE ACCESS' CONTAINS AN INCORRECT LOCATION NAME
IV63743	SELECTING A LANGUAGE OPTION OTHER THAN ENGLISH FOR EXTREME SECURITY LOG MANAGER DOES NOT WORK
IV63792	THE DESTINATION IP SOURCEPORT IS APPENDED TO THE DESTINATION IP WHEN QUERYING TYPE-B SUPERFLOWS
IV63798	NETWORK ACTIVITY SEARCH RIGHT-CLICK FILTER OPTIONS FOR APPLICATION IS OR IS NOT 'OTHER' NOT RETURNING CORRECT
IV63799	CHANGE IN LOCALE SETTINGS FROM ENGLISH TO ANY OTHER LANGUAGE CAUSES NO DATA RESULTS FROM FLOW DATA APPLICATION SEARCHES.
IV64011	THE NUMBER OF DATA VARIABLES IN AN OFFENSE CRE SNMP TRAP DOES NOT MATCH THAT OF THE ASSOCIATED EXTREME SECURITY FILE.
IV64141	EXTREME SECURITY PATCH MAY FAIL OR COMPLETE BUT WITH ERRORS THAT REFERENCE `722_PATCH_58912.INSTALL`
IV64252	REFERENCE MAP OF MAPS DOES NOT WORK AS DESCRIBED IN THE EXTREME SECURITY ADMIN GUIDE DOCUMENTATION
IV64738	QFLOW PROCESS STOPS AND THEN FAILS TO START
IV64977	LOG ACTIVITY ADVANCED SEARCH THAT SPECIFIES USING 'LOGSOURCEGROUPNAME' ONLY RETURNS RESULTS FROM GROUP 'OTHER'
IV65030	QVM - EXTREME SECURITY SYSTEM NOTIFICATION THAT REFERS TO 'QVMSCANCOMPLETELISTENER HAS REACHED FULL CAPACITY'
IV65081	MULTIPLE VULNERABILITIES IN EXTREME SECURITY (SIEM CVE-2014-0075, CVE-2014-0096, CVE-2014-0119)

Table 8: Issues Resolved in V7.7.2.4 (continued)

Number	Description
IV65711	MULTIPLE VULNERABILITIES IN EXTREME SECURITY SIEM (CVE-2014-3508, CVE-2014-3511)
IV66146	QIF - 'NO FILES TO DOWNLOAD' MESSAGE WHEN PERFORMING AN EXPORT AS PCAP
IV66369	QIF - THE 'LICENSE INFO' PAGE SHOWS 'DATABASE NOT ENABLED'
IV66371	RULES NO LONGER FIRING AFTER A REFERENCE SET IS FOUND TO BE EMPTY OR DOES NOT EXIST
IV66785	THE PARTITION /STORE/ARIEL/PERSISTENT_DATA IS NOT MONITORED BY DISK SENTINEL
IV66787	NO FLOW INFORMATION IS DISPLAYED WHEN USING NON ENGLISH LOCALE IN SOME INSTANCES
IV66874	THE ADMIN TAB, REMOTE NETWORKS AND SERVICES CONFIGURATION PAGE DOES NOT LOAD CORRECTLY IN THE EXTREME SECURITY UI
IV66882	QIF - CASES THAT ARE 'DELETED' FROM WITHIN CASE MANAGEMENT ARE NOT ACTUALLY DELETING