

# **Extreme Security Threat Protection Release Notes for Release 5.3.x**

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/](http://www.extremenetworks.com/company/legal/trademarks/)

## Support

For product support, including documentation, visit: [www.extremenetworks.com/documentation/](http://www.extremenetworks.com/documentation/)

For information, contact:

Extreme Networks, Inc.

145 Rio Robles

San Jose, California 95134

USA

# Table of Contents

---

- Preface..... 4**
  - Text Conventions..... 4
  - Providing Feedback to Us..... 4
  - Getting Help..... 5
  - Related Publications..... 5
- Chapter 1: About These Release Notes..... 7**
  - Compatibility..... 7
  - Installing Updates..... 7
  - Obtaining a License Key..... 8
- Chapter 2: 5.3.2.2 Release Notes..... 10**
- Chapter 3: 5.3.2.1 Release Notes..... 12**
- Chapter 4: 5.3.2 Release Notes..... 14**
- Chapter 5: 5.3.1.5 Release Notes..... 16**
- Chapter 6: 5.3.1.4 Release Notes..... 18**
- Chapter 7: 5.3.1.3 Release Notes..... 19**
- Chapter 8: 5.3.1 Release Notes..... 21**








# Preface

## Text Conventions

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

**Table 1: Notice Icons**

Icon	Notice Type	Alerts you to...
	General Notice	Helpful tips and notices for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
	New	This command or section is new for this release.

**Table 2: Text Conventions**

Convention	Description
Screen displays	This typeface indicates command syntax, or represents information as it appears on the screen.
The words <b>enter</b> and <b>type</b>	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.”
<b>[Key]</b> names	Key names are written with brackets, such as <b>[Return]</b> or <b>[Esc]</b> . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press <b>[Ctrl]+[Alt]+[Del]</b>
<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](mailto:internalinfodev@extremenetworks.com).

## Getting Help

---

If you require assistance, you can 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 1-603-952-5000. For the Extreme Networks support phone number in your country, visit: [www.extremenetworks.com/support/contact](http://www.extremenetworks.com/support/contact)
  - **Email:** [support@extremenetworks.com](mailto: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 Network 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 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 About These Release Notes

Compatibility  
Installing Updates  
Obtaining a License Key

These release notes cover Extreme Security Threat Protection for 5.3.x releases, including patches. These notes cover:

- New functionality
- Fixes
- Known Issues

For the upgrade procedure that covers all releases, see [Installing Updates](#) on page 7.

## Compatibility

The following web browsers are currently supported by the Extreme Security Threat Protection local management interface:

- Internet Explorer 10 or 11
- Firefox 28 or later
- Google Chrome 34 or later

To manage Extreme Security Threat Protection 5.3.2.2 appliances using the Security SiteProtector System, you must apply the following database service packs:

- **SiteProtector System 3.0** - Install all DBSPs up to and including SP3.0 DBSP 3.0.0.50
- **SiteProtector System 3.1.1** - Install all DBSPs up to and including SP3.1.1 DBSP 3.1.1.32



### Important

Ensure that the SiteProtector Core is at version 3.1.1.5 before applying this Database Service Pack (DBSP) update to the Extreme Security Threat Protection appliance.

## Installing Updates



### Note

After you install firmware updates, you must restart the appliance.

Firmware updates contain new program files, fixes or patches, enhancements, and online help. Firmware updates are available from the **Software** tab of the Extreme Security Threat Protection downloads page (<https://extranet.extremenetworks.com/downloads/Pages/SecurityThreatProtection.aspx>).

Intrusion prevention updates contain the most recent security content provided by Extreme Networks.

For more information about product issues and updates, see the product documentation at <http://documentation.extremenetworks.com>.

- 1 Click **Manage > Available Updates**.
- 2 In the **Available Updates** pane, use one or more of the following commands:

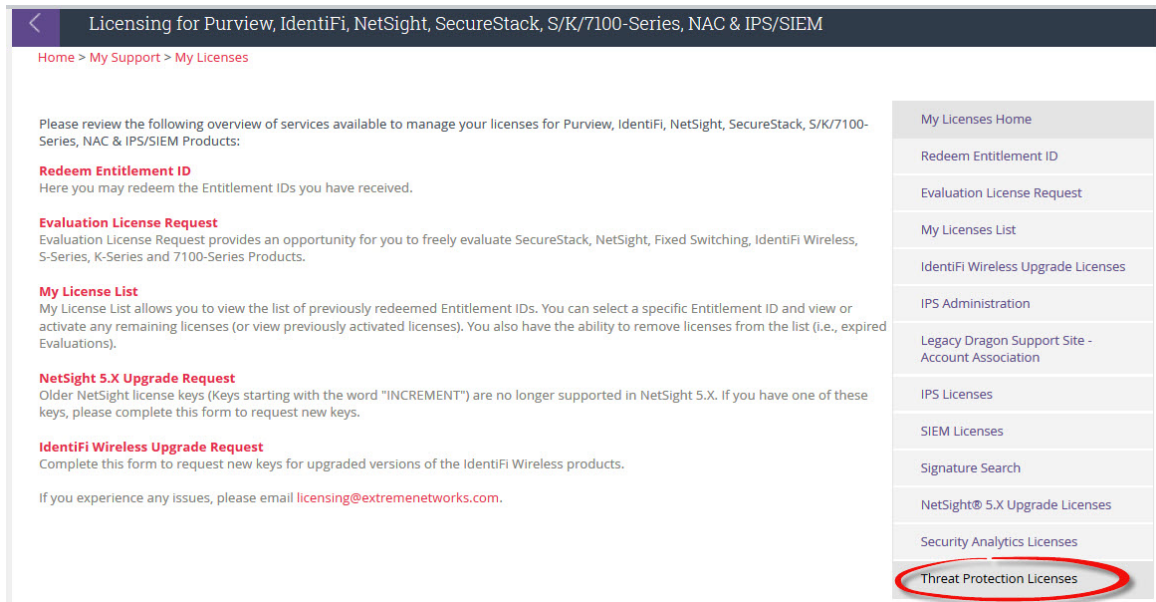
Option	Description
Upload	<ul style="list-style-type: none"> <li>To manually add an update, click <b>Upload</b>.</li> <li>In the <b>New Update</b> window, click <b>Select Update</b>, browse to the update file, click <b>Open</b>, and then click <b>Submit</b>.</li> </ul> <p><b>Note:</b> You can install the update after you manually add it.</p>
Refresh	To check for updates, click <b>Refresh</b> .
Install	To install an update, select the update, and then click <b>Install</b> .
Schedule	<p>To create or edit an update schedule, select an update, and then click <b>Schedule</b>.</p> <p>In the <b>Edit Schedule</b> window, perform one or more of the following actions:</p> <ul style="list-style-type: none"> <li>To remove an update schedule, select <b>Remove Schedule</b>.</li> <li>To create an update schedule, select a date and time to install the update.</li> </ul> <p>Click <b>Submit</b> to save your changes.</p>

## Obtaining a License Key

To obtain a License Key:

- 1 Log in to the Extreme Extranet (<https://extranet.extremenetworks.com>) using your username and password.
- 2 Under **Product Licensing**, click **Product Purview**, **IdentiFi**, **NetSight**, **SecureStack**, **S/K/7100-Series**, **NAC**, **Security Analytics and Threat Protection** from the bulleted list.

- Click **Threat Protection Licenses** from the menu bar on the right.



The registration form displays.

Use this form to enter information required to register your license key. You will need to include information from your Product License Certificate included with your Threat Protection appliance

Product Description:	IP5G2-X3-P-SSL-SW	
Serial Number:	1234567890	*
License Destination Email:	jdoe@email.com	*
Re-enter Destination Email:	jdoe@email.com	*

**SUBMIT**

If you need licenses for the older versions of Dragon IPS then [click here](#)

- Select your product from the **Product Description** drop-down list.
- Type your product's serial number in the **Serial Number** field.
- Enter and confirm the email address to which the license should be sent.
- Click **Submit**.

Within 48 hours you will receive an e-mail with your software License Key. If you have any questions, please contact [Extreme Networks Support](#).

# 2

## 5.3.2.2 Release Notes

---

Extreme Security Threat Protection firmware version 5.3.2.2 is available. These release notes address compatibility, installation, and other getting-started issues.

### Overview

Extreme Security Threat Protection firmware version 5.3.2.2 is a firmware update for the XGS IPS network protection platform.

### Fixed Defects

- **80786** - Embedded knowledge center contains unnecessary note for configuring IP address on protection interface pair for SSL decryption.
- **80776** - Security event SSL\_Malformed\_Certificate is triggered by outgoing SSL traffic on internal Network Protection appliance due to Outbound SSL inspection being enabled on external Network Protection appliance.
- **80593** - Changing the admin password using the CLI prints cleartext password in the system log.
- **80196** - Can not change speed/duplex on management interface M.1 through advanced tuning parameter with latest BMC firmware. For more information, see technote #1964988.
- **80171** - LMI login warning banner does not contain an OK button as acknowledgement.
- **80145** - Packet processing daemon crashes in ISNP 5.3.2.1 when traffic matches a domain certificate object used in a Network Access Policy rule and there are at least 10 Network Access Policy rules enabled.
- **80136** - In the SiteProtector Management policy, the proxy password in the Agent Manager configuration is stored in plain text.
- **80095** - The appliance fails to block IPv6 unspecified address ':::' when used in Network Access Policy rules.
- **79803** - If the **Enable X-Force Protection Level Blocking** option on the IPS Object general **Configuration** tab is disabled, installing a new XPU causes events to be blocked.
- **79723** - GLGUP1002E system event indicates a failed upgrade attempt is incorrectly logged after changing the active partition to an earlier firmware and accessing the Available Updates page in the LMI.
- **79664** - Hardware Diagnostics should be disabled on Extreme Security Threat Protection for VMware.
- **79662** - The Appliance SSL Certificate used by the LMI is renewed 1 day prior to expiration.
- **78614** - Open signature rules cannot be used to detect outbound SSL traffic. This requires XPU 36.020, released February 2016.
- **77677** - The USB device detection event GLGHW9001I does not contain USB manufacturer and product information.
- **81528** - When compiling the Network Access rule set, the packet processing daemon crashes with signal 11 if at least 10 Network Access Policy rules are enabled and at least one contains a schedule object.

## Changed Features

Due to the *DROWN* OpenSSL TLS vulnerability (CVE-2016-0800), SSLv2 was removed from the Outbound SSL inspection supported protocols.

## Known Issues

This release contains no known issues at this time.

## Security Bulletins

- <http://www.ibm.com/support/docview.wss?uid=swg21978438>
- <http://www.ibm.com/support/docview.wss?uid=swg21977281>
- <http://www.ibm.com/support/docview.wss?uid=swg21975835>
- <http://www.ibm.com/support/docview.wss?uid=swg21975225>
- <http://www.ibm.com/support/docview.wss?uid=swg21974989>
- <http://www.ibm.com/support/docview.wss?uid=swg21974550>

# 3

## 5.3.2.1 Release Notes

---

Extreme Security Threat Protection firmware version 5.3.2.1 is available. These release notes address compatibility, installation, and other getting-started issues.

### Overview

Extreme Security Threat Protection firmware version 5.3.2.1 is a firmware update for the XGS IPS network protection platform.

### Enhancements

- **78459** - Added ability to trigger different system events for different PSU/FAN sensor statuses.
- **77608** - Added tuning parameter `callhome.job.lifetimeinminutes` (default 4320, 3 days), for a specific lifetime to queue errors for problems without creating PMRs.
- **79481** - Added BMC firmware info into support file.
- **79097** - Added `du -h /var/support` (after "df") in support file in order to dump the disk usage of `/var/support` directory

### Fixed Defects

- **77793** - Missing translated MESA event catalogs for system event GLGSY0044W could result in broken event log records.
- **79416** - SNMP manager failed to query appliance info using `snmpget` through its IPv6 address.
- **77304** - During appliance startup, inappropriate process startup sequence caused false positives for some of the system events for `pktpd` and user identity.
- **79350** - The value of `callhome.job.frequency` should default to 60 minutes when any another `callhome` parameter is added.
- **78834** - Appliance incorrectly adds a quarantine response for `tcp_port_scan` event when quarantine response to probe events, such as `tcp_probe_ssh`, is set.
- **78825** - Changed severity for the the PMRs created through `callhome` to 2 for the system events related to `mesa_eventsd` (Events Processing Daemon).
- **78803** - Configuring XGS7100 in high availability mode with asymmetric traffic causes `alpsd` to crash.
- **78203** - Appliance incorrectly reports Quarantine End Time as Jan 1, 1970 8:00:00 AM in IPS Event Details window.
- **78149** - Local Management interface can be accessed from protection interface IP address if the client connects using fully qualified domain name (FQDN) of the appliance.
- **78117** - Incomplete resource cleanup during analysis process restart can cause management configuration to fail through CLI.
- **78088** - Improper handling of passive authentication event requests resulted in incorrect identity information.
- **77877** - The local management interface dashboard graphs for SSL inspection rate and connection rate are using up to 10% below the actual values because they are expressed as binary units.

- **77829** - Graphs on SSL connections statistics page on the local management interface (Monitor->Network Graphs) uses improper graph label "Connections/sec".
- **77815** - Incorrect format displayed in CLI (stat > show > 6 protection interface) when experiencing large frame numbers.
- **77732** - Large packet capture (more than 500MB) cannot be downloaded using the LMI.
- **77681** - Protection interface network graph for all NIM interfaces incorrectly shows a spike during XPU install/rollback.
- **77678**: Start and end time of ongoing packet capture file is corrupted when capturing traffic on management interface.
- **77339** - Inbound SSL inspection incorrectly logs an SSL decryption error event error: `Bad handshake sequence: error:14094085:SSL routines:SSL3_READ_BYTES:ccs` received early during SSL handshake.
- **77298** - Using capture connection can prematurely terminate the packet capture before connection being captured is closed completely.
- **77190** - After eight policy deployments, next NAP deployment fails and causes resource errors along with alpsd restart, due to connections retaining a reference to old NAP rulesets indefinitely.
- **77189** - When using Internet Explorer 11 to edit a rule in a long list of NAP rules, the page appears to jump around, making it difficult to double-click on a NAP rule to edit.
- **74318** - IPS events that are enabled in the default Trust XForce objects aren't actually turned off inside PAM when disabled in all in-used IPS objects.
- **73968** - DcaClient logs too much information when debug mode is enabled.

## Known Issues

This release contains no known issues at this time.

## Security Bulletins

- <http://www.ibm.com/support/docview.wss?uid=swg21972209>
- <http://www.ibm.com/support/docview.wss?uid=swg21969670>
- <http://www.ibm.com/support/docview.wss?uid=swg21969771>
- <http://www.ibm.com/support/docview.wss?uid=swg21974231>
- <http://www.ibm.com/support/docview.wss?uid=swg21972382>
- <http://www.ibm.com/support/docview.wss?uid=swg21974242>

# 4

## 5.3.2 Release Notes

---

Extreme Security Threat Protection firmware version 5.3.2 is available. These release notes address compatibility, installation, and other getting-started issues.

### Overview

Extreme Security Threat Protection firmware version 5.3.2 is a firmware update for the XGS IPS network protection platform. This release provides the following updates to Extreme Security Threat Protection firmware version 5.3.1:

- Support for session ID and session ticket resumption for inbound SSL inspection.
- Added Do Not Inspect action in the Network Access Policy to bypass traffic from analysis completely.
- CLI enhancement that provides access to information for the following statistics from the command line interface stats > show mode:
  - PU load information
  - Memory usage information
  - Storage usage information
  - Processed packet information
  - Protection interface information
  - Inbound SSL connections information
  - Outbound SSL connections information
  - Admin account password expiry information
  - NTP time drift information
  - Last policy modification time
  - Appliance reboot information
- LMI enhancements:
  - Added key services memory usage information to the **Monitor > System Graphs** page.
  - Completed web application framework migration to improve LMI stability.
- Policy migration enhancements:
  - Enhanced migration of Security Network IPS policies using child repositories in the SiteProtector™ System system.
  - Enhanced migration of filter object and service object names to reflect objects' contents.



#### Note

For information about policy migration, see the [Network IPS policy migration topics](#).

- Added Log with Raw option for intrusion prevention objects and Open Signature policy.

This release includes all of the defect fixes from firmware update 5.3.1.5. See the Extreme Networks Release Notes page at: [www.extremenetworks.com/support/release-notes](http://www.extremenetworks.com/support/release-notes) for a list of those fixes.

## Announcement

The Extreme Security Threat Protection firmware version 5.3.2 announcement is available at <http://www.ibm.com/common/ssi/index.wss>. See the announcement for the following information:

- Detailed product description, including a description of new functionality
- Product-positioning statement
- Packaging and ordering details
- International compatibility information

## Known Issues

- **72617** - Clicking **Manage > Overview** in the LMI does not display the last update time after firmware update.
- **74318** - IPS issues in the default Trust X-Force objects are not turned off inside PAM when disabled.
- **74415** - The Fps Dropped statistics graphs do not display correctly in the LMI when the response in an unanalyzed policy is set to Drop.
- **74484** - Remote syslog messages contain erroneous values, such as **APPNAME** and **PROCID**, which are not relevant to the event being forwarded.
- **75612** - UDP throughput testing for VMware shows high latency and low throughput when the frame size is larger than 1024.
- **76736** - Misleading event **GLGSY0000W - System service was terminated unexpectedly and subsequently restarted** is logged in system events when packet processing exits with a failure and analysis daemon is no longer running.
- **77189** - When using Internet Explorer 11 to edit a rule in a long list of NAP rules, the page appears to jump around, making it difficult to select a NAP rule to edit.
- **77298** - Packet capture can stop prematurely.
- **77339** - Inbound SSL inspection does not print the correct detail in system events when receiving an unexpected alert during handshake.
- **77380** - Unexpected quarantine responses for **tcp\_port\_scan** events blocks internal traffic, affecting application access for network users.

As a work-around, you can add IPS event filters to ignore **tcp\_probe** signatures that have enabled quarantine for specific VA hosts.

- **77385** - "Authorization is Required" error appears in messages log on every attempt to communicate with SiteProtector System.
- **77640** - LMI displays a JavaScript error message when you remove a network object from a Management Access Policy rule and delete it.
- **77641** - Network objects using CIDR format that is not supported in Management Access Policy are not filtered out in LMI.
- **77677** - The USB device detection event **GLGHW9001I** missing the USB manufacturer and product.
- **77678** - Start and end time of ongoing packet capture is incorrectly displayed on LMI immediately after the management interface capture starts.
- **77681** - NIM protection interface network graph shows spike during an XPU installation or rollback.
- **77732** - Large packet captures (greater than 500MB) cannot be downloaded using the LMI. Users can use SFTP as a workaround.

# 5

## 5.3.1.5 Release Notes

---

Extreme Security Threat Protection firmware version 5.3.1.5 is available.

### Overview

Extreme Security Threat Protection version 5.3.1.5 is a firmware update to version 5.3.1.

### Fixes

Firmware update 5.3.1.5 provides fixes for the following issues for version 5.3.1:

- **64621** - The value of the SSL Connection Statistics graph for date range is shown as a floating point value, which is the incorrect type. This is corrected by changing the type to an integer value.
- **69647** - System alerts FNXY0003I and FNXY0004I are not generated when there is unanalyzed traffic in 5.3.
- **73870** - When a defective Network Interface module is installed in a running system, the inspection engine crashes, which can cause a kernel segfault. System alert GLGHW9008E is logged in System Events, which includes the serial number and the bank of the failed NIM.
- **74300** - CLI no longer displays Invalid arguments when the user cancels the **Services > Restart** command.
- **74813** - Maximum latencies of 8ms on 3100 and 4100 onboard ports.
- **74881** - Because Extreme Security Threat Protection policy accepts any input and VLAN regardless of its case, some upper and lower case combinations of the 3 letters can cause migration to incorrectly migrate the VLAN policy.
- **74963** - NTP policy does not accept NTP server names that begin with a number.
- **75006** - HTTPS traffic is not captured by the user authentication portal when Outbound SSL Inspection policy is not configured. This fix displays the user authentication portal when a user attempts to access an HTTPS site whenever the Unauthenticated User NAP rule is configured, whether or not outbound SSL inspection is enabled.
- **75079** - Cannot change the number of FNXY1001E messages (VLAN tagged outbound SSL traffic is skipped) that are shown in system logs. Added the following advanced tuning parameters\*:  
alpsd.ssl.event.throttle = 10 Per Interval for system. If 0 then disables throttling altogether.  
alpsd.ssl.event.interval = 60 In Seconds
- **75124** - When an address list object is imported via the Merge or the Migrate to Repository commands in SiteProtector, the VLAN value is changed from a blank to a 0.
- **75129** - Inspection engine crashes during receipt of non-sequitur events.
- **75141** - When the primary inspection engine process is shut down, Primary Icores are resuming is incorrectly recorded to (syslog/messages log). This message will no longer appear.
- **75299** - Coalescer update/info events are implicitly non-sequitur but are not handled that way.
- **75413** - Update to the latest GKSit to add LMI access using Firefox when appliance is FIPS enabled and ALPN is enabled in Firefox.
- **75730** - Trigger a system event when a fan or power supply goes bad. System event GLGHW0101E is now triggered.

- **75771** - Some hardware events have incorrect IDs. Added GLGHW0011W and GLGHW0012E to the event ID list
- **75774** - The log no longer displays TEMP: messages when debug logging is at default level.
- **76027** - Remove unwanted information and add result debug level information to the CLI analysis commands output.
- **76366** - Add tuning parameters to specify URL to be used to redirect both the authentication request and block pages. Added the following tuning parameters\*:
  - `tune.block.redirect.url = http://<url>` — Redirects blocked sites to an external customer block page instead of system injected block page.
  - `tune.auth.redirect.url = http://<url>/script?orig=` — Redirects user to an external customer authentication portal for login.
- **76653** - ICMP-based events are reported against the default IPS object instead of the one from the matching NAP rule.
- **76721** - Traffic by User and Application graphs display a straight line in the LMI, instead of rising and falling traffic levels.
- **76768** - Process hangs in soft bypass mode are not always detected and logged correctly, causing difficulty in diagnosing crash data. This fix improves support oriented crash data generation.

## Known Issues

Firmware update 5.3.1.5 contains the following known issues:

- Large file uploads and downloads might stall and eventually fail when outbound SSL inspection is enabled.

---

\* **Important:** Change advanced tuning parameter values only under the supervision of Extreme Customer Support.

# 6 5.3.1.4 Release Notes

---

Extreme Security Threat Protection firmware version 5.3.1.4 is available.

## Overview

Extreme Security Threat Protection version 5.3.1.4 is a firmware update to version 5.3.1.

## New Functionality

The Network Protection appliance can now be installed and deployed on a VMware platform. The following VMware Tools are integrated in the Network Protection image:

- power on
- power off
- restart
- suspend
- resume

The CLI analysis mode has been added.

## Fixes

The following issues were fixed in firmware version 5.3.1.4:

- **74586** - The title of the Network Traffic Details for User page does not display the user IP address. To view the Network Traffic Details for User page, click **Monitor > Traffic Details by User**, and then click a user in the **Traffic Details** table.
- **74573** - Traffic can be dropped for several seconds if a security XPU is applied while a URL or application database is being updated.
- **74520** - You cannot upload a Local User Database Archive file that has parentheses in the file name.
- **74361** - Packets collected by the packet capture feature are truncated to 1500 bytes because the value is hard coded.
- **74192** - The appliance terminates bypass mode before it is ready to accept network traffic, which causes packet loss.
- **62988** - When some policy changes are deployed, network users sometimes experience stalled or dropped connections and network disruption.

## Known Issues

Firmware update 5.3.1.4 contains the following known issues:

- LMI pages do not always open correctly in the Chrome browser.

# 7

## 5.3.1.3 Release Notes

---

Extreme Security Threat Protection firmware version 5.3.1.3 is available.

### Overview

Extreme Security Threat Protection version 5.3.1.3 is a firmware update to version 5.3.1.

### Fixes related to the Outbound SSL Inspection Issues

---



#### Note

It is recommended that you install the August 2015 X-Press Update, which includes additional fixes for Outbound SSL inspection.

---

- **72271:** Facebook loads slowly or video does not play when Outbound SSL inspection is enabled.
- **71317:** Video streaming on Youtube does not work when Outbound SSL inspection is enabled.
- **71131:** duckduckgo.com loads slowly or does not open when Outbound SSL inspection is enabled.
- **71125:** Yahoo is unstable when Outbound SSL inspection is enabled.

### Fixes Not Related to the Outbound SSL Inspection Issues

---



#### Note

The Outbound SSL inspection feature does not support the SPDY protocol. See [technote 1903522](#) for more detail.

---



#### Note

This fixpack includes fixes for some CVEs. Check the security bulletins for more information.

---

- **74369:** HTTP GET requests that span more than one packet are not handled correctly, which results in incorrect Network Access policy matching.
- **73592:** MitM implementation does not use burst transmission to send rewritten SSL records. This change improves outbound SSL performance.
- **62017:** NAP rules intended to block unknown URLs do not work. If a network user accesses a URL that is listed in the Unknown URL web filter category, the Network Access Policy does not trigger the rule.
- **74228:** Dropped packet counters in packetif don't include dropped unanalyzed packets, which causes a network statistic error.
- **74092:** Possible crash with signal 49 timer expiration on TLS heartbeats when Inbound SSL inspection is enabled.
- **73861:** Simulation mode does not disable outbound SSL inspection. In Simulation mode, no frames are modified, dropped, or held. This change prevents unnecessary inspection in Simulation mode.
- **73783:** Many signal 49 watchdog timer expirations are reported in the log when the appliance is busy. When the main inspection thread is busy, it can delay sending a reset timer command to other inspection threads. The watchdog timer can send and log a false positive signal 49 expiration.

- **73690:** Simulation mode setting in the Protection Interfaces policy is not honored when Connection Table is full, which results in unanalyzed traffic being dropped.
- **73598:** The XGS 3100 hard drive might become locked if wipe operation is interrupted. The original wipe operation sets a temporary password, wipes the hard disk, then removes the temporary password. The wipe operation was changed on the XGS 3100 model to prevent the hard disk from locking.
- **73450:** The Chinese string of LMI performance level setting translation string is truncated.
- **73392:** On the XGS 5100 model, when Flexible Performance Licensing is set to 4 (MAX), and captive portal is enabled, the captive portal response is slow.
- **73391:** In the User Authentication Portal, Firefox save Password window tries to save password for "X," rather than username that is logged in.
- **73295:** The appliance crashes when no protection interfaces are enabled.
- **73231:** Improve suspicious program weakness based on source scan result.
- **73149:** Unnecessary event GLGSY0008W generated when creating snapshot in firmware versions 5.3.1.1 and 5.3.1.2.
- **72987:** Probable crash when processing anonymous ciphers due to use of uninitialized value.
- **72795:** Can only access captive portal from one side of the appliance for some protection interface pairs.
- **72741:** The Edit window in the OpenSignature policy indicates conflicting settings between multiple OpenSignature rules with the same settings.
- **72740:** The available list of response objects are empty when add or edit OpenSignature rules
- **72293:** The validation chain (the root CA and the intermediate CA must be uploaded in separate files) for the appliance certificate does not work, which results in the appliance certificate status being incomplete.
- **72490:** Migrated GX filter and service object names should reflect the object's contents to easily differentiate each object in the collection.
- **66870:** Add a tuning parameter `spad.event.queue.size` to change the event queue size to handle an event burst. This tuning parameter allows you to increase the event queue size, so that uncommitted events are not lost if SiteProtector is offline for a significant period of time.
- **66376:** Non-sequitur IPS events are not reported to matched IPS policy of the original connection, which results in incorrect Network Access Policy matching.

## Known Issues

Firmware update 5.3.1.3 contains the following known issues:

- Large file downloads may stall and eventually fail when downloading over HTTPS and using Outbound SSL Inspection.
- Websites using the SPDY protocol fail to load over HTTPS when using Outbound SSL Inspection.
- The statistic **Fps Dropped** is not displayed correctly in the LMI when unanalyzed policy is set to **Drop**.
- If you created an URL category object to block Unknown URL while running firmware versions 5.3.1.0, 5.3.1.1, or 5.3.1.2, then applied the 5.3.1.3 DBSP or firmware update, the Unknown URL category checkbox is deselected (defect 62017). After applying the firmware update or DBSP, you must select the Unknown URL category checkbox again, and then deploy the policy.

# 8

## 5.3.1 Release Notes

---

Extreme Security Threat Protection firmware version 5.3.1 is available.

### Overview

Extreme Security Threat Protection firmware version 5.3.1 is a firmware update for the XGS IPS network protection platform. This release provides the following updates to Extreme Security Threat Protection firmware version 5.3:

- Serviceability and support enhancements:
  - Display system CPU, memory, storage information in the command line interface.
  - Restart the following system services in the command line interface: packet processing, packet capture, LMI, SiteProtector communication, and license and update services.
  - View and search system logs in command line interface.
  - Ability to retrieve support files via SFTP.
- Response enhancements:
  - Support of TCP for syslog forwarding.
  - Events (rsyslog) forwarded over TCP in LEEF or non-LEEF format show the same details as the content that is sent to the SiteProtector System.
- Network Access Policy enhancements:
  - Ability to determine the packet source and then control traffic by IP or by identity, based on the HTTP X-Forward-For header.
- IPS Policy enhancements:
  - Ability to derive a new IPS object from an existing IPS object.
  - Prompt warning message when enabling non-sequitur events and status type events in a non-default IPS object.
- Performance: Support FPL5 (25G bps) on XGS 7100
- Miscellaneous updates and implementation changes:
  - Disabled Top 10 URLs and Web Categories dashboard widget.
  - Customers who are pushing the boundaries of Connections per Second rates are likely affected by gathering Top Ten URL metrics for the dashboard.
  - Disabled mDNS responder due to a possible security issue.
  - Support for mutual certificate authentication for communication between the Network Security appliance and the SiteProtector System

---

### Note



- 1 The Top 10 URLs and Web Categories dashboard widget is now disabled by default. You can enable this widget by changing the value of tuning parameter `tune.url.topten.tracking` to enabled and restarting the packet processing service.
  - 2 The Outbound SSL Inspection feature currently has several known issues that will cause inspection to fail for some websites when the client is using the latest Firefox or Chrome browsers. These issues are under investigation, and will be addressed in a future fix pack.
-

## Known Issues



### Note

The ISNP Outbound SSL Inspection feature currently has several known issues that will cause inspection to fail for some websites when the client is using Firefox or Chrome browsers. These issues are under investigation, and will be addressed in a future fixpack

- 1 If you assign multiple protection interface segments to the same subnet, only the first interface assigned to that segment works for portal user authentication. The connection to the portal server cannot be established.
- 2 After you change a login password using SSH or the management console password expiration prompt, SiteProtector might fail to retrieve certain Security Network Protection agent information such as Users and Groups objects. The password change by SSH or Management console shell due to password expiration uses an Open SSH shell. This causes the agent credentials stored in SiteProtector to be out of sync with the appliance. To avoid this issue, or to correct the problem after it occurs, change the login password using the local management interface.
- 3 The system event log displays an error when the packet processing service is restarted. When you restart the packet processing service, the protection interfaces going offline and coming back online create events in the Events log. If a DCA download is in progress, the following error message is also displayed in the Events log: An error occurred performing an application database update. This is a known issue and expected behavior.
- 4 By default, the Top 10 URLs and Web Categories dashboard widget counts only URLs reported by Network Access Policies that have a response object. To enable the widget to count all URLs, you can change the value of tuning parameter `tune.url.topten.tracking` to enabled.
- 5 If you disable all protection interfaces, packet processing no longer functions. This causes Site Protector to display a failed health check for the appliance. It also causes other functions to fail, such as the CLI command `show interface`.
- 6 The default schedule object policy migrated from a previous firmware version might cause the following error message to appear in the system log: `Element '{http://www.iss.net/cml/alps/schedule_objects}policy': Character content other than whitespace is not allowed because the content type is 'element-only'`. Disregard this error. There is no functional impact.
- 7 If you are using Outbound SSL Inspection and enable the "Block connection if server certificate is invalid" option in the SSL Inspection Settings, many HTTPS sites are blocked. FNXSII001E system events are generated with the message "unable to get local issuer certificate." Disable this setting to allow the connection to proceed past the TLS handshake.
- 8 If you are using Outbound SSL Inspection, SSL/TLS connections that negotiate the use of TLS ALPN extension and support for TLS status request extension (example `https://www.yahoo.com`) are not decrypted and therefore do not have their cleartext payloads inspected.
- 9 If you are using Outbound SSL Inspection, network users using Firefox 37 and Chrome 42 cannot connect to web sites that support TLS False Start.
- 10 If you are using Outbound SSL Inspection, some pages do not load or only partially load due to incorrect TCP ACK values, window size manipulation, and keep-alive handling. This might also impact large file downloads.
- 11 Outbound SSL Inspection is not performed on connections to Google web sites from a Chrome browser. No impact to end user.
- 12 In 5.3.0.x firmware, if you have any custom rules in the Management Access Policy that contain address objects and are deployed from the SiteProtector system, the incorrect format of the policy causes the firmware 5.3.1 upgrade to fail. Use the following workaround:

- a Apply the latest SiteProtector DBSP first, and then migrate your policies from 5.3.0.x to 5.3.1 using the SiteProtector system.
- b Remove any Management Access Policy rules that contain address objects in 5.3.0.x Agent Version, and deploy to the agents.
- c Perform the 5.3.1 firmware upgrade.