Extreme Security Threat Protection Installation and Configuration Guide

9034908

Published October 2015

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, tricks, 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 Networks Security API Reference Guide*
- *Extreme Networks Security Application Configuration Guide*
- *Extreme Networks Security Ariel Query Language Guide*
- *Extreme Networks Security DSM Configuration Guide*
- *Extreme Security DSM Configuration Guide Addendum*
- *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 Sources User Guide*
- *Extreme Networks Security Managing Log Sources Guide*
- *Extreme Networks Security Offboard Storage Guide*
- *Extreme Security Release Notes*
- *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 Risk Manager Migration Guide*
- *Extreme Networks Security Risk Manager User Guide*
- *Extreme Networks Security Troubleshooting System Notifications Guide*
- *Extreme Networks Security Upgrade Guide*
- *Extreme Networks Security Vulnerability Manager Release Notes*
- *Extreme Networks Security Vulnerability Manager User Guide*
- *Extreme Networks Security WinCollect User Guide*
- *Extreme Networks SIEM Administration Guide*
- *Extreme Networks SIEM Getting Started Guide*
- *Extreme Networks SIEM High Availability Guide*
- *Extreme Networks SIEM Troubleshooting Guide*
- *Extreme Networks SIEM Tuning Guide*
- *Extreme Networks SIEM Users Guide*
- *Migrating Extreme Security Log Manager to Extreme SIEM*

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 Getting Started

After you determine where to place the Security Network Protection appliance on your network, you can install network cabling and connect to the local management interface to configure initial appliance settings.

Installing or replacing a network interface module

Your can install a variety of different network interface modules on your Security Network Protection appliance.

Turn off the appliance by either shutting the appliance down from the Local Management Interface (LMI) or by pressing the power button on the front of the appliance.

Perform the following steps to install or replace a network interface module.

1 Unplug all power cords to the appliance.

2 Grasp the blue latch on the back of the appliance and pull outward.

3 Pull the lever toward you to pull out the module, as shown in Figure 1.

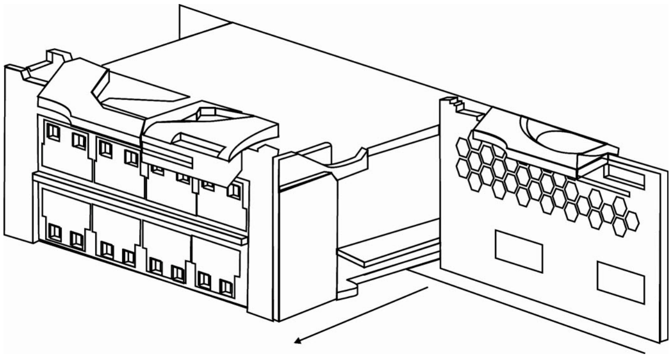


Figure 1: Removing a network interface module from the back of the appliance

4 Unpack the new network interface module.

> Attention
> Make sure that the gold connectors at the rear of the module do not come into contact with your hands or with the packing material as you unpack the network interface module. Avoid damaging the gold connectors against the chassis as you insert the replacement module.

5 Carefully align the network interface module, and fully insert and push the module forward into the chassis until the module is in place.
6 Push the blue latch on the back of appliance back in place.
7 Plug in all power cords to the appliance.
8 Turn on the appliance by pressing the power button on the front of the appliance.
9 Verify that the LCD Panel on the front of the appliance is illuminated.

Check whether the module is working correctly by logging in to the LMI and verifying that the new module was recognized by the appliance.

Connecting cables and starting the appliance

Connect the Security Network Protection appliance to your network after you determine where you want to place it on the network. Install network cabling and verify that traffic flows before you turn on the appliance.

1 Connect the power cable to the Security Network Protection appliance.
2 Connect Management Interface 1 to the network you want to use to manage the Network Protection appliance.
3 Connect the network cables to the protection interfaces.

   You must connect both protection interfaces in a pair to enable traffic to flow through the Security Network Protection appliance.
4 Ping a computer on the network on the other side of the Network Protection appliance to verify that traffic passes.
5 Turn on the Security Network Protection appliance.

Navigate to the local management interface to configure network settings for the Security Network Protection appliance.

Important
If you install an XGS appliance between a proxy server and user workstations, then users must configure their web browsers to exclude the IP address of the XGS appliance protection interface from the proxy settings. If users do not exclude this IP address, the browser is not redirected to the requested website.

Accessing the local management interface

Access the Web-based local management interface to perform first-time configuration on the Security Network Protection appliance.

Use the LCD panel to determine the IP address of the appliance and connect to the LMI.

Using the LCD

Use the LCD panel to determine the IP address of the Security Network Protection appliance.

1 Press the OK button on the LCD panel to view the main menu.

2 Use the arrow buttons to select **IP Address**, and then press **OK**.

> Note
>
> The LCD panel displays the IP address of the Security Network Protection appliance. Make a note of the address.

3 Type the IP address into your browser to access the local management interface.

Using zero configuration networking

Zero configuration networking allows you to automatically create a network of devices without having to manually configure a DHCP server, DNS services, or network settings for each device that you want to connect to that network.

How zero configuration networking works with the Security Network Protection appliance

You can use zero configuration networking applications to discover the Security Network Protection appliance on your network to configure network settings.

Zero configuration networking is based on the following three elements:

- Automatic IP address selection for networked devices (which eliminates the need to configure a DHCP server)

  If the Security Network Protection appliance does not have an IP address assigned to it, then zero configuration networking uses link-local addressing to create an IP address in a range from 169.254.1.0 to 169.254.254.255. When an IP address is chosen, the link-local process sends out a query with that IP address onto the network to see if the IP address is already in use. If there is no response, the IP address is then assigned to the Security Network Protection appliance.
- Automatic domain name resolution and distribution of computer host names (which eliminates the need to configure a DNS server)

  Zero configuration networking implements multicast DNS (mDNS). mDNS allows the Security Network Protection appliance to select a domain name in the local namespace and then broadcast that name using a special multicast IP address, allowing other devices on the network to connect to it by name instead of by numbered IP address.
- Automatic location of network services through DNS service discovery (which eliminates the need for you to set up a directory server)

  Zero configuration networking enables the Security Network Protection appliance to use standard DNS queries to discover devices registered on the network that are broadcasting the services that they provide.

Zero configuration networking applications

You can use the following zero configuration networking applications with this release of the Security Network Protection appliance:

- Bonjour

Bonjour is a zero configuration networking application from Apple that allows you to automatically create a network of devices in which hosts and services can connect to one another without requiring any user configuration. The services for each device are automatically registered on the network, and can be discovered by other devices on the network.

If you are using a Windows™ computer, you must install the Bonjour plug-in for Windows™.

If you are using a Mac OS computer, there is no additional configuration needed because the Bonjour service discovery is already built into the Mac operating system.

- Avahi

  Avahi is an implementation of zero configuration networking that you use with Linux™ operating systems. Avahi is installed by default on most Linux™ systems and can run multicast DNS and DNS service discovery.

Using a DNS-SD browser to discover services

Use a DNS-SD enabled browser to discover the Security Network Protection appliance on your network and access the local management interface.

DNS-SD plugins are available for most web browsers. You must install the appropriate DNS-SD plugin to use zero-configuration networking on your browser. If you are using a Windows™ computer, you must also install the Bonjour plug-in for Windows™.

1. Open your web browser and open a DNS-SD browser window.
2. In the services list, select the Security Network Protection appliance you want to configure.

   The mDNS service advertisement is ***Product name Product version model*** [***serial number***].

   ISNP 5.1 XGS 5100 [*serial number*]

   Tip
   The serial number is located on the Security Network Protection appliance hardware.

3. On the Certificate window, click Accept Certificate.
4. Navigate to the listed IP address to access the local management interface.

Using Bonjour from a Windows™ command line to discover services

If you are using a Windows™ computer, you can use Bonjour through a command line interface (CLI) to browse for services that are being broadcast on the local network.

DNS Service Discovery (DNS-SD) protocol

The DNS Service Discovery (DNS-SD) protocol can identify and discover devices on the network that are enabled with the zero configuration standard. DNS-SD uses multicast DNS (mDNS). mDNS sends packets to every node on the network to resolve duplicate host names and to query the network for services.

From a Windows™ command-line, you can use the **dns-sd** command to browse for services that are being broadcast on the local network by mDNSResponder (a Bonjour system service that uses Multicast DNS Service Discovery for discovery of services on the local network).

Link-local address space

The range for the link-local address space is 169.254.0.0 - 169.254.255.255. However, 169.254.0.1 - 169.254.0.255 and 169.254.255.0 - 169.254.255.255 are reserved for future use.

DNS queries that end in .local are sent to the address 224.0.0.251 (for IPv6: FF02::FB / FF02:0:0:0:0:0:0:FB) which is reserved for mDNS. Any packets that are sent to these addresses are not forwarded beyond the local link or forwarded to the local link from outside the network. Any link-local multicast packet that is sent remains on the local link. Any link-local multicast packets that are received must originate from the local link.

Using the DNS-SD protocol to browse for services

Type **`dns-sd -B _ssh._tcp`** at the command line to see all SSH service broadcasts on the network.

Looking up the host name of a service

Type **`dns-sd -L "ISNP 5.1 XGS 5100 [`*`serial number`*`]" _ssh._tcp`** at the command line. The serial number is located on the Security Network Protection appliance hardware.

Important
Make sure you use quotation marks around the instance name.

After you discover the Security Network Protection appliance on your network, navigate to the appliance host name or IP address in your browser to access the local management interface.

Using Avahi command-line programs to discover services

If you are using a Linux™ computer, you can use Avahi to browse for services that are being broadcast on the local network.

Note
Before you begin, you must install the Avahi RPM package for the Linux™ operating system you are using before you can use these command-line programs.

Using the avahi-browse command-line program /usr/bin/avahi-browse

Use the avahi-browse command-line program to do these things

- browse for all mDNS broadcasts on the network
- resolve the host name and IP address of the device performing the broadcasts

Avahi-browse command-line options: avahi-browse `<options> <service type>`

Use the following command-line options with the avahi-browse program:

`-d <domain>`	Specifies the domain in which you want to browse for services. If you do not specify a domain, then all domains are browsed. The Security Network Protection appliance broadcasts on the .local domain.

`--resolve`	Displays the host name and the IP address of the Security Network Protection appliance, including the service advertisement string. Example "ISNP 5.1 XGS 5100 [*`serial number`*]"
`-t`	Terminates the avahi-browse program after dumping the current list of named services. The avahi-browse program no longer runs or listens for new broadcasts.
`-a`	Displays all service broadcasts on the network. You do not need to specify a `<`*`service type`*`>` with this command-line option.
`--no-db-lookup`	Instructs the avahi-browse program not to translate service types. Example Translating `_ssh._tcp` to a friendlier name such as "SSH Remote Terminal" or translating `_http._tcp` to "website"

After you discover the Security Network Protection appliance on your network, navigate to the appliance host name or IP address in your browser to access the local management interface.

Using the avahi-discover-standalone command-line program /usr/bin/avahi-discover-standalone

The avahi-discover-standalone command-line program is an X Window program that displays all the discoverable services across all domains. You can run this program only from an X Window session.

This command-line program does the same thing that the **`avahi-browse -a --resolve`** command does. After you discover the Security Network Protection appliance on your network, type the appliance host name or IP address in your browser to access the local management interface.

2 Configuring initial appliance settings

You can use the local management interface or the command line interface wizard to configure initial appliance settings.

Local management interface

The Security Network Protection appliance offers a browser-based graphical user interface for local, single appliance management.

To log in to the local management interface, type the IP address or host name of your Network Protection appliance into your web browser.

Tip
You can also manage your appliance using the command-line interface.

Use the default credentials to log in to the LMI the first time:

- User Name: admin
- Password: admin

After you log in for the first time, use the first-time configuration pages to change your password.

To log out of the local management interface, click Logout.

Security Network Protection was developed by using research from the X-Force® research and development team. Click the link on the login page to learn more about X-Force.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

Compatibility

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

- Internet Explorer 10 or 11

- Firefox 28 and newer
- Google Chrome 34 and newer

For more information on supported browsers, see technote #1595890 on the IBM Support Portal.

Configuring initial appliance settings in the LMI

When you log in to the Security Network Protection appliance for the first time, a Welcome page appears, prompting you to configure initial settings.

To begin, you must accept the Software License Agreement.

1 Select your language and then read the Software License Agreement.

2 Select **I agree** to accept the Software License Agreement and then click **Next Page**.

Use the first-time configuration wizard to configure the remaining settings.

Enabling FIPS mode

If you need your installation to comply with Federal Information Processing Standards (FIPS), you must enable FIPS mode during the initial configuration.

Enable FIPS mode only if you must comply with FIPS requirements. There is no advantage to enabling FIPS mode if your installation does not require it. To disable FIPS mode, you must re-image the appliance. When you re-image the appliance, all the policy configuration and appliance settings are lost.

Note
If you enable FIPS mode on your appliance and plan to use the user authentication feature, you must enable TLS 1.0 and TLS 1.1 during the FIPS configuration process to enable the use of Mozilla Firefox or Google Chrome browsers. You do not need to enable TLS 1.0 and TLS 1.1 if all of your network users use Microsoft Internet Explorer.

1 On the Welcome page, click **FIPS Mode**.

2 To enable FIPS mode, select **Enable FIPS 140-2 mode**.

Note
NIST SP800-131a prohibits the use of TLS protocols, version 1.1 or earlier. When you enable FIPS mode on the Security Network Protection appliance, TLS V1.0, TLS V1.1, and all versions of SSL are automatically disabled for LMI connections. Because TLS V1.2 support is not available in most browsers, you can configure your appliance to accept TLS V1.0 and V1.1 during the initial setup.

3 To allow users to connect to the LMI using TLS version 1.0 or 1.1, select one or both of the following options:

- Allow TLS V1.0 for LMI sessions
- Allow TLS V1.1 for LMI sessions

Tip
After you complete initial setup, you can configure LMI TLS settings using the following advanced tuning parameters:

- lmi.security.tlsv10 = ***true/false***
- lmi.security.tlsv11 = ***true/false***

Important
Change advanced tuning parameter values only under the supervision of Extreme Support.

4 Click Save Configuration.

5 Click Yes to confirm.

Note
When you enable FIPS mode, the appliance restarts to run the required integrity checks. After the appliance restarts, log in again to continue the setup process.

Installing a license

You must install a current license file to receive updates to the Network Protection appliance. To obtain a license key, refer to Obtaining a License Key on page 16.

You must have an extra license to use the following appliance features:

Location	Description
Application ID	Enables the appliance to receive URL Category and Web Application database updates.
Flexible Performance	Enables the configuration of appliance performance levels. When the appliance performance level is increased, it uses more system resources.
IP Reputation	Enables the appliance to receive IP Reputation database updates.
SSL Inspection	Enables the appliance to inspect encrypted connections.

1 Optional: If you are not configuring your appliance for the first time, click Manage > Licensing and Performance.

2 On the Licensing page, click Select License and locate the license file that you want to install.

3 Select the license file and click Open.

Tip
If you use one of the following browsers, you can select multiple license files at one time: Firefox, Chrome, or Internet Explorer 10. (Internet Explorer 9 does not support multiple file selection.)

4 Click Save Configuration.

5 Optional: From one of the following locations, change the appliance performance level:

Local Management Interface	Move the Current Performance Level slider, and then click Save Configuration Restriction Flexible performance options are not available when you are setting up the appliance for the first time.
SiteProtector™ System	To change the number of performance level increases you are using, perform the following actions: 1 Select the Policy view. In the My Sites pane, expand the Locally Configured Agents menu item, and then select your Network Protection agent. 2 In the Local Policies pane, select Flexible Performance, and then click Action > Open. 3 Move the Current Performance Level slider, and then click Save Configuration To view the number of allocated performance increase units, perform the following actions: 1 Click Tools > Licenses > Agent/Module. 2 In the Agent/Module License Information window, select the Summary tab. The number of allocated performance increase units is listed in the In Use column. Note A license can include multiple performance increase units. Each performance increase uses one performance increase unit per appliance.

Note

OCNID stands for Order Confirmation Number and ID.

A warning message informs you that the change is undeployed. To deploy the change, click Click here to review the changes or apply them to the system.

If you are setting up the appliance for the first time, continue the first-time setup process by installing a settings snapshot. If you are installing licenses for new features, such as Application ID, IP Reputation, and SSL Inspection, then configure options for those features.

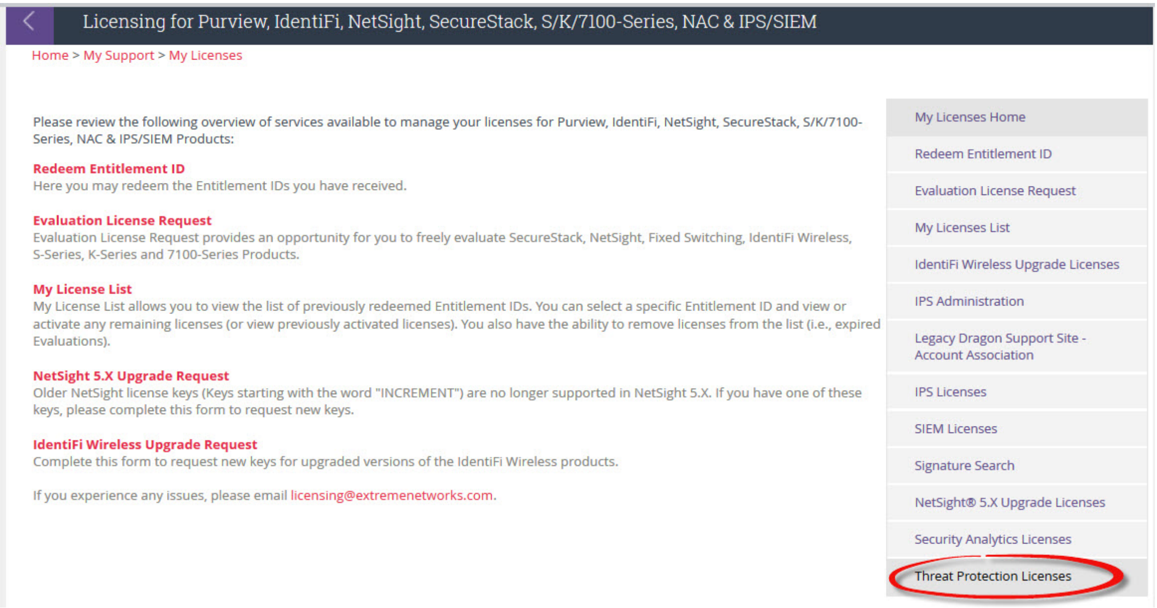
Obtaining a License Key

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.

3 Click Threat Protection Licenses from the menu bar on the right.



Licensing for Purview, IdentiFi, NetSight, SecureStack, S/K/7100-Series, NAC & IPS/SIEM

Home > My Support > My Licenses

Please review the following overview of services available to manage your licenses for Purview, IdentiFi, NetSight, SecureStack, S/K/7100-Series, NAC & IPS/SIEM Products:

Redeem Entitlement ID
Here you may redeem the Entitlement IDs you have received.

Evaluation License Request
Evaluation License Request provides an opportunity for you to freely evaluate SecureStack, NetSight, Fixed Switching, IdentiFi Wireless, S-Series, K-Series and 7100-Series Products.

My License List
My License List allows you to view the list of previously redeemed Entitlement IDs. You can select a specific Entitlement ID and view or activate any remaining licenses (or view previously activated licenses). You also have the ability to remove licenses from the list (i.e., expired Evaluations).

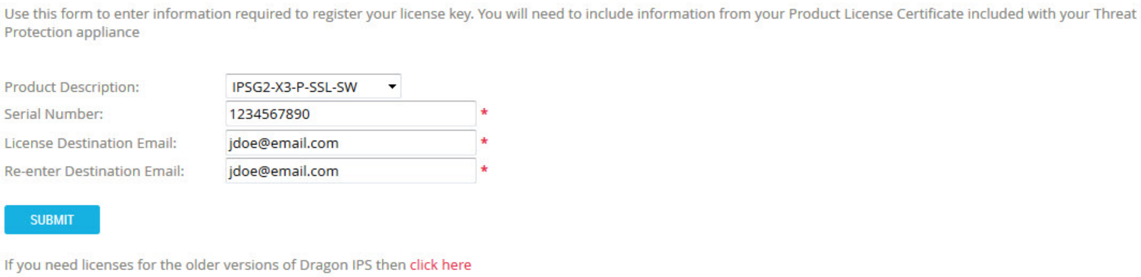
NetSight 5.X Upgrade Request
Older NetSight license keys (Keys starting with the word "INCREMENT") are no longer supported in NetSight 5.X. If you have one of these keys, please complete this form to request new keys.

IdentiFi Wireless Upgrade Request
Complete this form to request new keys for upgraded versions of the IdentiFi Wireless products.

If you experience any issues, please email licensing@extremenetworks.com.

My Licenses Home
Redeem Entitlement ID
Evaluation License Request
My Licenses List
IdentiFi Wireless Upgrade Licenses
IPS Administration
Legacy Dragon Support Site - Account Association
IPS Licenses
SIEM Licenses
Signature Search
NetSight® 5.X Upgrade Licenses
Security Analytics Licenses
Threat Protection Licenses

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:	IPSG2-X3-P-SSL-SW
Serial Number:	1234567890 *
License Destination Email:	jdoe@email.com *
Re-enter Destination Email:	jdoe@email.com *

If you need licenses for the older versions of Dragon IPS then click here

4 Select your product from the Product Description drop-down list.

5 Type your product's serial number in the Serial Number field.

6 Enter and confirm the email address to which the license should be sent.

7 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.

Installing a settings snapshot

You can install a settings snapshot during first time configuration to restore prior configuration and policy settings.

You can download a settings snapshot to restore the Security Network Protection appliance in case of system failure. You can also apply a settings snapshot that you downloaded from another appliance.

1 On the Settings Snapshots page, click Browse.

2 In the Snapshots pane, use one or more of the following commands:

Option	Description
New	To create a snapshot, click **New**, type a comment describing the snapshot, and then click **Submit**.
Edit	To edit the comment for a snapshot, select the snapshot, click **Edit**, type a new comment, and then click **Submit**.
Delete	To delete snapshots, select one or more snapshots, and then click **Delete**.
Apply	To apply a snapshot, select the snapshot, and then click **Apply**. Note If configuration or policy versions are newer than the firmware version, the settings are rejected. If the configuration and policy versions are older than the firmware version, the settings are migrated to the current firmware version.
Download	To download a snapshot, select the snapshot, click **Download**, browse to the drive where you want to save the snapshot, and then click **Save**. Note If you download multiple snapshots, the snapshots are compressed into a .zip file.
Upload	To upload snapshots, click **Upload**, browse to the snapshots you want to upload, select the snapshots, and then click **OK**. Note You can only upload one snapshot at a time.
Refresh	To refresh the list of snapshots, click **Refresh**.

Changing passwords

Use the Password page to change the password you use to access your Security Network Protection appliance.

1 On the **Password** page, type the password you want to change in the **Current Password** box.

2 To change the timeout interval for administrator sessions, type or select a value (in minutes) in the **Session Timeout** box.

3 Type your new password twice to confirm it, and then click **Save Configuration**.

4 When you see the confirmation message, click **Next Page** to configure the next setting.

Configuring management interfaces

Use the **Management Interfaces** page to view and configure the network management interfaces for the appliance.

Navigating in the Local Management Interface: Click **Manage** > **Management Interfaces**.

Navigating in the SiteProtector™ System:

1 Select the **Policy** view.

2. In the My Sites pane, expand the **Locally Configured Agents** menu item, and then select your Network Protection agent.
3. In the **Local Policies** pane, select **Management Interfaces**, and then click **Action** > **Open**.

> Remember
> When you change the IP address of the management interfaces, connect your web browser to the new IP address for future sessions.

> Note
> Changing the appliance host name causes the system to reset the network connection. You must reconnect after the network connection is reset. This process does not interrupt traffic through the appliance protection interfaces.

1. On the **Management Interfaces** page, type a **Host name**.
2. To enable network users to locate the appliance by using zero configuration networking, select **Advertise management interface using multicast DNS**.
3. Select the **Default Interface**.
4. Optional: To configure a secondary management interface to inject TCP reset frames in monitoring mode make the following selections:
   a. On the tab for the interface you want to use as a secondary management, select **Enable *interface name***.
   b. On the **General** tab, select the secondary management interface in the **Use as monitoring mode TCP reset interface** list.
   c. Optional: To ensure that injected TCP resets are correctly routed to their destination, you can specify the MAC address of the gateway that is connected to the same network segment as the TCP reset interface. Type the **Gateway MAC address** to use as the destination of the TCP reset frame in the **Gateway MAC Address** field.

   > Restriction
   > You cannot select the default management interface as the TCP reset interface.

5. Click the tab for the primary interface, and then configure the following IPV4 and IPV6 options:

Auto/Manual	Choose the appropriate mode: • Select **Auto** to acquire an IP address from a DHCP server. • Select **Manual** to specify a static IP address, Netmask, and Gateway (IPv4) or Prefix (IPv6).
Address	If you selected **Manual** mode, type the IP address that you want to use for the interface.
Gateway	If you selected **Manual** mode, type the Gateway for the interface.
Netmask (IPv4)	If you selected **Manual** mode for IPv4, type the Subnet Mask for the interface.
Prefix (IPv6)	If you selected **Manual** mode for IPv6, type the prefix length for the interface.

6. Click the **DNS** tab, and then configure the following options:

Auto/Manual	Choose the appropriate mode: • Select **Auto** to acquire DNS server addresses from a DHCP server. • Select **Manual** to specify DNS servers.

Primary DNS	Specifies the IP address of the primary DNS server.
Secondary DNS	Specifies the IP address of the secondary DNS server.
Tertiary DNS	Specifies the IP address of an optional third DNS server.
DNS Search Path	Specifies one or more DNS search paths. Use a comma to separate each path.

7 Click the tab for the secondary interface, and then configure the following IPV4 and IPV6 options:

> Note
> IP addresses are not assigned to an interface that is designated as the TCP reset interface for monitoring mode.

8 To enable more management interfaces, select Enable ***interface name*** on the related interface management tabs.

9 Click Save Configuration.

Configuring host name and DNS information

Use the Hosts page to set any network options, such as a host name, a DNS server, or a search path.

1 On the Hosts page, click Edit, and then configure the following options:

Host Name	Specifies a name for the host.
Multicast DNS	Specifies whether to enable Multicast DNS (mDNS). Enabling mDNS will broadcast its availability so that you can configure the appliance using an mDNS browser utility, such as Bonjour. Note When you disable the mDNS Responder, the appliance does not broadcast a local management web interface or SSH. The appliance firewall will reject multicast packets to destination address 224.0.0.251.
Primary DNS	Specifies the primary DNS server IP address.
Secondary DNS	Specifies the secondary DNS server IP address.
Tertiary DNS	Specifies an optional third DNS server IP address.
Search Paths	Specifies one or more DNS search paths. Type each path separated by a comma.

2 Click Save Configuration.

3 Click Next Page to configure the next setting.

Configuring protection interfaces

Use the Protection Interfaces page to configure the Protection Mode and the Speed and Duplex mode for each interface.

> Important
> If your appliance is deployed on a VMware platform, you must perform special configuration tasks. For more information about configuring your virtual appliance, see Configuring the Network Protection for VMware on page 26.

Navigating in the Local Management Interface: if you are not configuring your appliance for the first time, click Manage > Protection Interfaces.

Navigating in SiteProtector™ Management: select the Protection Interfaces policy.

1. On the Protection Interfaces page, select a protection interface pair, and then click Edit.
2. Configure the following options:

Enable	Enables or disables the protected interface pair.
Inspection Mode	Use this setting to determine how the appliance monitors and inspects traffic. Note The default inspection mode is Protection. • Protection. The appliance monitors all traffic inline and blocks packets according to how you configured the Network Access Policy rules. • Simulation. The appliance monitors traffic inline, but does not block any traffic. Instead, the appliance monitors traffic and provides passive responses. • Monitoring. The appliance monitors traffic from a tap, hub, or span (mirror) interface of switches. Interfaces that are configured in Monitoring mode are not paired and each one can be used to monitor a different network segment. Tip To select or disable high availability (HA) modes, use the High Availability tab on the Protection Interfaces page.
Maximum Transmission Unit	The largest size packet or frame to be accepted by each protection pair. Type a value of 68 - 9216 bytes. Note The default value is 1500, which is Ethernet standard MTU. Larger MTU values can provide greater efficiency for bulk protocol throughput. However, larger MTU values can increase lag and minimum latency.
Unanalyzed Policy	Use this setting to determine what happens to network traffic that cannot be fully analyzed. • Forward. The appliance performs connection tracking if possible. It continues to discard packets that belong to blocked connections. Other packets are transmitted. • Drop. The appliance discards any packets that cannot be fully analyzed.
Propagate Link	Use this setting with inline protection interface pairs. • Yes. The link on the corresponding inline interface breaks when one of the links is down (such as when a cable is broken or disconnected). • No. The link on the corresponding inline interface is left intact when one of the links is down. • Auto. The appliance selects the appropriate setting that is based on the interface mode. In inline modes, link propagation is enabled. In Monitoring mode, link propagation is disabled.
Hardware Bypass Mode	Select the mode to allow or to prevent traffic if the appliance fails or is powered off: • Auto. In non-HA modes, all traffic is allowed to pass through the appliance (fail open). In HA mode, interface links are closed and traffic is prevented from passing through the appliance (fail closed).

	• Fail Open. Allows all network traffic to pass through the appliance. • Fail Closed. Closes the links for the interface pair and prevents any network traffic from passing through the appliance.
Interface Settings	Select the link speed and mode for each interface in a protected interface pair. • Auto. Allows two interfaces on a link to select the best common mode automatically, the moment a cable is connected. This setting is the best option for most environments. Exceptions include environments with a switch or other network device that does not support auto-negotiation, or in situations where the auto-negotiation process takes too long to establish a link. • 10 Mb Full Duplex. Allows information to be transmitted at 10 megabits per second in both directions at the same time. • 10 Mb Half Duplex. Allows a device to either transmit or receive at 10 megabits per second, but not at the same time. • 100 Mb Full Duplex. Allows information to be transmitted at 100 megabits per second in both directions at the same time. • 100 Mb Half Duplex. Allows a device to either transmit or receive at 100 megabits per second, but not at the same time. • 1000 Mb Full Duplex. Allows information to be transmitted at 1000 megabits per second in both directions at the same time. • 10,000 Mb Full Duplex. Allows information to be transmitted at 10,000 megabits per second in both directions at the same time.
TCP Resets (Monitoring mode only)	This setting indicates the interface that is used to inject TCP reset frames to terminate TCP connections in monitoring mode. The appliance cannot block or reject traffic in monitoring mode, but it can terminate TCP traffic connections. Select one of the following settings: • This interface. The appliance injects the TCP reset frame into the same monitoring interface that received the TCP traffic that triggered an IPS event or that matched a Network Access Policy rule. This option cannot be used if the monitoring interface is connected to a read-only link, such as a read-only tap. • TCP reset interface. The appliance injects the TCP reset frame into the management interface that is designated as the TCP Reset interface. You must configure a management interface as the TCP Reset interface on the Management Interfaces page. • Disabled. The appliance does not inject any TCP resets for the traffic that is received on this monitoring interface. Important Terminating TCP connections by injecting resets is not guaranteed to be effective in Monitoring mode. To ensure effective blocking, use Protection mode.
MTU (Maximum Transmission Unit)	The largest size packet or frame to be accepted by each protection pair. Type a value of 68 - 9216 bytes. Note The default value is 1500, which is Ethernet standard MTU. Larger MTU values can provide greater efficiency for bulk protocol throughput. However, larger MTU values can increase lag and minimum latency. Larger packets are also more likely to become corrupted.
IPv4/IPv6 Settings	This setting provides the IP address that users are redirected to by a Network Access Policy rule that requires user authentication or that blocks HTTP traffic.

	Enter a static IP address that the client network can reach and an appropriate netmask. The gateway is the next hop to the external network (usually this address is the IP address of your router). Note A separate IP configuration is required for IPv4 and IPv6 traffic. Only the type of traffic that is inspected on your network requires a protection pair IP address. Select either **IPv4 Settings** or **IPv6 Settings**, and then type the appropriate information in each box. **IPv4 Settings**: • Address • Netmask • Gateway **IPv6 Settings**: • Address • Prefix • Gateway

Note

Before you configure a protection interface pair to decrypt SSL traffic, you must assign an IP address to the protection pair.

3 Click **Submit**.

4 Optional: If you are configuring your appliance for the first time, click **Next Page** to configure the next setting.

If you are not configuring your appliance for the first time, you must deploy the updated policy for the changes to take effect.

Configuring date and time settings

Use the **Date/Time Configuration** page to configure the date, time, time zone, and NTP server information.

1 On the **Date/Time** page, click **Edit**.

2 Configure the following options:

Option	Description
Time Zone	Specifies the time zone for the appliance.
Date/Time	Specifies the day, month, year, and time for the appliance.

Option	Description
NTP Server address	Lists the NTP (NIST Internet Time Service) servers the appliance uses. You can enter multiple NTP servers, separated by commas.

Note
You cannot set the Time Zone or Date/Time using the SiteProtector™ System console. You can only specify NTP server addresses.

3 Click Save Configuration.

4 Click Next Page to configure the next setting.

Completing configuration settings

Review the summary of the Security Network Protection management settings and all configuration settings before completing the setup process.

Verify that all settings are correct, and then click Complete Setup.

The appliance might take several minutes to complete the setup process.

After the setup process is complete, you must log in to the Local Management Interface to access the appliance.

CLI initial appliance settings wizard

The initial appliance settings wizard runs the first time an administrator logs in to the command-line interface (CLI) of an unconfigured appliance.

Navigation

You can move between screens in the wizard using the following options:

- **p**: Previous Screen
- **n**: Next Screen

To cancel the setup process at any time, use the exit command.

Modules

You must configure the following modules to set up your appliance:

Module	Description
Welcome	Describes the appliance settings that you can configure using the wizard.
Software License Agreement	Describes the appliance license agreement, machine code terms, Extreme Networks® terms, and non-Extreme terms.
FIPS mode	Allows you to enable FIPS mode, if necessary. If you finish the initial setup without enabling FIPS mode, you cannot enable it later without reinstalling the appliance. When

Module	Description
	you enable FIPS mode, the appliance restarts to run the required integrity checks. After the appliance restarts, log in again to continue the setup process. Note Do not enable FIPS mode if you do not need to be compliant with FIPS or if your firmware is not FIPS certified.
Password Configuration	Allows you to change your password.
Host Configuration	Allows you to change the host name.
Management Interface Settings	Allows you to configure the management network interfaces. Displays device settings and the current working-set policy for the primary and secondary interfaces.
DNS Configuration	Allows you to configure the DNS servers used by the appliance.
Time Configuration	Allows you to configure the time, date, and time zone on the appliance.
FIPS TLS Configuration	Allows you to configure Transport Layer Security (TLS) communication for browsers connecting to the LMI. Note This module appears only if you have enabled FIPS mode.

Configuring initial appliance settings by using a serial console connection

Use a terminal emulation program to configure initial settings for the Network Protection appliance.

1 Connect the serial console cable to the appliance and to a computer.

> Note
>
> Your Network Protection appliance package might contain a USB serial console cable and a DB-9 serial console cable, or the package might contain only a DB-9 serial console cable. If you use the USB serial console cable and your computer does not recognize the cable, you might need to install the device driver.
>
> The drivers are available for download from http://public.dhe.ibm.com/software/security/products/infrastructure_protection/USBDeviceDrivers or from the driver supplier at http://www.prolific.com.tw/US/ShowProduct.aspx?p_id=225&pcid=41.

2 Connect to the appliance with Hyperterminal or another terminal emulation program by using the following settings:

Option	Description
Communication Port	Typically `COM1`
Emulation	`VT100`
Bits per second	`9600`
Data bits	`8`
Parity	None

Option	Description
Stop bits	1
Flow control	None

3 Follow the instructions listed in the documentation for the terminal emulation program to configure initial appliance settings.

Configuring the Network Protection for VMware

To configure the Network Protection appliance for VMware, you must perform a first-time setup and perform special configuration tasks for some features.

After the Network Protection appliance is deployed on a virtual network, the appliance behaves like a hardware appliance. However, it requires special configuration for some features.

Note
Product information that is related to hardware components does not apply to the Network Protection appliance if the appliance is deployed on a virtual network.

3 Installing firmware

This chapter provides important information about installing firmware on the Security Network Protection appliance to resolve software and configuration errors that cause your appliance not to work properly.

Installing firmware from a USB boot drive: Windows™ or Linux™ OS

Create a USB boot drive in a Windows™ OS and use it to install firmware on the Network Protection appliance.

You might choose to install new firmware to resolve software and configuration errors that cause your appliance not to work properly. For example, you can use this procedure to install new firmware on an appliance that does not boot due to a software error.

Refer to the Extreme Support Portal for help troubleshooting appliance problems.

1. Download the appliance firmware from the Extreme extranetand save it to a secure host in your network.
2. Insert the USB flash drive into a USB port on the same host and note where the operating system assigns the USB flash drive.
3. Use an image writer program to overwrite the contents of the USB flash drive with the firmware image.

   Tip
   Common writer programs for Windows™ include Win32DiskImager.exe and USB Image Tool. USB ImageWriter is included in most Linux™ distributions.

4. Turn off the appliance.
5. Connect the USB flash drive to the appliance and turn the appliance on.

   The appliance boots from the USB boot drive.

6. Log on to the installer command-line interface as an administrator.
   - `install login: admin`
   - `password:admin`

Tip
You can type `help` for a list of commands available in the current mode.

7. Type `restore`.
8. Type **YES** and press Enter.

Note
The installation takes approximately 30 minutes to complete.

The firmware is installed and the appliance restarts.

Installing firmware from a USB boot drive: Mac OS

Create a USB boot drive in a Mac OS and use it to install firmware on the Network Protection appliance.

You might choose to install new firmware to resolve software and configuration errors that cause your appliance not to work properly. For example, you can use this procedure to install new firmware on an appliance that does not boot due to a software error.

Refer to the Extreme Support Portal for help troubleshooting appliance problems.

1. Download the appliance firmware from the Extreme extranetand save it to a secure host in your network.
2. On the secure host, open the Terminal application.
3. In the Terminal application window, run `diskutil list` to get a current list of devices.
4. Connect the USB flash drive to the secure host.
5. Run `diskutil list` again and determine which device node the system assigned the USB device to.
6. Run `sudo dd if=/path/to/downloaded.img of=/dev/rdiskN bs=1m`. Replace `/path/to/downloaded.img` with the path to the firmware file.

Note
If you get the following error, replace `bs=1m` with `bs=1M`:

```
dd: Invalid number `1m', you are using GNU dd
```

7. Run `diskutil eject /dev/diskN` and remove your device after the command is complete.
8. Turn off the appliance.
9. Connect the USB flash drive to the appliance and turn the appliance on.

   The appliance boots from the USB boot drive.

10 Log on to the installer command-line interface as an administrator.

- `install login: admin`
- `password:admin`

Tip
You can type **`help`** for a list of commands available in the current mode.

11 Type `restore`.

12 Type **YES** and press Enter.

Note
The installation takes approximately 30 minutes to complete.

The firmware is installed and the appliance restarts.

Manually backing up firmware

Use the Firmware Settings page to manually create a backup of your active firmware version before applying a fix pack.

It is only necessary to perform a manual backup if you need to install a fix pack provided by Extreme Software Support.

Note
The backup process can take several minutes to complete.

1 Click Manage > Firmware Settings.
2 On the Firmware Settings page, select the active partition.
3 Click Create Backup.

Next, apply the fix pack provided by Extreme Support.

Installing updates

Install firmware and intrusion prevention updates to improve the Network Protection appliance and the network protection that is provided by the appliance.

Important
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 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 X-Force® research and development team.

For more information about product issues and updates, see the Security Network Protection release notes on the Extreme Security Threat Protection Downloads Page (https://extranet.extremenetworks.com/downloads/Pages/SecurityThreatProtection.aspx).

Tip
You can also install available updates from the **Overview** page.

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

Option	Description
Upload	To manually add an update, click **Upload**. In the New Update window, click **Select Update**, browse to the update file, click **Open**, and then click **Submit**. Note You can install the update after you manually add it.
Refresh	To check for updates, click **Refresh**.
Install	To install an update, select the update, and then click **Install**.
Schedule	To create or edit an update schedule, select an update, and then click **Schedule**. In the **Edit Schedule** window, perform one or more of the following actions: • To remove an update schedule, select **Remove Schedule**. • To create an update schedule, select a date and time to install the update. Click **Submit** to save your changes.

A References

Command-line interface

The command-line interface (CLI) provides a limited set of commands to control and receive responses from the Network Protection appliance.

Global commands

Table 3: Global commands

Global command	Description
`back`	Return to the previous command mode.
`exit`	Log off from the appliance.
`help <command>`	Display the information for using the specified command.
`reboot`	Reboot the appliance.
`shutdown`	End system operation and turn off the power.
`top`	Return to the top level.

Mode commands

Note
The installer mode is only available when the appliance is booted from a USB flash drive.

Table 4: Installer mode commands

Installer mode command	Description
`restore`	Restore a firmware image.
`wipe`	Wipe the appliance hard disk drive.

Table 5: Top mode commands

Top mode command	Description
certificates	Work with certificates.
firmware	Work with firmware images.
fixpacks	Work with fix packs.
license	Work with licenses.
logs	Work with log files.
management	Work with management settings.
opensig	Work with profiling information for OpenSignatures.
protection	Work with protection interfaces.
services	Work with certain system services.
snapshots	Work with policy snapshot files.
ssh	Work with SSH keys
support	Work with support information files.
tools	Work with network diagnostic tools.
updates	Work with security updates.

Table 6: Certificates mode commands

Certificates mode command	Description
regen_cert	Regenerate device-signing CA. Note The keyboard command Ctrl + C does not interrupt the regen_cert command in Certificates mode.
show_active	Display the active CA certificate in PEM encoded format.

Table 7: Firmware mode commands

Firmware mode command	Description
backup	Back up firmware on the primary partition to the inactive partition.
get_comment [<*index*>]	View the comment that is associated with a firmware image.
get_info [<*index*>]	View the version information that is associated with a firmware image.
list	List information about installed firmware images. Firmware information includes the active firmware image, a description of the firmware, the date the firmware was installed, and optional backup information.
set_comment [<*index*> [<*comment*> ...]]	Replace the comment that is associated with a firmware image.
swap_active	Swap the active firmware image. The appliance restarts the system by using the inactive firmware image.

Table 8: Fixpacks mode commands

Fixpacks mode command	Description
`install`	Install available fix packs from the inserted USB flash drive.
`list`	List available fix packs on the inserted USB flash drive.
`rollback`	Uninstall most recently installed fix pack.
`view_history`	Display installation history for all fix packs.

Table 9: License mode commands

License mode command	Description
`install`	Install a license file from inserted USB flash drive.
`list`	List the available license files on the inserted USB flash drive.
`show`	Display current active license information.

Table 10: Logs mode commands

Logs mode command	Description
`less[` *`<log-file-name>`* `]`	View and search a log file. The following log files are available: • system • webserver • updates • analysis
`tail[` *`-n`* *`<NUM_LINES>`* `] [` *`-F`* `] [` *`<log-file-name>`* `]`	Tail a log file. Data is appended to output as the file grows when *`-F`* is specified. When *`-n`* <*`NUM_LINES`*> is not specified, the default value for NUM_LINES is 10. The following log files are available: • system • webserver • updates • analysis

Table 11: Management mode commands

Management mode command	Description
`dns`	Work with the DNS appliance settings. The following commands are available for `dns`: • `set [dns]`: Set the appliance DNS. • `show`: Show the appliance DNS.
`force_heartbeat`	Force a heartbeat to the SiteProtector™ System. Note If the appliance is not managed by SiteProtector™ System, the following error message is displayed: `Force heartbeat is unavailable when the appliance is not managed by the SiteProtector` .
`hostname`	Work with the appliance host name. The following commands are available for `hostname`: • `set [hostname]`: Set the appliance host name. • `show`: Show the appliance host name.
`interfaces`	Work with management interface settings. The following commands are available for interfaces: • `list`: List the management interfaces on the appliance. • `set [interface-name]`: Set the network configuration for a management interface. • `show [interface-name]`: Display the configuration of a management network interface.
`set_password`	Set the appliance password.
`snmp`	Work with SNMP settings. • engineid • assign: Set the SNMP engine ID in hex string format on appliance. • get: Get the SNMP engine ID on appliance. • reset: Reset the engire ID to factory default.

Table 12: Opensig mode commands

Opensig mode command	Description
show_stats[all|*n*]	Display the profiling stats. Displays the following OpenSignature rule performance statistics for each open signature: • `<SID>` • `<Checks>` • `<Matches>` • `<Ticks>` • `<Ticks Per PCRE>` • `<Alerts>` Note Define the ***n*** variable to see statistics for the top ***n*** active rules. For example, type `show_stats 10` to see the profiling information for the top 10 active open signatures.

Table 13: Protection mode commands

Protection mode command	Description
list	List the names of the protection interfaces available on this appliance.
show [<*interface name*>]	Display the link status (up or down) and the negotiated speed and duplex for the specified interface. If this command runs with no arguments, the system displays the current link status and the speed and duplex for all protection interfaces.

Table 14: Services mode commands

Services mode command	Description
restart	List services that can be restarted. Select one of the following services to restart: • Packet Processing • Packet Capture • Local Management Interface • License and Update • SiteProtector Communication

Table 15: Session mode commands

Session mode command	Description
delete [<*ip address*>]	Delete the active session that is associated with the specified address.
delete_all [<*ip address*>]	Delete all active sessions.
list	List the active sessions. Show all users that authenticated against the appliance.

Table 16: Snapshots mode commands

Snapshots mode command	Description
`apply [<index>]`	Apply a policy snapshot file to the system. Note The keyboard command Ctrl + C does not interrupt the `apply` command in Snapshots mode.
`create [<comment> ...]`	Create a snapshot of current policy files.
`delete [<index>]`	Delete a policy snapshot file.
`download`	Download a policy snapshot file to a USB flash drive.
`get_comment [<index>]`	View the comment that is associated with a policy snapshot file.
`list`	List the policy snapshot files.
`set_comment [<index> [<comment> ...] ]`	Replace the comment that is associated with a policy snapshot file.
`upload`	Upload a policy snapshot file from a USB flash drive.

Table 17: SSH mode commands

SSH mode command	Description
`regen_ssh_keys`	Regenerate SSH keys.

Table 18: Support mode commands

Support mode command	Description
`create [<comment> ...]`	Create a support information file.
`delete [<index>]`	Delete a support information file.
`download [<index>]`	Download a support information file to a USB flash drive.
`get_comment [<index>]`	View the comment that is associated with a support information file.
`list`	List the support information files.
`set_comment [<index> [<comment> ...] ]`	Replace the comment that is associated with support information file.

Table 19: Tools mode commands

Tools mode command	Description
`capture`	Work with packet captures.
`nslookup [<host>] [<server>]`	Query internet domain name servers.

Table 19: Tools mode commands (continued)

Tools mode command	Description
`ping [-6] [-c <count>] [-s <size>] <host>`	Send an ICMP ECHO_REQUEST to network hosts. Note The count must be 0 - 5535. If the count is 0, then the system sends ICMP ECHO_REQUEST pings until interrupted by the user with Ctrl + C. The default count is 0. The size must be 0 - 65535. The default size is 56 bytes.
`sysinfo [memory] [storage] [cpu]`	Query the memory usage, disk space, or cpu usage to troubleshoot the appliance.
`telnet [-l <user>] <host> [<port>]` Note User and port are optional.	Communicate with a remote computer that is using the Telnet protocol.
`traceroute [-6] <host> [<size>]`	Trace a packet from a computer to a remote destination, showing how many hops the packet made to reach the destination and how long each hop took. Note Size must be 38 - 32768. Default size is 38 bytes.

Table 20: Updates mode commands

Updates mode command	Description
`install[type][usb|server]`	Install an update from the inserted USB flash drive or update server. Restriction Only updates that are available for your appliance model are displayed. Note The keyboard command Ctrl + C does not interrupt the `install` command in Updates mode.
`list[type] [usb|server]`	List available updates on the inserted USB flash drive or on the update server. Any of the following updates might be available: • firmware • IPS Note The types of updates that are available depend on the model of your appliance.

Table 20: Updates mode commands (continued)

Updates mode command	Description
`rollback`	Undo a security update. Note The keyboard command Ctrl + C does not interrupt the `rollback` command in Updates mode.
`show`	Display version information for the security update that is installed and current.
`view_history`	Display installation and rollback history for all updates.

Wiping the appliance: Linux™

Perform a secure wipe on the appliance when you want to make it impossible to recover any data that was previously on the drive.

You might wipe an appliance as part of the RMA process or before you discard the appliance. You can wipe an appliance that will not boot due to software or configuration errors. You can also wipe an appliance with some hardware failures. However, a wipe is unlikely to work on some hardware failures, such as a failed hard disk.

Wiping an appliance does not restore functionality to the appliance.

1. Download the appliance firmware from the Extreme extranetand save it to a secure host in your network.
2. Insert the USB flash drive into a USB port on the same host and note where the operating system assigns the USB flash drive.
3. On the secure host, from the command line, type `dd if=file.usb of=/dev/yourflashdevice`.

   Note
   `/dev/yourflashdevice` is the full drive path, not a partition. For example, type `/dev/sdb` (not `/dev/sdb1`).

4. Turn off the appliance.
5. Connect the USB flash drive to the appliance and turn the appliance on.

   The appliance boots from the USB boot drive.
6. Log on to the installer command-line interface as an administrator.
   - `install login: admin`
   - `password:admin`

   Tip
   You can type `help` for a list of commands available in the current mode.

7 Type **wipe** and press Enter.

> Note
> The wipe procedure takes approximately 30 minutes to complete.

Wiping the appliance: Mac OS

Perform a secure wipe on the appliance when you want to make it impossible to recover any data that was previously on the drive.

You might wipe an appliance as part of the RMA process or before you discard the appliance. You can wipe an appliance that will not boot due to software or configuration errors. You can also wipe an appliance with some hardware failures. However, a wipe is unlikely to work on some hardware failures, such as a failed hard disk.

Wiping an appliance does not restore functionality to the appliance.

1 Download the appliance firmware from the Extreme extranetand save it to a secure host in your network.

2 On the secure host, open the Terminal application.

3 In the Terminal application window, run `diskutil list` to get a current list of devices.

4 Connect the USB flash drive to the secure host.

5 Run `diskutil list` again and determine which device node the system assigned the USB device to.

6 Run `sudo dd if=/path/to/downloaded.img of=/dev/rdiskN bs=1m`. Replace `/path/to/downloaded.img` with the path to the firmware file.

> Note
> If you get the following error, replace `bs=1m` with `bs=1M`:
>
> ```
> dd: Invalid number `1m', you are using GNU dd
> ```

7 Run `diskutil eject /dev/diskN` and remove your device after the command is complete.

8 Turn off the appliance.

9 Connect the USB flash drive to the appliance and turn the appliance on.

The appliance boots from the USB boot drive.

10 Log on to the installer command-line interface as an administrator.

- `install login: admin`
- `password:admin`

> Tip
> You can type `help` for a list of commands available in the current mode.

11 Type **wipe** and press Enter.

> Note
> The wipe procedure takes approximately 30 minutes to complete.

Wiping the appliance: Windows™ OS

Perform a secure wipe on the appliance when you want to make it impossible to recover any data that was previously on the drive.

You might wipe an appliance as part of the RMA process or before you discard the appliance. You can wipe an appliance that will not boot due to software or configuration errors. You can also wipe an appliance with some hardware failures. However, a wipe is unlikely to work on some hardware failures, such as a failed hard disk.

Wiping an appliance does not restore functionality to the appliance.

1 Download the appliance firmware from the Extreme extranetand save it to a secure host in your network.
2 Insert the USB flash drive into a USB port on the same host and note where the operating system assigns the USB flash drive.
3 Use an image writer program to overwrite the contents of the USB flash drive with the firmware image.

Tip
Common writer programs for Windows™ include Win32DiskImager.exe and USB Image Tool. USB ImageWriter is included in most Linux™ distributions.

4 Turn off the appliance.
5 Connect the USB flash drive to the appliance and turn the appliance on.

The appliance boots from the USB boot drive.

6 Log on to the installer command-line interface as an administrator.
- `install login: admin`
- `password:admin`

Tip
You can type **`help`** for a list of commands available in the current mode.

7 Type **`wipe`** and press Enter.

Note
The wipe procedure takes approximately 30 minutes to complete.

Index