



ExtremeControl IA-A-25 Installation Guide

*Extreme Management Center® Extreme Access
Control Engine*



Copyright © 2018 Extreme Networks 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

Software Licensing

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:

www.extremenetworks.com/support/policies/software-licensing

Support

For product support, phone the Global Technical Assistance Center (GTAC) at 1-800-998-2408 (toll-free in U.S. and Canada) or +1-408-579-2826. For the support phone number in other countries, visit: <http://www.extremenetworks.com/support/contact/>

For product documentation online, visit: <https://www.extremenetworks.com/documentation/>

Table of Contents

- About this Guide..... 4**
 - Text Conventions.....4
 - Providing Feedback to Us..... 4
 - Getting Help.....5
 - Related Publications..... 5

- Chapter 1: Engine Overview and Setup..... 6**
 - Kit Contents.....6
 - Specifications.....6
 - Front Panel Features..... 8
 - Back Panel Features..... 9
 - Removing and Installing the Front Bezel.....10
 - Installing the Engine into a Rack..... 11

- Chapter 2: Configuration..... 13**
 - Pre-Configuration Tasks..... 13
 - Configuring the Engine.....13
 - Changing Engine Settings.....17
 - Upgrading Engine Software.....19

- Chapter 3: Reinstalling Engine Software..... 20**

- Appendix A: Product Regulatory and Compliance Information.....21**

- Index..... 30**

- Glossary..... 26**



About this Guide

This document describes the installation and initial configuration of the Extreme Networks® Extreme Access Control IA-A-25 hardware engine.

This document is intended for experienced network administrators who are responsible for implementing and maintaining communications networks.

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.
<i>New!</i>	New Content	Displayed next to new content. This is searchable text within the PDF.

Table 2: Text Conventions

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

Providing Feedback to Us

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

- Content errors or confusing or conflicting information.

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

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

Getting Help

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

- **GTAC (Global Technical Assistance Center) for Immediate Support**
 - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
 - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- **Extreme Portal** — Search the GTAC knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
- **The Hub** — A forum for Extreme customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

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

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

Related Publications

Extreme Management Center™ Documentation

Extreme Management Center (XMC) documentation, including release notes, are available at: <http://documentation.extremenetworks.com>.

Extreme Management Center online help is available by clicking the **?** icon in all XMC pages. The online help provides detailed explanations of how to configure and manage your network using XMC.

For complete regulatory compliance and safety information, refer to the document *Intel® Server Products Product Safety and Regulatory Compliance*.
ExtremeAnalytics PV-A-305 Installation Guide

1 Engine Overview and Setup

Kit Contents
Specifications
Front Panel Features
Back Panel Features
Removing and Installing the Front Bezel
Installing the Engine into a Rack

This chapter lists the components shipped with the IA-A-25 engine, describes the front and back panels, and provides information on engine specifications.

For complete regulatory compliance and safety information, refer to the document *Intel® Server Products Product Safety and Regulatory Compliance*, available at the following links:

http://download.intel.com/support/motherboards/server/sb/g23122003_safetyregulatory.pdf
<http://www.extremenetworks.com/support/documentation/>

Kit Contents

The engine ships with the following components:

- Extreme Networks URL card
- Front bezel label
- A rack mounting kit
- Two rack handles and appropriate screws
- AC power cord bracket and cable clamp kit
- One USB flash drive

Specifications

The physical specifications for the engine is listed in [Table 3](#). The environmental requirements are listed in [Table 4](#) on page 7.

Table 3: IA-A-25 Physical Specifications

Processor	
Processor type	IA-A-25 - Intel® Xeon® E5-2620 v4 processor
Processor speed	2.1 GHz
CPU Cores	8
Memory	
Architecture	2400 MHz Dual Ranked Registered (RDIMM) ECC DDR4

**Table 3: IA-A-25 Physical Specifications
(continued)**

Memory module capacities	4 GB DIMMs
Minimum RAM (included)	16 GB (four 4 GB DIMMs)
Maximum RAM	48 GB (twenty-four 2 GB RDIMMs)
Drives	
Hard drives	One 150 GB SSD hard drive
Connectors	
Back	
NIC	Four RJ-45
Serial	9-pin, DTE, 16550-compatible
USB	Three 4-pin, USB 2.0-compliant
Video	15-pin VGA
Networking	Two 1 GB Ethernet
Front	
USB	Two 4-pin, USB 2.0-compliant
Video	15-pin VGA
Power	
AC power supply (per power supply)	Redundant power supply
Wattage	750 watts
Input voltage	<ul style="list-style-type: none"> 90 – 132 V at 47/63 Hz 8.2 A 180 – 264 V at 47/63 Hz 4.4 A
Output voltage	<ul style="list-style-type: none"> 62.0A at 12 V 2.1A at 12 VSB
Physical	
Height	4.45 cm (1.72 in.)
Width	43.0 cm (16.93 in.)
Depth	70.99 cm (27.95 in.)
Weight (maximum configuration)	13.15 kg (29 lb.)

Table 4: IA-A-25 Environmental Specifications

Parameter	Limits
Operating temperature	+10°C (+50°F) to +35°C (+95°F) with the maximum rate of change not to exceed 10°C (+50°F) per hour
Storage temperature	-40°C (-40°F) to +70°C (+158°F)
Storage humidity	50% to 90%, non-condensing at 28°C (82°F)
Vibration, unpackaged	5 Hz to 500 Hz, 2.20 g RMS random

Table 4: IA-A-25 Environmental Specifications (continued)

Parameter	Limits
Shock, operating	Half sine, 2 g-force peak, 11 milliseconds
Shock, unpackaged	Trapezoidal, 25 g, velocity change 136 inches/second (40 lb to < 80 lb)
Shock, packaged	Non-palletized free fall in height 24 inches (40 lb to < 80 lb)
ESD	±12 KV except I/O port ±8 KV per Intel® Environmental test specification
Estimated thermal dissipation	1550 BTU/Hr

Front Panel Features

Figure 1 shows the front panel features. Figure 2 on page 8 shows the front control panel.

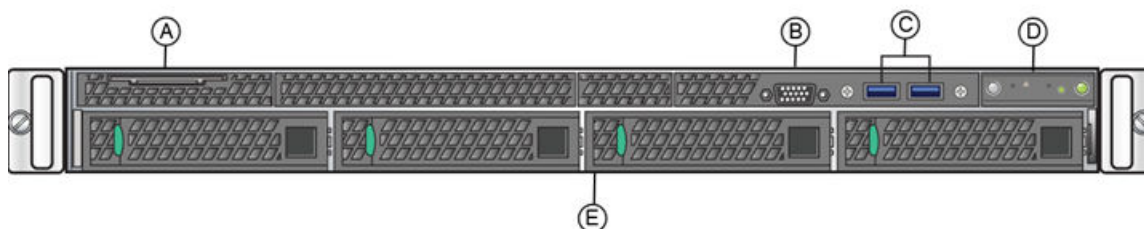


Figure 1: IA-A-25 Front Panel Features

A	System label pull-out	D	Front control panel (see Figure 2 on page 8)
B	Video Connector	E	Hard disk drive bays
C	USB 3.0 Ports		

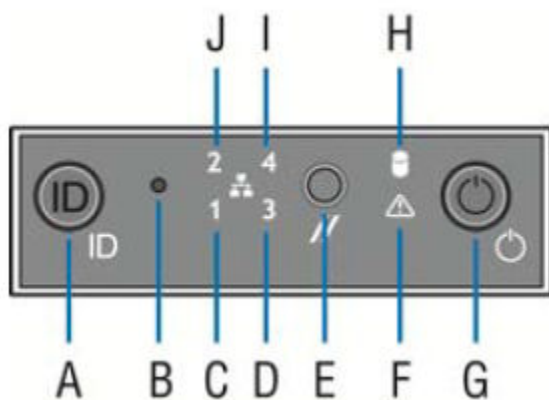


Figure 2: Front Control Panel

A	System ID button w/integrated LED	F	System status LED
B	NMI button (recessed, tool required for use)	G	Power button w/integrated LED

C	Mgmt port activity LED	H	Hard drive activity LED
D	Not used	I	Not used
E	System cold reset button	J	Not used

Hard Drive LED Indicator Patterns

The hard drive has two LED indicators visible from the front of the system: one is a green LED for disk activity, and the other is amber and indicates hard drive status. The LEDs have the following states, as described in [Table 5](#).

Table 5: Hard Drive Activity LED Indicator Patterns

Hard Drive Condition	Activity LED Patterns
Power on and drive spinning up or spinning down	Off
Power on with drive activity	Blinking green

Table 6: Hard Drive Status LED Indicator Patterns

Hard Drive Condition	Status LED Patterns
No access or no fault	Off
Hard drive fault has occurred	Solid amber

Back Panel Features

[Figure 3](#) shows the back panel.

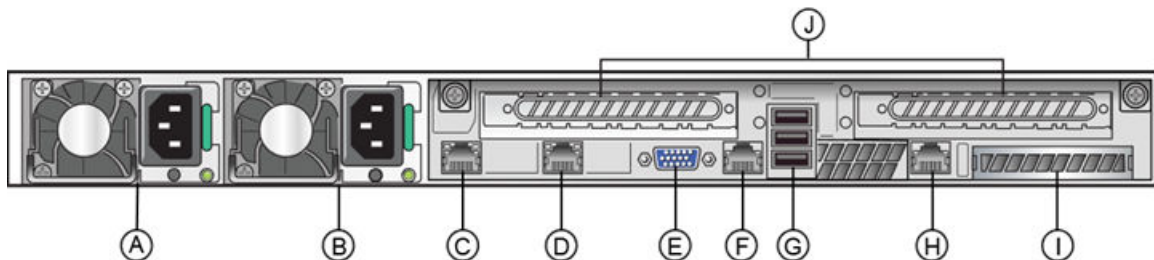


Figure 3: IA-A-25 Back Panel

A	Power supply module #1	F	Serial port
B	Power supply module #2	G	USB 2.0 ports
C	eth0	H	Mgmt port, out of band
D	eth1	I	I/O Module Bay
E	Video connector	J	Riser cards, Not used

[Table 7](#) describes the LEDs for the RJ45 management port.

Table 7: RJ45 Port LEDs (Management Port)

LED Type	LED Pattern	Status Indication
Network speed (right)	Off	10 Mbps
	Amber	100 Mbps
	Green	1000 Mbps
Link activity (left)	Off	No link
	Solid green	Active link
	Blinking green	Data traffic activity

Power Supply Status Indicator Patterns

The engine has two power supplies, supplying hot-pluggable power redundancy. The system distributes the power load across both power supplies to maximize efficiency.

Each power supply has a single bi-color LED to indicate power supply status, as described in [Table 8](#).

Table 8: Power Supply Status LED Indicator Patterns

LED Pattern	Power Supply Condition
Green	Output on and OK
Off	No AC power to all power supplies
1Hz blinking green	AC present / Only 12VSB on (PS off) or PS in cold redundant state
Amber	AC power cord unplugged or AC power lost. With a 2nd PS in parallel still with AC input power
1Hz blinking amber	Power supply warning events where PS continues to operate — high temp, high power, high current, slow fan
Amber	Power supply critical event causing a shutdown, failure, OCP, OVP, fan fail
2Hz blinking green	Power supply firmware updating

Removing and Installing the Front Bezel

The engine comes with an optional front panel bezel that you can attach to the front of the chassis by snapping the bezel onto the chassis handles. A key lock allows you to lock the bezel in place so that front panel controls cannot be used. You can still monitor system status indicators with the bezel in place.

Removing the Front Bezel

To remove the front bezel:

- 1 Unlock the bezel if it is locked.
- 2 Remove the left end of the front bezel from rack handle.

- 3 Rotate the front bezel counterclockwise to release the latches on the right end from the rack handle.

Installing the Front Bezel



Note

Before installing the bezel, you must install the rack handles. See [Installing the Engine into a Rack](#) on page 11.

To install the front bezel:

- 1 Lock the right end of the front bezel to the rack handle.
- 2 Rotate the front bezel clockwise till the left end clicks into place.
- 3 Lock the bezel, if needed.

Installing the Engine into a Rack

A rack mounting kit and installation guide are included with the engine. The rack mounting kit allows you to install the engine into a four-post rack cabinet. Refer to the installation guide for complete installation instructions.

If you are table mounting the engine, ensure at least 6 cm of clearance on all sides of the engine for proper ventilation.

If you are installing the engine in a rack:

- 1 Install the rack handles by aligning a rack handle with the two holes on each side of the engine and attaching each handle to the engine with two screws as shown in [the figure below](#).

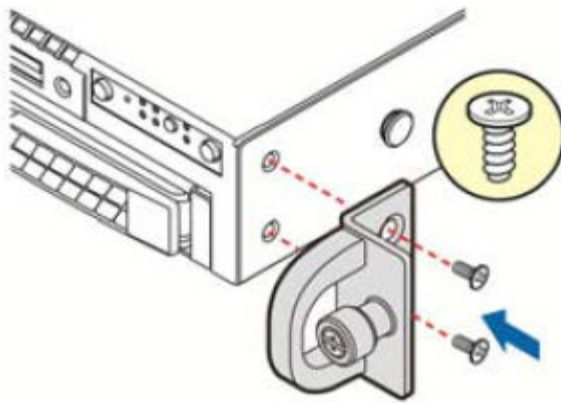


Figure 4: Installing the Rack Handles

- 2 Read the installation guide included with the rack mounting kit.
- 3 Install the rails and mount the controller in the rack as instructed.

Torque Values

The following table describes the recommended torque values to use when installing the engine using standard threaded fastener machine screws and bolts.

Table 9: Recommended Torque Values by Screw Size

Screw Size		Torque in Pounds			Bit Size
English	Metric	-%5	Nominal	+%5	
N/A	N/A	1.42	1.5	1.57	0
2 - 56	1.5	2.85	3.0	3.15	0
4 - 40	2.5	4.75	5.0	5.25	0/1
6 - 32	3.5	8.55	9.0	9.45	1
8 - 32	4.5	17.10	18.0	18.90	2
10 - 32	5	30.40	32.0	33.60	2
1/4 - 20	6.5	63.65	67.0	70.35	3

2 Configuration

Pre-Configuration Tasks
Configuring the Engine
Changing Engine Settings
Upgrading Engine Software

Once you have installed the engine into a rack, you need to connect a monitor and a USB keyboard, connect the power cord and network cable, and power the engine on (see [Figure 1](#) on page 8 and [Figure 3](#) on page 9).

After the engine boots and the engine installation is complete, you must go through the initial configuration process described in this chapter.

This chapter also includes information on how to change your engine settings following your initial configuration (see [Changing Engine Settings](#) on page 17).

Pre-Configuration Tasks

Ensure that you have the following information prior to executing any of the procedures in this chapter:

- Engine hostname, IP address, and netmask
- Default gateway IP address
- Extreme Management Center server IP address
- Name server IP address and domain name
- Network Time Protocol (NTP) server IP address

Configuring the Engine

After the initial engine installation is complete, use the following steps to configure the engine to run the Extreme Access Control engine software:

- 1 Login as root with no password, and press **[Enter]**.
The following screen appears.

```
=====
Extreme Networks - Access Control Engine
- Welcome to the Access Control Engine 7.1.2.11 Setup
=====

Please enter the information as it is requested to continue with
the configuration. Typically a default value is displayed in brackets. Pressing the
[enter] key without entering a new value will use the bracketed value and proceed to
the next item.

If a default value cannot be provided, the prompt will indicate that the item is either
(Required) or (Optional). The [enter] key may be pressed without entering data for
(Optional) items. A value must be entered for (Required) items.
```

At the end of the setup process, the existing settings will be displayed and opportunity will be provided to correct any errors.

=====

Press [enter] to begin setup or CTRL-C to exit:

- 2 Press **[Enter]** to begin the setup.

The **Root Password Configuration** screen appears:

=====

Root Password Configuration

=====

There is currently no password set in the system administrator account (root). It is recommended that you set one that is active the first time the machine is rebooted.

=====

Would you like to set a root password (y/n) [y]?

- 3 Press **[Enter]** to set a new root password. Enter the new password as prompted.

Enter new UNIX password:

Retype new UNIX password:

Password updated successfully.

- 4 In the **Access Control Engine Configuration** screen, enter the requested information for each line and press **[Enter]**.

=====

Access Control Engine Configuration

=====

Enter the hostname for the engine [nacappliance]:
 Please enter the IP address for nacappliance (Required): 10.15.76.100
 Enter the IP netmask [255.255.255.0]:
 Enter the engine address [10.50.76.1]:
 Enter the IP address of the name server (Optional): 1.2.3.4
 Enter the IP address of an alternate name server (Optional): 1.2.3.4
 Enter the domain name for nacappliance (Required): extremenetworks.com
 Enter the IP address of the NetSight Server (Required): 1.3.4.5^\

- 5 In the **SNMP Configuration** screen, enter the requested information for each line and press **[Enter]**.

=====

SNMP Configuration

=====

The following information will be used to configure SNMP management of this device. The SNMP information entered here must be used to contact this device with remote management applications such as Extreme Management Center Console.

=====

Please enter the SNMP user name [snmpuser]:
 Please enter the SNMP authentication credential [snmpauthcred]:
 Please enter the SNMP privacy credential [snmpprivcred]:

- 6 In the **Configure Date and Time Settings** screen, select whether you want to use an external Network Time Protocol (NTP) server. Enter **y** to use NTP, and enter your NTP server IP address(es). Enter **n** to configure the date and time manually and proceed to step 8.

=====

Configure Date And Time Settings

```

=====
The engine date and time can be set manually or using an external Network Time Protocol
(NTP) server. It is strongly recommended that
NTP is used to configure the date and time to ensure accuracy of time
values for SNMP communications and logged events. Up to 5 server
IP addresses may be entered if NTP is used.
=====
Do you want to use NTP (y/n) [y]? y
Please enter a NTP Server IP Address (Required): 144.131.10.120
Would you like to add another server (y/n) [n]? y
Please enter a NTP Server IP Address (Required): 144.131.10.121
Would you like to add another server (y/n) [n]? n

```

- 7 In the NTP validate selection screen, enter 0 to accept the current settings and proceed to the Set Time Zone screen at step 10.

```

=====
NTP Servers
=====
These are the currently specified NTP servers. Enter 0 or any key other than a valid
selection to complete NTP configuration and continue.

If you need to make a change, enter the appropriate number from the choices listed
below.
144.131.10.120
144.131.10.121

0. Accept the current settings
1. Restart NTP server selection
2. Set date and time manually
=====
Enter selection [0]: 0

```

- 8 If you answered no to using an NTP server to set date and time, set the date and time in the **Set Date and Time** screen.

```

=====
Set Date And Time
=====
The current system date and time is: Thu Apr 24 09:34:08 2008
Please enter the values for date and time as directed where input is expected in the
following format:

MM - 2 digit month of year
DD - 2 digit day of month
YYYY - 4 digit year
hh - 2 digit hour of day using a 24 hour clock
mm - 2 digit minute of hour
ss - 2 digit seconds
=====

Please enter the month [06]:
Please enter the day of the month [24]:
Please enter the year [2013]:
Please enter the hour of day [09]:
Please enter the minutes [34]:
Please enter the seconds [34]:

```

- 9 In the **Use UTC** screen, select whether you want the system clock to be set to use UTC.

```

=====
Use UTC
=====
The system clock can be set to use UTC. Specifying no for using UTC, sets the hardware
clock using localtime.
=====
Do you want to use UTC (y/n) [n]?

```



- 10 In the **Set Time Zone** screen, select the appropriate time zone and press **[Enter]**.

```

=====
Set Time Zone
=====
You will now be asked to enter the time zone information for this system. Available
time zones are stored in files in the
/usr/share/zoneinfo directory.
Please select from one of the following example time zones:

1. US Eastern
2. US Central
3. US Mountain
4. US Pacific
5. Other - Shows a graphical list
=====

Enter selection [1]:
    
```

- 11 In the **Current Engine Configuration** screen, review the current settings and press **[Enter]** to continue.

```

Access Control Engine Configuration:
Host Info:                nacappliance 10.50.76.100/255.255.255.0
Gateway/Name Server/Domain: 10.50.76.1/1.2.3.4/extremenetworks.com
Alternate Name Server:     1.2.3.4
SNMP User/Auth/Privacy:   snmpuser/snmpauthcred/snmpprivcred
Netsight Server IP:       1.3.4.5

Press [enter] to continue:
    
```

- 12 In the **Engine Network Configuration Complete** screen, you can accept the current configuration or modify the settings.

```

=====
Access Control Engine Network Configuration Complete
=====
Configuration of the Access Control Engine network settings is now complete.
Enter 0 or any key other than a valid selection to continue.
If you need to make a change, enter the appropriate number from
the choices listed below.
=====

0. Accept the current settings
1. Edit Access Control Engine settings
2. Edit SNMP settings
3. Edit date and time
4. Modify all settings
=====

Enter selection [0]:
    
```

When you see the following screen, configuration is complete.

```

=====
Extreme Networks - Access Control Engine - Setup Complete
=====

Setup of the Access Control is now complete. Details of the engine setup process are
located in the log files in the /var/log/install directory.
=====
    
```

You are now ready to use Management Center to manage your engine.



If you have reinstalled your Extreme Access Control engine software, use Management Center to enforce the engine. Enforcing writes your Management Center configuration information to the engine.

Changing Engine Settings

This section provides instruction for changing your engine settings following your initial engine configuration, should the need arise. Depending on the settings you want to change, you can use either Extreme Management Center or the engine CLI to make the changes.

Using Extreme Management Center

Use Management Center to easily change engine settings including DNS, NTP, SSH, and SNMP configuration. You can also use Management Center to change the engine hostname and default gateway, as well as configure static routes for advanced routing configuration.

Changing DNS, NTP, SSH, and SNMP Settings

Use the **Engine Settings** window in Management Center to change the following:

- DNS Configuration — Search domains and DNS servers
- NTP Configuration — Time zone and NTP servers
- SSH Configuration — Port number and RADIUS authentication
- SNMP Configuration — SNMP credentials for the engine

To access the **Engine Settings** window:

- 1 In Management Center, select **Control > Access Control**.
The **Access Control** tab opens.
- 2 In the left-panel tree, expand the Engines folder and then expand the All Engines folder.
- 3 Right-click the desired engine and select **Engine Settings**.
The **Engine Settings** window opens.
- 4 Select the **Network Settings** tab to change your engine configurations.
For more information, see the "Engine Settings Window" topic in the Management Center online Help.

Changing Hostname, Gateway, and Static Routes

In Management Center, use the Interface Summary section of the **Details** tab for an engine to change the engine hostname, default gateway, and static routes.

- 1 In Management Center, select **Control > Access Control**.
The **Access Control** tab opens.
- 2 In the left-panel tree, expand the Engines folder and then expand the All Engines folder.
- 3 Select the engine you are configuring.
- 4 In the right-panel, select the **Details** tab.
- 5 Click **Edit** in the Interface Summary section of the tab to open the **Interfaces** window, where you can change the engine Host Name and Gateway.
For more information, see the "Interface Configuration Window" topic in the Management Center online Help

- 6 Click **Static Routes** in the Interface Summary section to open the **Static Route Configuration** window, where you can add or edit the static routes used for advanced routing configuration. For more information, see the "Static Route Configuration Window" topic in the Management Center online Help.

Using the Engine CLI

Use the engine CLI to change the engine IP address, Extreme Management Center server IP address, and web service credentials. Use Management Center to make these changes, if possible. You can also use the CLI to change basic network settings such as engine hostname, SNMP configuration, and date and time settings, if necessary (see [Using Extreme Management Center](#) on page 17).

Changing the Extreme Management Center Server IP Address

To change the IP address of the Extreme Management Center server, enter the following command at the engine CLI:

```
/opt/nac/configMgmtIP <IP address>
```

Then, start using the new Extreme Management Center server by typing:

```
nacctl restart
```

Changing Web Service Credentials

The web service credentials provide access to the Access Control Engine Administration web page and the web services interface between the Extreme Management Center server and the Access Control engine. Engines ship with a preconfigured default password.

If you change the web service credentials in Management Center (in the Engine Settings), the new credentials automatically propagate to the new engine when you enforce the engine.

In the event that you need to manually change the web service credentials on the engine, enter the following command at the engine CLI:

```
/opt/nac/configWebCredentials <username> <password>
```

Then, restart the engine by entering:

```
service nacservices restart
```

Changing the Engine IP Address and Basic Network Settings

To change the engine IP address, as well as basic network settings such as hostname and SNMP configuration (including system contact, system location, trap server, SNMP trap community string, SNMP user, SNMP authentication, and SNMP privacy credentials), enter the following command at the engine CLI:

```
/usr/postinstall/nacconfig
```

This starts the network configuration script and allow you to make the desired changes.

Changing Date and Time Settings

To enable or disable NTP for engine date and time, or to manually set the date and time on the engine, enter the following command at the engine CLI:

```
/usr/postinstall/dateconfig
```

This starts the date and time configuration script and allow you to change the settings.

Upgrading Engine Software

Upgrades to the Extreme Access Control engine software are available on the Extreme Portal: <https://extremeportal.force.com/>. After entering your email address and password, you will be on the Support page. Click on the **Products** tab and select **ExtremeControl**. Click the ExtremeControl link in the right panel and select a version of ExtremeControl. Scroll down to see the Access Control engine images.

Instructions for performing the software upgrade are also available on the Extreme Management Center web page. Click on the **Documentation** tab and follow this path to the document:
Manuals & Release Notes > select a version > Extreme Access Control.

3 Reinstalling Engine Software

Use the procedure in this chapter to reinstall the engine software, in the event a software reinstall becomes necessary. Be aware that this procedure reformats the hard drive and reinstalls all the engine software, the operating system, and all related Linux packages.

You will need to connect a monitor and a USB keyboard to the engine prior to performing these steps.

- 1 Download the Extreme Access Control Engine Image 64bit (ZIP) file to your system.

To download an engine image:

- 1 Access the Extreme Portal at:
<https://extremeportal.force.com/>.
 - 2 After entering your email address and password, you are on the Support page.
 - 3 Click the **Products** tab and select **ExtremeControl**.
 - 4 Click **ExtremeControl** in the right-panel.
 - 5 Select a version.
 - 6 Download the image and extract the file to a directory on your system.
- 2 Insert the USB flash drive that came with the engine into the USB port on your system and note the drive letter it is assigned.
 - 3 Open a command prompt window and cd to the directory where you extracted the file.
 - 4 Type `make_disk.bat <drive letter>:`. Since the reinstall procedure reformats the drive, be sure you have specified the correct drive letter. Press **[Enter]**.
The files are copied to the USB flash drive. When the copy is complete you see the message:
`Successfully installed into <drive letter>: Press any key to continue.`
 - 5 Remove the USB flash drive from your system.
 - 6 Insert the USB flash drive into a USB port on the engine (see [Figure 1](#) on page 8).
 - 7 Boot the engine from the USB drive using either of these two methods.
 - Method 1:
 - 1 Press the power button, and then press F6 to go to the Boot Menu.
 - 2 Select the USB drive on the menu.
 - 3 The engine starts booting from the USB flash drive.
 - 4 When the boot is complete, the Engine Installation screen appears and the installation begins.
 - Method 2:
 - 1 Press the power button, and then press F2 to go to the BIOS setup.
 - 2 Use the arrow keys to navigate to the Boot Options menu.
 - 3 Ensure that the USB flash drive is listed as Boot Option #1 at the top.
 - 4 Save changes and exit.
 - 5 The engine starts booting from the USB flash drive.
 - 6 When the boot is complete, the Engine Installation screen appears and the installation begins.
 - 8 After the installation completes, reboot the engine and remove the USB flash drive.
 - 9 Proceed to [Configuration](#) on page 13, and follow the instructions for configuring the engine.

A Product Regulatory and Compliance Information

For complete regulatory compliance and safety information, refer to the document Intel® Server Products Product Safety and Regulatory Compliance, available at the following links:

http://download.intel.com/support/motherboards/server/sb/g23122003_safetyregulatory.pdf
<https://www.extremenetworks.com/support/documentation/>

Federal Communications Commission (FCC) Notice

This product has been tested and found to comply with the limits for a class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This product uses, generates, and can radiate radio frequency energy and if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference to radio communications. Operation of this product in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment. The customer is responsible for ensuring compliance of the modified product.

Intel Corporation
5200 N.E. Elam Young Parkway
Hillsboro, OR 97124-6497
Phone: 1-800-628-8686

Industry Canada, Class A

This Class A digital apparatus complies with Canadian ICES-003.

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of the Canadian Department of Communications.

Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques", NMB-003 édictée par le Ministre Canadien des Communications.

CE Notice

This product has been determined to be in compliance with 2006/95/EC (Low Voltage Directive), 2004/108/EC (EMC Directive).

VCCI Notice

This is a class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI EMC Statement — Taiwan

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Hazardous Substances

This product complies with the requirements of Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

European Waste Electrical and Electronic Equipment (WEEE) Notice



In accordance with Directive 2012/19/EU of the European Parliament on waste electrical and electronic equipment (WEEE):

- 1 The symbol above indicates that separate collection of electrical and electronic equipment is required.
- 2 When this product has reached the end of its serviceable life, it cannot be disposed of as unsorted municipal waste. It must be collected and treated separately.
- 3 It has been determined by the European Parliament that there are potential negative effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment.
- 4 It is the users' responsibility to utilize the available collection system to ensure WEEE is properly treated.

For information about the available collection system, please contact Enterasys Customer Support at +353 61 705500 (Ireland).

产品说明书附件 Supplement to Product Instructions

部件名称 (Parts)	有毒有害物质或元素 (Hazardous Substance)					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr ⁶⁺)	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
金属部件 (Metal Parts)	×	○	○	○	○	○
电路模块 (Circuit Modules)	×	○	○	○	○	○
电缆及电缆组件 (Cables & Cable Assemblies)	×	○	○	○	○	○
塑料和聚合物部件 (Plastic and Polymeric parts)	○	○	○	○	○	○
电路开关 (Circuit Breakers)	○	○	○	○	○	○

○： 表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T 11363-2006 标准规定的限量要求以下。
Indicates that the concentration of the hazardous substance in all homogeneous materials in the parts is below the relevant threshold of the SJ/T 11363-2006 standard.

×： 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006 标准规定的限量要求。
Indicates that the concentration of the hazardous substance of at least one of all homogeneous materials in the parts is above the relevant threshold of the SJ/T 11363-2006 standard.

对销售之日的所售产品, 本表显示, 极进供应链的电子息产品可能包含这些物质。注意: 在所售产品中可能会也可能不会含有所有所列的部件。
This table shows where these substances may be found in the supply chain of Extreme's electronic information products, as of the date of sale of the enclosed product. Note that some of the component types listed above may or may not be a part of the enclosed product.

除非另外特别的标注, 此标志为针对所涉及产品的环保使用期标志。某些零部件会有一个不同的环保使用期(例如, 电池单元模块)贴在其产品上。
此环保使用期限只适用于产品是在产品手册中所规定的条件下工作。
The Environmentally Friendly Use Period (EFUP) for all enclosed products and their parts are per the symbol shown here, unless otherwise marked. Certain parts may have a different EFUP (for example, battery modules) and so are marked to reflect such. The Environmentally Friendly Use Period is valid only when the product is operated under the conditions defined in the product manual.



Declaration of Conformity

Application of Council Directive(s):	2004/108/EC 2006/95/EC 2011/65/EU
Manufacturer's Name:	Extreme Networks, Inc.

Manufacturer's Address:	145 Rio Robles San Jose, CA 95134 USA
European Representative Name:	Enterasys Networks Limited
European Representative Address:	Nexus House, Newbury Business Park London Road, Newbury Berkshire RG14 2PZ, England
Conformance to Directive(s)/Product Standards:	EC Directive 2004/108/EC EN55022:2006 A1:2007 EN 55024:1998 A1:2001 A2:2003 EN 61000-3-2:2006 A1:2009 A2:2009 EN 61000-3-3:2008 EC Directive 2006/95/EC EN 60950-1:2006 A1:2009 EN 60825-1:2007 EN 60825-2:2004 A1:2007 EC Directive 2011/65/EU
Equipment Type/Environment:	Information Technology Equipment, for use in a Commercial or Light Industrial Environment.

The object of the declaration described above is in conformity with Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

Glossary

ad hoc mode

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an AP.

ARP

Address Resolution Protocol is part of the TCP/IP suite used to dynamically associate a device's physical address (MAC address) with its logical address (IP address). The system broadcasts an ARP request, containing the IP address, and the device with that IP address sends back its MAC address so that traffic can be transmitted.

ATM

Asynchronous Transmission Mode is a start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

BSS

Basic Service Set is a wireless topology consisting of one access point connected to a wired network and a set of wireless devices. Also called an infrastructure network. See also [IBSS \(Independent Basic Service Set\)](#).

Chalet

Chalet is a web-based user interface for setting up and viewing information about a switch, removing the need to enter common commands individually in the CLI.

CHAP

Challenge-Handshake Authentication Protocol is one of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.

CLI

Command Line Interface. The CLI provides an environment to issue commands to monitor and manage switches and wireless appliances.

Data Center Connect

DCC, formerly known as DCM (Data Center Manager), is a data center fabric management and automation tool that improves the efficiency of managing a large virtual and physical network. DCC provides an integrated view of the server, storage, and networking operations, removing the need to use multiple tools and management systems. DCC automates VM assignment, allocates appropriate network resources, and applies individual policies to various data objects in the switching fabric (reducing VM sprawl). Learn more about DCC at <http://www.extremenetworks.com/product/data-center-connect/>.

DoS attack

Denial of Service attacks occur when a critical network or computing resource is overwhelmed so that legitimate requests for service cannot succeed. In its simplest form, a DoS attack is indistinguishable

from normal heavy traffic. ExtremeXOS software has configurable parameters that allow you to defeat DoS attacks.

DSSS

Direct-Sequence Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare with [*FHSS \(Frequency-Hopping Spread Spectrum\)*](#).)

EAP-TLS/EAP-TTLS

EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards.

IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.

In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication.

EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.

EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.

(See also [*PEAP \(Protected Extensible Authentication Protocol\)*](#).)

ESRP

Extreme Standby Router Protocol is an Extreme Networks-proprietary protocol that provides redundant Layer 2 and routing services to users.

Extreme Access Control

EAC, formerly NAC™, featuring both physical and virtual appliances™, is a pre- and post-connect solution for wired and wireless LAN and VPN users. Using Identity and Access appliances and/or Identity and Access Virtual Appliance with the [*XMC \(Extreme Management Center\)*](#) software, you can ensure only the right users have access to the right information from the right place at the right time. EAC is tightly integrated with the Intrusion Prevention System (IPS) and Security Information and Event Manager (SIEM) to deliver best-in-class post-connect access control. Learn more about EAC at <http://www.extremenetworks.com/product/extreme-access-control/>.

Extreme Application Analytics

EAA, formerly Purview™, is a network powered application analytics and optimization solution that captures and analyzes context-based application traffic to deliver meaningful intelligence about applications, users, locations, and devices. EAA provides data to show how applications are being used.

This can be used to better understand customer behavior on the network, identify the level of user engagement, and assure business application delivery to optimize the user experience. The software also provides visibility into network and application performance allowing IT to pinpoint and resolve performance issues in the infrastructure whether they are caused by the network, application, or server. Learn more about EAA at <http://www.extremenetworks.com/product/extremeanalytics/>.

Extreme Management Center

Extreme Management Center (XMC), formerly Netsight™, is a web-based control interface that provides centralized visibility into your network. XMC reaches beyond ports, VLANs, and SSIDs and provides detailed control of individual users, applications, and protocols. When coupled with wireless and Identity & Access Management products, XMC becomes the central location for monitoring and managing all the components in the infrastructure. Learn more about XMC at <http://www.extremenetworks.com/product/management-center/>.

ExtremeCloud

ExtremeCloud is a cloud-based network management Software as a Service (SaaS) tool. ExtremeCloud allows you to manage users, wired and wireless devices, and applications on corporate and guest networks. You can control the user experience with smarter edges – including managing QoS, call admission control, secure access policies, rate limiting, multicast, filtering, and traffic forwarding, all from an intuitive web interface. Learn more about ExtremeCloud at <http://www.extremenetworks.com/product/extremecloud/>.

ExtremeSwitching

ExtremeSwitching is the family of products comprising different switch types: **Modular** (X8 and 8000 series [formerly BlackDiamond] and S and K series switches); **Stackable** (X-series and A, B, C, and 7100 series switches); **Standalone** (SSA, X430, and D, 200, 800, and ISW series); and **Mobile Backhaul** (E4G). Learn more about ExtremeSwitching at <http://www.extremenetworks.com/products/switching-routing/>.

ExtremeWireless

ExtremeWireless products and solutions offer high-density WiFi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at <http://www.extremenetworks.com/products/wireless/>.

ExtremeXOS

ExtremeXOS, a modular switch operating system, is designed from the ground up to meet the needs of large cloud and private data centers, service providers, converged enterprise edge networks, and everything in between. Based on a resilient architecture and protocols, ExtremeXOS supports network virtualization and standards-based SDN capabilities like VXLAN gateway, OpenFlow, and OpenStack Cloud orchestration. ExtremeXOS also supports comprehensive role-based policy. Learn more about ExtremeXOS at <http://www.extremenetworks.com/product/extremexos-network-operating-system/>.

FHSS

Frequency-Hopping Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that 'hops' in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare with *DSSS (Direct-Sequence Spread Spectrum)*.)

IBSS

An IBSS is the 802.11 term for an ad hoc network. See [ad hoc mode](#).

MIC

Message Integrity Check (or Code), also called 'Michael', is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte ICV appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks.

Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with.

netmask

A netmask is a string of 0s and 1s that mask, or screen out, the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the netmask allows the specific host computer address to be visible.

PEAP

Protected Extensible Authentication Protocol is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (See also [EAP-TLS/EAP-TTLS](#).)

SSL

Secure Socket Layer is a protocol for transmitting private documents using the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. SSL uses the public-and-private key encryption system, which includes the use of a digital certificate. SSL is used for other applications than SSH, for example, OpenFlow.

syslog

A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.

syslog uses the UDP as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC 3164)

Index

Numerics

1U appliance:back panel connections 9
1U appliance:front panel features 8
1U appliance:kit contents 6
1U appliance:specifications 6
2U Multi-Gigabit appliance:Installing and removing bezel 10
2U Multi-Gigabit appliance:rack installation 11

B

Back panel features:1U appliance 9
Bezel:Installing and removing:2U Multi-Gigabit appliance 10

C

Changing:Basic Network Configuration 18
Changing:TAG Settings 17
conventions
 notice icons 4
 text 4

D

documentation
 feedback 4
Documentation, related 5

F

Front panel features:1U appliance 8

P

Pre-configuration 13

R

Rack installation:2U Multi-Gigabit appliance 11

S

support, see technical support

T

technical support
 contacting 5
Torque Values 12