

ExtremeCloud[™] IQ - Site Engine, ExtremeControl[®], and ExtremeAnalytics[®] Virtual Engine Installation Guide



Copyright © 2022 Extreme Networks, Inc. All Rights Reserved.

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys 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/

Contact

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

- Global Technical Assistance Center (GTAC) for Immediate Support
 - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or 1-603-952-5000. For the Extreme Networks support phone number in your country, visit: www.extremenetworks.com/support/contact
 - Email: <u>support@extremenetworks.com</u>. To expedite your message, enter the product name or model number in the subject line.
- <u>GTAC Knowledge</u> Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- <u>The Hub</u> A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- <u>Support Portal</u> Manage cases, downloads, service contracts, product licensing, and training and certifications.

Table of Contents

ExtremeCloud™ IQ - Site Engine, ExtremeControl®, and ExtremeAnalytics® Virtual Engin Installation Guide	e 1
Table of Contents	3
Engine Deployment	6
Deploying the Virtual Engine on a VMware ESX Server	6
Deployment Requirements	6
Deploying the Virtual Engine	6
Shutting Down the Engine	10
Deploying the Virtual Engine on a Hyper-V Server	10
Deployment Requirements	10
Deploying the Virtual Engine	10
ExtremeCloud IQ - Site Engine Engine Configuration	16
Pre-Configuration Tasks	16
ExtremeCloud IQ - Site Engine And ExtremeAnalytics Licensing	16
Licensing for Devices	17
License Limits and Violations	18
Devices Marked as Unmanaged	18
Configuring the ExtremeCloud IQ - Site Engine Engine	19
Launching ExtremeCloud IQ - Site Engine	25
Onboarding ExtremeCloud IQ - Site Engine	26
After Upgrading to ExtremeCloud IQ - Site Engine from Extreme Management Center Versions 8.4.4 or 8.5.5	26
After Initial Installation of ExtremeCloud IQ - Site Engine	28
Onboarding Devices	29
XIQ Onboarded Status for Devices	29
Restoring a Database from a Windows Server to the Engine	31
Changing Console	31
Changing Syslog Location	31

Changing Traps Location	32
Changing Inventory Settings	 ۲۵
Changing ExtremeCloud IQ - Site Engine Engine Settings	
Changing Basic Network Configuration	
Changing SNMP Configuration	32
Changing Date and Time Settings	
Upgrading ExtremeCloud IQ - Site Engine Engine Software	
Reinstalling ExtremeCloud IQ - Site Engine Appliance Software	
ExtremeControl Engine Configuration	35
Pre-Configuration Tasks	
Licensing for ExtremeControl	
After Upgrading From Extreme Management Center versions 8.4.4 or 8.5.5	35
Upon Initial Installation	36
Configuring the ExtremeControl Engine	
Changing ExtremeControl Engine Settings	40
Using the Access Control tab	41
Changing DNS, NTP, SSH, and SNMP Settings	41
Changing Hostname, Gateway, and Static Routes	41
Using the vSphere Client Console Tab	42
Changing the ExtremeCloud IQ - Site Engine Server IP Address	
Changing Web Service Credentials	42
Changing the Engine IP Address and Basic Network Settings	
Changing Date and Time Settings	43
Upgrading ExtremeControl Engine Software	
Reinstalling ExtremeControl Engine Software	43
ExtremeAnalytics Engine Configuration	44
Pre-Configuration Tasks	44
ExtremeCloud IQ - Site Engine And ExtremeAnalytics Licensing	44
Licensing for Devices	45
License Limits and Violations	46

Devices Marked as Unmanaged	. 46
Configuring the ExtremeAnalytics Engine	. 47
Launching the ExtremeAnalytics Application	56
Adding the ExtremeAnalytics Engine	. 56
Changing ExtremeAnalytics Engine Settings	57
Changing Basic Network Configuration	. 57
Changing SNMP Configuration	57
Changing Date and Time Settings	. 57
Changing the ExtremeAnalytics Server IP Address	58
Changing the Web Service Credentials	.58
Upgrading ExtremeAnalytics Engine Software	58
Reinstalling ExtremeAnalytics Engine Software	59

Engine Deployment

This chapter provides an overview of ExtremeCloud IQ - Site Engine, ExtremeControl, and ExtremeAnalytics virtual engine deployment requirements and provides instructions for deploying a virtual engine on a VMware® and Hyper-V server.

Deploying the Virtual Engine on a VMware ESX Server

Deployment Requirements

A virtual engine is a software image that runs on a virtual machine. The ExtremeCloud IQ - Site Engine, ExtremeControl, and ExtremeAnalytics virtual engines are packaged in the .ovA file format defined by VMware and must be deployed on a VMware ESXi[™] 6.0 server with a vSphere[™] client, or on a VMware ESXi[™] 6.5, 6.7, or 7.0 server using the web client.

For information about the different ExtremeCloud IQ - Site Engine, ExtremeControl, and ExtremeAnalytics virtual engine configurations, see the latest ExtremeCloud IQ - Site Engine Release Notes.

Deploying the Virtual Engine

Use the following steps to deploy an ExtremeCloud IQ - Site Engine, ExtremeControl, or ExtremeAnalytics virtual engine on a VMware ESX or ESXi server.

1. Download the ExtremeCloud IQ - Site Engine, ExtremeControl, or ExtremeAnalytics virtual engine software image to your local machine where the client is installed and running.

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. Select the Products tab and select ExtremeManagement.
- 4. Select ExtremeCloud IQ Site Engine in the right-panel.
- 5. Select a version.
- 6. Download the ExtremeCloud IQ Site Engine, ExtremeControl, or ExtremeAnalytics virtual engine (appliance) image from the appropriate section.

Extreme Portal	Support Products	Partners	3		
Search					- (
Automation ExtremeAnalytics DetremeCampus ExtremeCloud Applications ExtremeCloud IQ ExtremeCloud IQ ExtremeCloud IQ ExtremeCloud IQ - Site Engine	ExtremeCloud™ IQ - Site ExtremeCloud IQ - Site Engine, part of the connected, scalable SaaS management so granular visibility with real-time analytics, ExtremeCloud IQ - Site Engine offers you Center, now with real-time flexibility and one license application.	Engine ExtremeCloud Judion that prov and multi-vend all the features reduced time-to	IQ suite of produ vides you with tar for device manag and functionality abenefit, all for ti	cts and services, is a c k automation, access ement across your net of Extreme Managem te convenience and lo	loud- control, tworks. ient w cost of
 ExtremeCloud[™] IQ - Site Engine 				📕 License D	lependencj
+ ExtremeCloud IQ On Premise	Software & Downloads				^
+ ExtremeWireless (Formerly IdentiFl)	Download / Release Name 🛦 👘 File Size 🔺	Release Type 🔺	Release Date 🕶) EOVM Date 🛋 () Tags	Link 🔺
+ On-Premise / Private Cloud	C 21.04.10.99 Analytics	Major	5/18/2021		
ExtremeControl					
ExtremeManagement	C 21.04.10.99.Control	Major	5/18/2021		
ExtremeRouting	3 21.04.10.99.Fabric Mgr	Major	5/18/2021		
ExtremeSecurity	B				
ExtremeSwitching	E@ 21.04.10.9930Q-58	Major	5/18/2021		
ExtremeWireless					
NetworkPacketBroker	Release Notes				^
	Name 🔺	,	ile Size 🔺	Release Date 🔻	

2. Open the VMWare software. From the Host menu, select Create/Register VM.

vmware ESXi	
To Navigator	
- E Host Manage	🖉 Get vCenter Server 🕴 🥵 Greate Register VM 📔 🏠 Shut down 🔥 Reboot 🕴 🤁 Refresh 🕴 🧔 Actions
Monitor	essesx1 Version: 6.5.0 (build 4867370)
	State: Normal (not connected to any vCenter Server) Uptime: 270.11 days

3. From the Select creation type panel, select Deploy a virtual machine from an .OVF or .OVA file. Select Next.

Select creation type	Select creation type	
Select OVF and VMDK files	How would you like to create a Virtual Machine?	
Select storage		
license agreements	Create a new virtual machine	This option guides you through the process of creating a
Deployment options		virtual machine from an OVF and VMDK files.
Additional settings	Deploy a virtual machine from an OVF or OVA file	
ceady to complete	Register an existing virtual machine	

4. Enter the name of the virtual machine and select the .OVA file. Select **Next** to continue.

1 New virtual machine - ExtremeClou	dIQ-SiteEngine
 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 	Select OVF and VMDK files Select the OVF and VMDK files or OVA for the VM you would like to deploy
4 License agreements 5 Deployment options 6 Additional settings 7 Ready to complete	Enter a name for the virtual machine. ExtremeCloudIQ-SiteEngine Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.
vmware [.]	× 🔤 ExtremeCloudIQSiteEngine_64bit.21.4.10.98-Small.ova
	Rack Next Finish Cancel

5. Select your datastore. Select **Next** to continue.

😚 New virtual machine - ExtremeCloudIQ - Site Engine						
 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 4 License agreements 5 Deployment options 	Select storage Select the datastore in which to store the confi The following datastores are accessible from th virtual machine configuration files and all of the	guration and dis he destination re e virtual disks.	k files. esource that you	u selected. Sele	ct the destinatio	n datastore for the
6 Additional settings 7 Ready to complete	Name v	Capacity 🗸	Free ~	Type v	Thin pro 🗸	Access ~
/ Heady to complete	datastore1	7.27 TB	7.02 TB	VMFS5	Supported	Single
						1 items
vmware.						
Villware						
			Ва	ick Ne	xt Finis	h Cancel

6. Select your deployment options and select Next.

S New virtual machine - ExtremeClour	dIQ - Site Engine		
 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 	Deployment options Select deployment options		
4 Deployment options 5 Ready to complete	Network mappings	eth0	•
	new bostonering	U Thin W Thick	
vm ware [.]			
		Back Nex	Finish Cancel

7. Review and select **Finish** to start the deployment.

1 New virtual machine - ExtremeClou	dlQ - Site Engine	
 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 4 Deployment options 5 Ready to complete 	Ready to complete Review your settings selection before fini	shing the wizard
	Product VM Name Disks Datastore Provisioning type	netsight_appliance_64bit.21.4.10.98-Small ExtremeCloudIQ - Site Engine netsight_appliance_64bit.21.4.10.98-Small-disk1.vmdk datastore1 Thin
	Network mappings Guest OS Name	eth0: Vlil Network Unknown
vm ware [,]	Do not refresh your brown	ser while this VM is being deployed.
		Back Next Finish Cancel

After the .OVA file has finished uploading and importing, you are now ready to begin configuring the <u>engine</u>.

Shutting Down the Engine

To properly shut down the virtual engine, enter the following command at the login prompt in the vSphere client **Console** tab: poweroff

This shuts down the engine and updates the vSphere client with the new engine state.

Deploying the Virtual Engine on a Hyper-V Server

Deployment Requirements

A virtual engine is a software image that runs on a virtual machine. The , ExtremeCloud IQ - Site Engine, ExtremeControl, and ExtremeAnalytics virtual engines are packaged in the .ZIP file format and must be deployed on a Microsoft Hyper-V server.

Deploying the Virtual Engine

Use the following steps to deploy an ExtremeCloud IQ - Site Engine, ExtremeControl, or ExtremeAnalytics virtual engine on a VMware ESX or ESXi server.

1. Download the ExtremeCloud IQ - Site Engine, ExtremeControl, or ExtremeAnalytics virtual engine software image to your local machine where the vSphere client is installed and running.

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. Select the **Products** tab and select ExtremeCloud IQ Site Engine.
- 4. Select ExtremeCloud IQ Site Engine in the right-panel.
- 5. Select a version.
- 6. Download the ExtremeCloud IQ Site Engine, ExtremeControl, or ExtremeAnalytics virtual engine (appliance) image from the appropriate section.

Extreme Portal	Support Products	Partner	'S		
Search					٩
Automation ExtremeAnalytics ExtremeCampus ExtremeCloud Applications ExtremeCloud IQ ExtremeCloud IQ ExtremeCloud IQ - Site Engine	ExtremeCloud [™] IQ - Sit ExtremeCloud IQ - Site Engine, part of 1 connected, scalable SaaS management granular visibility with real-time analyti ExtremeCloud IQ - Site Engine offers yo Center, now with real-time flexibility an one license application.	e Engine the ExtremeClour solution that pro cs, and multi-ven u all the feature d reduced time-t	d IQ suite of produ ovides you with tas dor device manage s and functionality to-benefit, all for th	cts and services, is a c k automation, access ement across your net of Extreme Managem e convenience and lo	loud- control, tworks. ent w cost of
 ExtremeCloud[™] IQ - Site Engine 				📕 License D	ependency
+ ExtremeCloud IQ On Premise	Software & Downloads				^
 ExtremeWireless (Formerly IdentiFi) 	Download / Release Name 🔺 🛛 File Size	Release Type	▲ Release Date ▼	EOVM Date A() Tags	Link 🔺
+ On-Premise / Private Cloud	21.04.10.99 Analytics	Major	5/18/2021		
+ ExtremeControl					
+ ExtremeManagement	G 21.04.10.99.Control	Major	5/18/2021		
+ ExtremeRouting	5 21.04.10.99.Fabric Mgr	Major	5/18/2021		
+ ExtremeSecurity	E warmen a	Maine	100000		
 ExtremeSwitching 	L0 21.04.10.99.002.98	Major	5/18/2021		
+ ExtremeWireless					
 NetworkPacketBroker 	Release Notes				^
	Name 🔺		File Size 🔺	Release Date 🕶	
	🗎 XIQ-SE 21.04.10.99 Release Notes		1.49 MB	5/18/2021	

- 2. Extract the virtual engine file to a local directory.
- 3. Open the Hyper-V Manager.
- 4. From the Action menu, select Import Virtual Machine.

	_
File Action View Help	
🗢 🖬 New 🔸	
H Import Virtual Machine Actions	
Hyper-V Settings Il Machines WIN-9GLMPQG4PV0	
Virtual Switch Manager A State CPU Usage Assigned Memory Uptime Status New	•
Virtual SAN Manager No virtual machines were found on this server.	
Edit Disk 🖻 Hyper-V Settings	
inspect use	
Stop service Virtual SAN Manager	
Refrech militation (Charles Control of Charles Cont	
Help	
No vitual machine selected.	
Remove Server	
G Refresh	
View	•
2 Help	
Details	
No tem selected.	
Contract Micro	

The Import Virtual Machine wizard opens to the Before You Begin panel.

2	Import Virtual Machine
Before You B	egin
Before You Begin Locate Folder Select Virtual Machine Choose Import Type Summary	This wizard helps you import a virtual machine from a set of configuration files. It guides you through resolving configuration problems to prepare the virtual machine for use on this computer.
	< Previous Next > Finish Cancel

Select Next.

- 5. The Locate Folder panel opens.
- 6. Select the **Browse** button and navigate to the folder where you saved the engine image.
- 7. Select **Select Folder**, and then **Next**.

2	Import Virtual Machine	x	
Locate Folde	r		Select Folder X (<) (<) v (<) (<) (<) (<) (<) (<) (<) (<) (<) (<)
Before You Begin Locate Folder Select Virtual Machine Choose Import Type Summary	Specify the folder containing the virtual machine to import. Folder: Browse.		Organize New folder P Downloads P Music P Music P Pictures P Pictures P Virtual Hard Disks 2/27/2015 2:37 F Imac_appliance_64bit.6.2.0.189_hyperv P Program Files P Program Files P Program Files P Program Files P Select Folder
	< Previous Next > Finish Cancel		

The Select Virtual Machine panel opens.

8. Select the virtual machine you are importing, and then select Next.

*	Import Virtual Machine	x
Select Virtual	Machine	
Before You Begin	Select the virtual machine to import:	
Locate Folder Select Virtual Machine Choose Import Type Summary	Name Date Created nac_appliance_64bit.6.2.0.189 2/6/2015 8:07:58 PM	
	< Previous Next > Finish Canc	:el

The Choose Import Type panel opens.

	Import Virtual Machine
Choose Imp	ort Type
Before You Begin	Choose the type of import to perform:
Locate Folder	Register the virtual machine in-place (use the existing unique ID)
Select Virtual Machine	 Restore the virtual machine (use the existing unique ID)
Choose Import Type	O Copy the virtual machine (create a new unique ID)
Summary	
	< Previous Next > Finish Cancel

- 9. Select the radio button that corresponds to the appropriate type for your machine.
 - Register the virtual machine in-place (use the existing unique ID)—Select this option if your virtual machine files are saved on your virtual machine in the correct location.
 - Restore the virtual machine (use the existing unique ID)—Select this option if your virtual machine files are saved on a file share or removable drive and you want Hyper-V to move the files to the correct location.
 - Copy the virtual machine (create a new unique ID)—Select this option if you have a set of virtual files you want to import multiple times (e.g., if you are using them as a template for new virtual machines).
- 10. Select Next.

The Summary panel opens.

2	Import Virtual Machine
Completing	Import Wizard
Before You Begin Locate Folder Select Virtual Machine	You are about to perform the following operation. Description: Virtual Machine: nac. appliance. 64bit.6.2.0.189
Choose Import Type Configure Processor Connect Network Connect Network Summary	Import file: C:\VAC\nac_appliance_64bit.6.2.0.189_hyperv\nac_appliance_64bit.6.2.0. Import Type: Register (keep ID) Number of processors: 4 Network connection: Intel(R) PRO/1000 MT Network Connection - Virtual Switch Network connection: Intel(R) PRO/1000 MT Network Connection - Virtual Switch
	III > To complete the import and close this wizard, click Finish.
	< Previous Next > Finish Cancel

You are now ready to begin configuring the engine.

- If you are configuring an ExtremeCloud IQ Site Engine virtual engine, see <u>ExtremeCloud IQ Site</u> Engine Engine Configuration.
- If you are configuring an ExtremeControl virtual engine, see ExtremeControl Engine Configuration.
- If you are configuring on an ExtremeAnalytics virtual engine, see <u>ExtremeAnalytics Engine</u> <u>Configuration</u>.

ExtremeCloud IQ - Site Engine Engine Configuration

After the ExtremeCloud IQ - Site Engine virtual engine has been deployed on a VMware ESX or ESXi server, or a Hyper-V server using the instructions in <u>Engine Deployment</u>, you are ready to perform the initial engine configuration process described in this chapter.

This chapter also includes information on how to change your engine settings following your initial configuration, and how to upgrade or reinstall the engine software.

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
- Name Server IP address and domain name
- NIS (Network Information Services) Server IP address (optional)
- Network Time Protocol (NTP) server IP address

ExtremeCloud IQ - Site Engine And ExtremeAnalytics Licensing

If you are an existing Extreme Management Center customer, contact your representative to have your Extreme Management Center license migrated to an ExtremeCloud IQ - Site Engine license. The ExtremeCloud IQ - Site Engine license also includes licensing for ExtremeAnalytics.

- **NOTES:** ExtremeCloud IQ Site Engine is a subscription-based -only licensing model.
 - ExtremeCloud IQ Site Engine is not compatible with ExtremeCloud IQ Connect level account. Either the Pilot or Navigator level is mandatory.

You can view ExtremeCloud IQ and ExtremeCloud IQ - Site Engine license information by accessing Administration > Licenses.

There are three tiers of licenses for ExtremeCloud IQ - Site Engine and devices:

- Pilot Extreme devices
- Navigator 3rd party devices
- No License Status-Only devices

As you begin to <u>onboard ExtremeCloud IQ - Site Engine</u> and your devices, ExtremeCloud IQ will determine if you meet or exceed the <u>license limits</u> for each license type.

NOTE: Devices that do not have serial numbers or MAC addresses in Extreme Management Center must be Rediscovered after you upgrade to ExtremeCloud IQ - Site Engine before they can be onboarded to ExtremeCloud IQ.

> For the first 90 days after ExtremeCloud IQ - Site Engine is released, license usage will not be enforced for devices onboarded to ExtremeCloud IQ. When ExtremeCloud IQ starts evaluating license usage, if your number of devices exceeds your licenses available, ExtremeCloud IQ - Site Engine transitions to a license violation state and your access to ExtremeCloud IQ - Site Engine features and functionality is locked. To resolve the license shortage you need to access the Extreme Networks portal or ExtremeCloud IQ to evaluate the quantities of available Pilot and Navigator licenses versus the number of licenses required by ExtremeCloud IQ - Site Engine.

Licensing for Devices

When ExtremeCloud IQ - Site Engine has been <u>onboarded</u>, it starts sending requests to add the devices from its database to ExtremeCloud IQ.

As devices are added and discovered in ExtremeCloud IQ - Site Engine, they are onboarded to ExtremeCloud IQ, with a request for a license of the appropriate tier (Navigator, Pilot or No License) that each device will require.

Devices can be marked as <u>Unmanaged</u> in ExtremeCloud IQ, which means they are not using a license and available features are very limited.

The following arid	datails the type of licens	a required by each	device and engine type
The following grid	details the type of licens	e lequileu by each	device and engine type.

Device Type	License Tier Type	Number of Licenses Per Device
Extreme-supported Device (Includes VOSS/Fabric Engine, SLX, Extreme Access, VDX, Fabric Manager, Unified Switching VOSS/Fabric Engine, Unified Switching EXOS/Switch Engine, Summit Series, ERS Series, 200 Series, 700 Series, A Series, B Series, C Series, ICX Series, Security Appliances, MLXe Series)	Pilot	1
Chassis	Pilot	1
ExtremeControlengine	Pilot	1

ExtremeAnalyticsengine	Pilot	1
ExtremeCloud IQ - Site Engine	Pilot	1
Extreme Management Center	Pilot	1
vSensor	Pilot	1
All Other Devices (Includes Non-Extreme Device)	Navigator	1
Devices with Ping-Only profile	No License	0
Devices Added with No Access Profile	No License (These are not onboarded to ExtremeCloud IQ)	0
Status-Only Devices	No License (These are not onboarded to ExtremeCloud IQ)	0

For HiveOS APs, a Pilot license is required, but currently not enforced in ExtremeCloud IQ - Site **NOTE:** Engine Version 21.04.10. These are not onboarded to ExtremeCloud IQ through ExtremeCloud IQ -Site Engine.

License Limits and Violations

For each request to add a device to ExtremeCloud IQ - Site Engine, ExtremeCloud IQ determines if there are enough licenses of that type available.

As a result, one of the following actions happens:

- If there are enough licenses, device onboarding is successful.
- If there are not enough Navigator licenses, a Pilot license is used instead.
- If there are not enough Pilot licenses, the request is considered a license violation.

To correct a license limit violation, you must acquire more licenses (and, when the updated license is sent to ExtremeCloud IQ, it is used by ExtremeCloud IQ - Site Engine).

Devices Marked as Unmanaged

When devices are marked as Unmanaged in ExtremeCloud IQ, they are also Unmanaged in ExtremeCloud IQ - Site Engine.

Onboarded Unmanaged devices are indicated in the <u>XIQ Onboarded column</u> of the **Network > Site > Device** table by a red **X**.

• Add Denote ® Experts CV III Test State No. No. No. No. Config Change No. No. Config Change No. No.	• Asd Device © Inpurts CV If Pervice Type Family Primaze Reference Connector Top Oneconfield Upta Arthveid Config Chai Up 1362 Device 0 M850-62-86-64 Summit Serie 311.1.3 Image: Config Chai Mitter Config Chai Upta Arthveid Config Chai Up 1362 Device 0 vm3862003 Summit Serie 311.1.3 S61.8 Image: Config Chai S61.8 Image: Config Chai S61.8 Image: Config Chai Image: Config Cha	Prote through the barrier	ary Endpoint Location	s FlexReports							
Path Databitis Device Type Family Premare Reference Connector Non- Conducated Update Arthveid Config Change 103.328 Down 0 x850-62-64-64 Summt Sen 31.1.3	Pail Parmage Parmage Parmage Reference Connector NO Originational (0 bited and bi	 Add Device Export to C 	p/ ■								ς α
Vale 328 Down 0 X400-02-04-04 Summitiser. 31.1.13 X000-000000000000000000000000000000000	U20 324 Down 0 M60-62-04-04 Summit Serie 311.1.3 K K Computed on the content of the content	Pol Details	Device Type	Family	Firmware	faterence	Connector	XIQ Onboarded	Upda	Archived	Config Change
Up: 188 Down D vm8880105 Summitiser. 304.0483 MQ Unmarkaged Softmitiser. 30.0.0483 Softmitiser. 30.0.000000000000000000000000000000000	Up 186 Down 0 vm8868103 Summt Sant. 304.0483 Santa Configuration staged for device. vm3865103 Summt Sant. 311.13 S6.1.8 Up 2 Down 182 X485-24*445 Summt Sant. 311.13 8.8.1.8 Image: Configuration Staged for device. Vm3865105 Summt Sant. 311.13 S6.1.8 Image: Configuration Santa Vm3865105 Summt Santa Sinta Image: Configuration Santa Sinta Image: Configurati Sinta Image: C	Up: 326 Down: 0	X#50-02-240-04	Summit Seri	\$1.1.1.3			×			
Configuration stages for device. VIR38EDIDS SummitSeri	Configuration staged for device vm3865035 SummitSanL 311.13 361.8 Up 2 Down 192 X485-241-45 SummitSanL 311.13 4 86.1.8 Up 2 Down 192 X405-247-45 SummitSanL 311.13 4 86.1.8 Up 2 Down 192 X405-247-45 SummitSanL 311.13 4 86.1.8 Up 2 Down 192 X405-247-45 SummitSanL 81.3.3 4 36.1.8 Up 0 Down 193 Vmail Application AL Externe An 85.3.46 4 Up 0 Down 196 Vmail Access Contract Externe An 85.512 4 Up 2 Down 192 M68HCM3R Reinci Man 85.325 36.1.6	Up: 196 Down: 0	vm3860/05	Summit Seri	30.4.0.483			200	Unmanage	1	
Up: 2 Devin: 192 X485-24T-45 Summit Seru. 31.1.3 ✓ 36.1.8 ✓ Up: 2 Devin: 192 X485-24T-45 Summit Seru. 31.1.3 ✓ 3.6.1.8 ✓ Up: 2 Devin: 192 X485-24T-45 Summit Seru. 8.5.3.4 ✓ 3.6.1.8 ✓ Up: 0 Devin: 198 Vitual Application A Extreme An 8.5.3.4 ✓ ✓ Up: 0 Devin: 198 Vitual Application A Extreme An 8.5.1.2 ✓ ✓ Up: 0 Devin: 198 Vitual Application A Bit Serue Site Serue ✓ ✓	Up 2 Down 162 XX85-241-45 Summit Sert. 31.1.3 4 3.6.1.8 4 Up 2 Down 162 XX85-241-45 Summit Sert. 31.1.3 4 3.6.1.8 4 Up 2 Down 162 XX85-241-45 Summit Sert. 31.1.3 4 3.6.1.8 4 Up 3 Down 162 XX85-241-45 Summit Sert. 8.8.3.46 4 4 Up 3 Down 166 Vinual Application A. Externe Co. 8.55.12 4 4 Up 3 Down 162 AVABRICHSR Reind Nam. 8.8.3.25 3.6.1.4 4	Configuration staged for device.	vm386D105	Summit Seri	\$1.1.1.5		3.6.1.8	_		-	
Up: 2 Down: 192 XX85-24T-45 Summit Seri	U0:2 Down M2 XX35-247-45 Summt Sert. 211.13 ¥ 3.61.8 ¥ Up 0 Down 108 Virtual Application A Extreme An 8.53.46 Up 0 Down 108 Virtual Application A Extreme An 8.53.46 Up 0 Down 108 Virtual Application A Extreme An 8.53.46 Up 0 Down 108 Virtual Application A Extreme Co 8.55.12 Up 2 Down 102 VieBRICMSR Reinc Man 8.53.28 3.61.4	Up 2 Down 162	2435-247-45	Summit Seri.	31.1.1.3	*	3.6.1.8			*	
Up 0 Devin 198 Vitual Application A Extreme An # 5.3.46 Up 0 Devin 196 Vitual Application A Extreme Co 8.5.512 Up 2 Devin 192 Av&RICKISR Ratic Vitual Application A 8.5.325	Up 8 Down 198 Virbuel Application A 8 85.48 Up 8 Down 198 Virbuel Application A 8 55.12 Up 8 Down 198 Virbuel Application A 8 55.12 Up 2 Down 198 Virbuel Application A 8 55.12 Up 2 Down 198 Virbuel Application A 8 55.12 Up 2 Down 192 Virbuel Application A 8 55.12 Up 2 Down 192 Virbuel Application A 8 55.12 Up 2 Down 192 Virbuel Application A 8 55.12 Up 2 Down 192 Virbuel Application A 8 55.12 Up 2 Down 192 Virbuel Application A 8 55.12 Up 2 Down 192 Virbuel Application A 8 55.12 Up 2 Down 192 Virbuel Application A 8 55.12 Up 2 Down 192 Virbuel Application A 8 55.12 Up 2 Down 192 Virbuel Application A 8 55.12 Up 2 Down 192 Virbuel Application A 8 55.12 Up 2 Down 192 Virbuel Application A	Up: 2 Down: 162	2435-247-45	Summit Seri	\$1.1.1.3	*	3.6.1.8			*	
Up 0 Down 196 Vinuel Access Contr & Draveme Co 85512 Up 2 Down 192 RelPCMSR Romon 85326 361.6	Up 2 Down: 188 Virtual Access Contr 6 streme Co 8 55.12 Up 2 Down: 182 HABRICHISH Rein: 18.8.28 3 61.4	Up: 0 Down: 198	Virtual Application A.,	Extension	8.5.3.40						
Up 2 Down 182 RABRONSR ReproVision. 8.8.3.25 8.6.1.6	Up 2 Down 162 RefRICMSR Retriction 8.8.326 3.6.1.6 ≪ < Rage 1 of1 > ≫ C ■ Retrict ■ Boolmark. Displaying 1-6.	Up: 0 Down: 196	Virtual Access Contr	Extreme Co	8.5.5.12						
	« < Eqs 1 of 1 > > C = Feet = Estimate Displaying 1-6	Up: 2 Down: 162	NBRICHSR	Rabric Man	1.5.3.25		3.6.1.6				
	« < Eqs 1 of 1 > > C Rest Rest Rest C Solvarit Opping 1-6										
	< < Iaps 1 of 1 > > C Benc Distinguist Distinguist - Distinguist										
	< < Iaps 1 of 1 > > C Benc District Dist										
	< < Iaps 1 of 1 > > C Bene Distant Displaying 1-6.										
	K < Eqs. 1 of 1 > > C France Q Boolmark Subject 1-6										
	K < Rape 1 of 1 > > C @ Reset @ Bookmark: Displaying 1-8.										

For more details on the Network > Site > Device table, visit Onboarding Unmanaged Devices.

Logging into ExtremeCloud IQ - Site Engine

Configuring the ExtremeCloud IQ - Site Engine Engine

To configure the virtual engine to run the ExtremeCloud IQ - Site Engine applications:

1. In the **Console** tab of the vSphere client, login as root with no password, and then press [Enter]. The following screen displays.



2. Press [Enter] to begin the setup.

The Root Password Configuration screen displays:



Note: You must set a new root password. The root password will be used to access the CLI of the ExtremeCloud IQ - Site Engine VM.

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



After you create the new root password, a screen displays where you can specify a user other than root to run the ExtremeCloud IQ - Site Engine server, if desired. This user becomes the admin user for the server. (Use the root user account when performing upgrades and accessing CLI).



4. Enter **y** to use the root user. Accept your selection.

Enter **n** to either use the "netsight" user or to specify a different user. Re-enter the password and then accept your selection.



5. In the **Suite Network Configuration** screen, enter the requested configuration information for each line and press **[Enter]**.

Enter the IP address of the name server. If you are using a name server, you must enter a domain name for the engine (appliance). If you are using an NIS server to authenticate users logging into the engine, make sure the NIS domain name is valid or users will not be able to log in to the ExtremeCloud IQ - Site Engine applications.



6. In the **Confirm Network Settings** screen, you can accept the current configuration or modify the settings.



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



8. In the SNMP Configuration summary screen, enter 0 to accept the settings.



9. 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 11.

Note that your NTP server should be using the same NTP settings as those configured for your virtual engine (i.e., the same settings as the VMs that are hosted on the NTP server).

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
NTD is used to configure the date and time to expuse accuracy of time
in it is used to configure the date and the to ensure accuracy of the
values for SMMP communications and logged events. Up to 5
server IP addresses may be entered if NTP is used.
Do you want to use NTP (yzn) [y]?
bo gou wane to ale nit ty n/ tg31
Please enter a NTP Server IP Address (Required): 192.168.1.200
Would you like to add another server (y/n) [n]?

10. In the NTP Servers validate selection screen, enter O to accept the current settings and proceed to the Set Time Zone screen at step 13.



11. 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: Fri 14 May 2021 01:01:58 PM EDT 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
ss - 2 digit seconds
Please enter the month [05]:
Please enter the day of the month [14]:
Please enter the year [2021]:
Please enter the hour of day [13]:
Please enter the minutes [04]:
Please enter the seconds [04]:

12. In the Use UTC screen, select whether you want the system clock to be set to 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 (u/n) [n]?	se UTC
Do you want to use UTC (y/n) [n]?	he system clock can be set to use UTC. Specifying no for using UTC, ets the hardware clock using localtime.
- 3	o you want to use UTC (y/n) [n]?

13. In the **Set Time Zone** screen, type the number that corresponds to the appropriate time zone and press **[Enter]**.



14. In the Modify Settings screen, you can accept the current configuration or modify the settings.



The ExtremeCloud IQ - Site Engine application software is automatically installed. This could take a few minutes. When you see the following screen, configuration is complete.



Note: After you have completed the configuration, it is important to take a snapshot of your engine configuration to be used in the event an engine image recovery is required. For instructions on how to take a snapshot, see your vSphere client documentation.

Launching ExtremeCloud IQ - Site Engine

Now that you have configured the ExtremeCloud IQ - Site Engine virtual engine, you are ready to access ExtremeCloud IQ - Site Engine from a remote client machine.

Open a browser window on the remote client machine and enter the ExtremeCloud IQ - Site Engine Launch page URL in the following format:

https://<servername>:8443/

where *<servername>* is the ExtremeCloud IQ - Site Engine virtual engine IP address or hostname, and 8080 is the required port number. For example, https://10.20.30.40:8443/ ExtremeCloud IQ - Site Engine login page opens.

Log in as root with the same password you defined in $\underline{\text{step 3}}$ or as the user you specified in $\underline{\text{step 4}}$.

This is because the ExtremeCloud IQ - Site Engine Server has a single pre-defined user, which is the user who performed the ExtremeCloud IQ - Site Engine installation. After the initial user has logged in, additional users (with usernames valid for Ubuntu) can log in.

Onboarding ExtremeCloud IQ - Site Engine

To access ExtremeCloud IQ - Site Engine, you must first complete the steps to onboard ExtremeCloud IQ - Site Engine to ExtremeCloud IQ.

There are two scenarios by which you can onboard ExtremeCloud IQ - Site Engine:

- <u>After Upgrading to ExtremeCloud IQ Site Engine from Extreme Management Center Versions</u> 8.4.4 or 8.5.5.
- <u>After Initial Installation of ExtremeCloud IQ Site Engine</u>

After Upgrading to ExtremeCloud IQ - Site Engine from Extreme Management Center Versions 8.4.4 or 8.5.5

When you upgrade from Extreme Management Center to ExtremeCloud IQ - Site Engine, if you used the softlaunch feature of Extreme Management Center in ExtremeCloud IQ, you need to remove Extreme Management Center from ExtremeCloud IQ before onboarding ExtremeCloud IQ - Site Engine.

After you upgrade your Extreme Management Center to ExtremeCloud IQ - Site Engine, you need to onboard ExtremeCloud IQ - Site Engine:

1. Log in to ExtremeCloud IQ - Site Engine. Enter your ExtremeCloud IQ - Site Engine username and password. Select Login.



2. Accept the License Agreement.

	License Agreement
PLEASE READ ALL OF T	HE FOLLOWING TERMS AND CONDITIONS OF THIS END USER LICENSE AGREEMENT.
This End User License Ag	reement ("Agreement") is a legal agreement between You and/or the entity You represent
and Extreme Networks, In	c., on behalf of itself and its affiliates, including, but not limited to, Extreme Network Ireland
Ops Limited (collectively, '	"Extreme") for the Software (defined below) licensed by Extreme or its licensors.
By downloading, installing	, copying, accessing, or using the Software, or activating a Software license key, or by
clicking an "I Agree" or sin	nilar button, or by opening the Software media, You agree to the terms and conditions of this
Agreement as a condition	of Your use of, and right to use, the Software.
If You do not agree to all t Software was delivered to Hardware Product.	he terms and conditions in this Agreement, do not download, install or use the Software. If the You embedded in an Extreme Hardware Product, do not install or use that Extreme
Extreme may make chang	es to this Agreement at any time and will provide written notice of such changes to You and
give You an opportunity to	accept those changes. Your continued use of the Software after such changes have been
posted will signify your as	sent to acceptance of the revised terms.
If You and Extreme have a	signed a separate written agreement covering Your rights and duties with respect to the
Software, then that writter	agreement take precedence over any conflicting terms in this Agreement.
Your privacy is important t	o Extreme. Extreme's Privacy Policy is located at
https://www.extremenetwo	orks.com/company/legal/privacy/. Please read our Privacy Policy for information related to
Extreme's collection, use	and disclosure of Your personal information. By agreeing to the terms of this Agreement, You
are also accepting the ter	ms of Extreme's Privacy Policy.
1 DEFINITIONS Capitali	zed terms used in this Arreement are defined in Section 18 helow
	✓ I accept the License Agreement

Select Next.

3. To onboard ExtremeCloud IQ - Site Engine to ExtremeCloud IQ, provide your ExtremeCloud IQ email address and password.

١	Nelcome to ExtremeCloud IQ - Site Engine
Back	Onboard to ExtremeCloud IQ
Please en	ter your ExtremeCloud IQ credentials to onboard the ExtremeCloud IQ - Site Engine.
	Email Password Don't have an account? Register here Advanced Onboard

After ExtremeCloud IQ - Site Engine has successfully onboarded, you can now access ExtremeCloud IQ - Site Engine.

If your environment requires HTTP Proxy or other advanced settings, select the Advanced link. If you do not have an ExtremeCloud IQ account, select the Register Here link.

After Initial Installation of ExtremeCloud IQ - Site Engine

Complete the following steps to onboard ExtremeCloud IQ - Site Engine after you install ExtremeCloud IQ - Site Engine:

1. Accept the ExtremeCloud IQ - Site Engine License Agreement.

	License Agreement
PLEASE READ ALL OF TH	E FOLLOWING TERMS AND CONDITIONS OF THIS END USER LICENSE AGREEMEN
This End User License Agre	eement ("Agreement") is a legal agreement between You and/or the entity You represent
and Extreme Networks, Inc	, on behalf of itself and its affiliates, including, but not limited to, Extreme Network Ireland
Ops Limited (collectively, "E	:xtreme") for the Software (defined below) licensed by Extreme or its licensors.
By downloading, installing,	copying, accessing, or using the Software, or activating a Software license key, or by
clicking an "I Agree" or simi	far button, or by opening the Software media, You agree to the terms and conditions of this
Agreement as a condition o	f Your use of, and right to use, the Software.
If You do not agree to all the Software was delivered to Y Hardware Product.	e terms and conditions in this Agreement, do not download, install or use the Software. If th fou embedded in an Extreme Hardware Product, do not install or use that Extreme
Extreme may make change	s to this Agreement at any time and will provide written notice of such changes to You and
give You an opportunity to a	accept those changes. Your continued use of the Software after such changes have been
posted will signify your asse	and to acceptance of the revised terms.
If You and Extreme have sig	ned a separate written agreement covering Your rights and duties with respect to the
Software, then that written a	agreement take precedence over any conflicting terms in this Agreement.
Your privacy is important to	Extreme. Extreme's Privacy Policy is located at
https://www.extremenetwori	ks.com/companyllegal/privacy/. Please read our Privacy Policy for information related to
Extreme's collection, use ar	di disclosure of Your personal information. By agreeing to the terms of this Agreement, You
are also accepting the term	s of Extreme's Privacy Policy.
1 DEFINITIONS Canitalize	ad terms used in this Arreement are defined in Section 18 helow
	I accept the License Agreement

2. Enter your ExtremeCloud IQ email address and password. Select Login.

v	Velcome to ExtremeCloud IQ - Site Engine
Back	Onboard to ExtremeCloud IQ
Please ent	ter your ExtremeCloud IQ credentials to onboard the ExtremeCloud IQ - Site Engine.
	Email
	Password
	Death have a second 2 Review have
	Don't have an accountr Register here Advanced
	Onboard

If your environment requires HTTP Proxy or other advanced settings, select the Advanced link. If you do not have an ExtremeCloud IQ account, select the Register Here link.

3. ExtremeCloud IQ retrieves the license information and sends it to ExtremeCloud IQ - Site Engine. ExtremeCloud IQ - Site Engine is onboarded to ExtremeCloud IQ.

ExtremeCloud IQ Site Engine	
Usentame	
LOON	
Copylight & 2021 Edwares Roburdin, Son, All rights resurred. Support 1 July	

You can now access the ExtremeCloud IQ - Site Engine login page.

Enter the Username and Password you specified during the ExtremeCloud IQ - Site Engine installation.

Onboarding Devices

When ExtremeCloud IQ - Site Engine has been onboarded, it can start sending requests to add the devices from its database to ExtremeCloud IQ.

NOTES: Devices with IPv6 addresses in ExtremeCloud IQ - Site Engine will not be onboarded as locally-managed devices in ExtremeCloud IQ. Only devices with IPv4 addresses qualify.

As devices are added and discovered in ExtremeCloud IQ - Site Engine, they are onboarded to ExtremeCloud IQ, with a request for a <u>license</u> of the appropriate tier (Navigator, Pilot or No License) that each device will require.

View the ExtremeCloud IQ - Site Engine and ExtremeCloud IQ Onboarding Flowchart for a detailed chart on how devices are onboarded to ExtremeCloud IQ and managed by ExtremeCloud IQ - Site Engine.

XIQ Onboarded Status for Devices

After an attempt is made to onboard a device, the XIQ Onboarded column of the Network > Site > Device table indicates the status of the onboarding attempt.

are Archives Configuration Temp	planes fleports								
Add Device Begort to CS	ry Endpoint Location	s PlexReports							τ. α
Pol Details	Device Type	Family	Firmware	faterence	Connector	XIQ Onboarded	Upda	Archived	Config Changed
Up: 326 Down: 0	X#50-02-245-04	Summit Seri	31.1.1.3			×			
Up: 196 Down: 0	VERBORIOS	Summit Seri	30.4.0.483				Unmanages		
Configuration staged for device.	vm3860105	Summit Seri	\$1.1.1.3		3.6.1.8	_		-	
Up 2 Down 162	3435-247-45	Summit Seri	31.1.1.3	*	3.6.1.8			*	
Ud: 2 Down: 162	2435-247-45	Summit Seri	31.1.1.3	*	3.6.1.8				
Up 0 Down: 198	Virtual Application A.,	Extension An	13.3.46						
Up: 0 Down: 196	Virtual Access Contr	Extreme Co	85512						
Up: 2 Down: 162	PABRICIUSR	Rabric Man	15325		3.6.1.6				
			_						
-4C - C Eage 1 of1	> > 0 8	S Reset	Bookmark						Displaying 1 - 8 of 8

- Black check mark Indicates that the device is onboarded to ExtremeCloud IQ.
- Red X Indicates the device is onboarded but Unmanaged, which means it is not using a license, it has read-only device-level support, and available features in ExtremeCloud IQ Site Engine are limited. Other functionality, including Status Polling, Historical Device + Port Statistics Collection, Existing Scheduled Tasks, and Archives, are supported for devices with Unmanaged status, but these devices cannot be configured for new tasks or new archives.
 - **NOTES:** In ExtremeCloud IQ Site Engine version 22.09.10, only use ExtremeCloud IQ to set an ExtremeCloud IQ Site Engine onboarded device to Unmanaged as a temporary measure while you obtain more licenses.

If you mark a device as Unmanaged so it does not trigger a <u>license limit violation</u>, you can then access ExtremeCloud IQ - Site Engine and delete the device before the license violation occurs.

You can perform an enforce for an ExtremeControl engine with an Unmanaged status; however, if the device has an Unmanaged status, then the enforce does not reconfigure the device and changes are not written to the device.

When devices are marked as Unmanaged in ExtremeCloud IQ, they are also Unmanaged in ExtremeCloud IQ - Site Engine.

In addition, existing ExtremeAnalytics functionality for devices with an Unmanaged status is still supported, but only with existing configuration.

• Blank - Indicates the device is not successfully onboarded to ExtremeCloud IQ from the ExtremeCloud IQ - Site Engine because either it is already onboarded to ExtremeCloud IQ (either from another ExtremeCloud IQ - Site Engine or by using the IQ Agent to connect directly), or because ExtremeCloud

- IQ Site Engine lost its connection to ExtremeCloud IQ.
- **NOTE:** If a device's status is Blank, it has limited features available in ExtremeCloud IQ Site Engine because management of the device is owned by ExtremeCloud IQ.
- N/A Indicates the device is not eligible to be onboarded to ExtremeCloud IQ because it does not have a valid serial number or MAC address, or Extreme does not yet offer onboarding support for the device.
 - **NOTE:** If ExtremeCloud IQ Site Engine does not recognize a device's serial number or MAC address, right-click on the device and select Rediscover to attempt to discover the device's serial number or MAC address. After the device's serial number or MAC address is discovered, it can be onboarded to ExtremeCloud IQ during the next onboarding cycle.

Restoring a Database from a Windows Server to the Engine

This section describes several ExtremeCloud IQ - Site Engine configuration changes that are required if you are moving your installation from a Windows platform system to the ExtremeCloud IQ - Site Engine virtual engine. Perform these steps after restoring your database to the new engine. (For information on restoring a database, see the Server Information section in the *ExtremeCloud IQ - Site Engine Suite-Wide Tools User Guide.*)

Changing Console

Use the following instructions to change the location of syslog and trap information to the new location on the engine.

Changing Syslog Location

Change the Syslog Log Manager to point to the new location on the engine. This will enable the display of syslog information in the **Syslog Event View** tab.

- 1. From the Console menu bar, select Alarm/Event > Tools > Event View Manager.
- 2. Select on the **Syslog** entry under Available Log Managers, and select the **Edit** button. **The Log Manager Parameters window opens.**
- 3. Change the path in the Log Directory field to /var/log/messages.
- 4. Change the Pattern to Red Hat LINUX Syslog Pattern.
- 5. Select OK.

Changing Traps Location

Change the Traps Log Manager to point to the new location on the engine. This will enable the display of trap information in the **Traps Event View** tab.

- 1. From the Console menu bar, select Tools > Alarm/Event > Event View Manager.
- 2. Select the **Traps** entry under Available Log Managers, and select the **Edit** button. **The Log Manager Parameters window opens.**
- 3. Change the path in the Log Directory field to %logdir%/traps.
- 4. Select OK.

Changing Inventory Settings

If you are using Inventory Settings in ExtremeCloud IQ - Site Engine, you must change the Data Storage Directory path to point to the new location on the engine. The Data Storage Directory is where all Inventory data is stored, including capacity planning reports, configuration templates, archived configurations, and property files.

- 1. Select Administration > Options.
- 2. Expand the Inventory Manager options folder and select Directory Path in the Data Storage section.
- Change the path to the correct new location. On a default installation, the path would be :/usr/local/Extreme_ Networks/NetSight/appdata/InventoryMgr/
- 4. Select OK.

Changing ExtremeCloud IQ - Site Engine Engine Settings

Use these steps if you need to change your ExtremeCloud IQ - Site Engine virtual engine settings following your initial engine configuration. Perform these steps in the vSphere client **Console** tab or login using an ssh session to ExtremeCloud IQ - Site Engine CLI..

Changing Basic Network Configuration

To change basic network configuration settings such as hostname and engine IP address, enter the following command at the login prompt in the **Console** tab: /usr/postinstall/dnetconfig

This will start the network configuration script and enable you to make the required changes. You must reboot the engine for the new settings to take effect.

Changing SNMP Configuration

To change SNMP configuration settings such as system contact, system location, Trap Server, SNMP Trap Community String, SNMP User, SNMP Authentication, and SNMP Privacy

credentials, enter the following command at the login prompt in the **Console** tab: /usr/postinstall/snmpconfig

This will start the SNMP configuration script and enable you to make the required 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 login prompt in the **Console** tab: /usr/postinstall/dateconfig

This will start the date and time configuration script and enable you to change the settings.

Upgrading ExtremeCloud IQ - Site Engine Engine Software

Upgrades to the ExtremeCloud IQ - Site Engine engine software are available on the ExtremeCloud IQ - Site Engine web page.

Prior to performing an upgrade, you can create a snapshot of the engine that you can revert to in the event an upgrade fails. Refer to the vSphere client documentation for instructions on creating a snapshot.

- 1. On a system with an internet connection, go to the ExtremeCloud IQ Site Engine web page: http://extranet.extremenetworks.com/downloads/pages/NMS.aspx.
- Enter your email address and password.
 You will be on the ExtremeCloud IQ Site Engine page.
- 3. Select the **Software** tab and select a version of ExtremeCloud IQ Site Engine.
- 4. Download the ExtremeCloud IQ Site Engine virtual engine image from the ExtremeCloud IQ Site Engine Virtual Appliance (engine) section.
- 5. Use FTP, SCP, or a shared mount point, to copy the file to the ExtremeCloud IQ Site Engine virtual engine.
- 6. SSH to the engine.
- 7. Cd to the directory where you downloaded the upgrade file.
- 8. Change the permissions on the upgrade file by entering the following command: chmod + x ./ExtremeCloudIQSiteEngine_<version>_64bit_install.bin
- 9. Run the install program by entering the following command: ./ExtremeCloudIQSiteEngine_<version>_64bit_install.bin The upgrade automatically begins.

The ExtremeCloud IQ - Site Engine Server are restarted automatically when the upgrade is complete. Because your ExtremeCloud IQ - Site Engine engine settings were migrated, you are not required to perform any configuration on the engine following the upgrade.

Reinstalling ExtremeCloud IQ - Site Engine Appliance Software

In the event that a software reinstall becomes necessary, restore an engine snapshot that you previously made using the vSphere client. Refer to the vSphere client documentation for instructions on restoring a snapshot.

If you do not have an engine snapshot to restore, you must re-deploy and reconfigure the ExtremeCloud IQ - Site Engine virtual engine following the instructions in <u>Engine Deployment</u> and this chapter.

Note: Be aware that a reinstall procedure reformats the hard drive, reinstalls all the ExtremeCloud IQ - Site Engine engine software, the operating system, and all related Linux packages. We recommend backing up your hard drive before reinstalling.

ExtremeControl Engine Configuration

After the ExtremeControl virtual engine has been deployed on a VMware ESX or ESXi server, or a Hyper-V server using the instructions in <u>Engine Deployment</u>, you are ready to perform the initial engine configuration process described in this chapter.

This chapter also includes information on how to change your engine settings following your initial configuration, and how to upgrade or reinstall the engine software.

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
- ExtremeCloud IQ Site Engine Server IP address
- Name Server IP address and domain name
- Network Time Protocol (NTP) server IP address

Licensing for ExtremeControl

The licensing details for ExtremeControl vary depending on whether ExtremeCloud IQ - Site Engine is <u>onboarded</u> after upgrading from Extreme Management Center or if it is initially installed.

After Upgrading From Extreme Management Center versions 8.4.4 or 8.5.5

If you are upgrading from Extreme Management Center versions 8.4.4 or 8.5.5 to ExtremeCloud IQ - Site Engine version 22.09.10, the licensing and capabilities of ExtremeControl does not change. The following are included in the licenses:

- NMS-ADV License includes 500 Access Control End-Systems and 50 Guest and IoT Manager (GIM) licenses.
- NMS-xx License includes 250 Access Control End-Systems and 25 GIM licenses.

If you had an NMS-xx License with Extreme Management Center, you can upgrade to an NMS-ADV License on the Extreme Portal after you onboard ExtremeCloud IQ - Site Engine.

NOTE: Air gapped mode (where ExtremeCloud IQ - Site Engine is not connected to ExtremeCloud IQ) is not supported for ExtremeCloud IQ - Site Engine version 21.04.10.

Upon Initial Installation

If you are completing an initial install of ExtremeCloud IQ - Site Engine, there is no end-system license included. The evaluation license can be generated on the Extreme Portal which includes unlimited end-systems and Guest and IoT Manager (GIM) licenses.

Configuring the ExtremeControl Engine

To configure the virtual engine to run the ExtremeControl software:

1. In the **Console** tab of the vSphere client, login as root with no password and press [Enter].

The following screens display: Welcome to Extreme Networks Access Control Engine 21.4.10.xx controlengine login: root Extreme Networks Access Control Engine 21.4.10.xx Configuration

Welcome to the ExtremeControl Engine 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 displays:

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.

- 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 ExtremeControl engine Configuration screen, enter the requested configuration information for each line and press [Enter].

ExtremeControl Configuration

Enter the hostname for the appliance [nacappliance]: Enter the IP address for <hostname> (Required): Enter the IP netmask [255.255.255.0]: Enter the gateway address [192.168.2.1]: Enter the IP address of the name server (Optional): Enter the domain name for <hostname> (Optional): Enter the IP address of the Server (Required):

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 ExtremeCloud IQ - Site Engine Console.
Please enter the SNMP user name [snmpuser]:
Please enter the SNMP authentication protocol - MD5 or SHA [MD5]:
Please enter the SNMP authentication credential [snmpauthcred]:
Please enter the SNMP privacy protocol - DES or AES [DES]:
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 <u>step 8</u>.

Configure Date And Time Settings

 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 Servers 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 2018
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 [04]:
Please enter the day of the month [24]:
Please enter the year [2018]:
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 local time.

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 Appliance Configuration screen, review the current settings and press [Enter] to continue.

Access Control Configuration Access Control Engine Configuration: Host Info: <hostname>/<IP address>/<netmask> Gateway/Name Server/Domain: <gateway>/<dns server>/<domain> SNMP User: snmpuser SNMP Authentication Protocol: snmpauthcred SNMP Authentication: snmpprivcred SNMP Privacy Protocol: SNMP Privacy: ExtremeCloud IQ - Site Engine Server IP: <ECC server ip> Press [enter] to continue:

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

Appliance Network Configuration Complete

When you see the following screen, configuration is complete.

Extreme Networks - ExtremeControl Appliance - Setup Complete

Setup of the NAC Appliance is now complete. Details of the appliance setup process are located in the log files in the /var/log/install directory.

Note: After you have completed the configuration, it is important to take a snapshot of your engine configuration to be used in the event an engine image reinstall is required. For instructions on how to take a snapshot, see your vSphere client documentation.

You are now ready to use ExtremeCloud IQ - Site Engine to manage your ExtremeControl. If this is your initial commissioning of the engine, you can launch ExtremeCloud IQ - Site Engine and select **Getting Started** from the **Help** menu for information on using ExtremeCloud IQ - Site Engine to configure and manage your ExtremeControl.

If you have reinstalled your ExtremeControl software, use ExtremeCloud IQ - Site Engine to enforce the engine. Enforcing writes your ExtremeCloud IQ - Site Engine configuration information to the engine.

Note:

When you add the virtual engine to ExtremeCloud IQ - Site Engine, you will be asked to supply a virtual ExtremeControl engine license number. (When you purchased your engine, you received a Licensed Product Entitlement ID. This Entitlement ID allows you to generate a product license. Refer to the instructions included with the Entitlement ID that was sent to you.)

Unlicensed virtual ExtremeControl engines will appear with an orange arrow icon in ExtremeCloud IQ - Site Engine, and cannot be enforced. You can view the engine license status in the Administration > Diagnostics > Server > Server Licenses tab in ExtremeCloud IQ - Site Engine.

Changing ExtremeControl Engine Settings

This section provides instructions for changing your ExtremeControl engine settings following your initial engine configuration, should the need arise. Depending on the settings you want to change, you can use either the Control > **Access Control** tab of ExtremeCloud IQ - Site Engine or

the vSphere client **Console** tab to make the changes.

Using the Access Control tab

Use the **Access Control** tab to easily change <u>Engine Settings</u> including DNS, NTP, SSH, and SNMP configuration. You can also use the **Access Control** tab 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 tab to change the following:

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

To access the Engine Settings tab:

- 1. Open the Control > Access Control tab.
- 2. In the left-panel tree, expand the Configuration folder.
- 3. In the Configuration folder, expand the Global & Engine Settings folder.
- 4. In the Global & Engine Settings folder, expand the Engine Settings folder.
- 5. Select the desired engine (typically **Default** unless you have configured a custom engine setting).
- 6. In the right panel, select the <u>Network Settings</u> tab.

Changing Hostname, Gateway, and Static Routes

On the Control > Access Control tab, use the Interfaces window for an engine to change the engine hostname, default gateway, and static routes.

- 1. Expand the Engines folder in the left-panel tree.
- 2. Select the ExtremeControl engine
- 3. Select the right-panel **Details** tab.
- 4. In the Interface Summary section, select **Edit** to open the <u>Interfaces window</u> where you can change the engine hostname and default gateway.
- 5. Select Save.
- 6. In the Interface Summary section, select **Static Routes** to open the <u>Static Route Configuration window</u> where you can add or edit the static routes used for advanced routing configuration.

Using the vSphere Client Console Tab

Use the vSphere client **Console** tab to change the engine IP address, ExtremeCloud IQ - Site Engine server IP address, and web service credentials. If desired, you can also use the **Console** tab to change basic network settings such as engine hostname, SNMP configuration, and date and time settings, although you should use NAC Manager to make these changes, if possible (see <u>Using the Access Control tab</u>).

Changing the ExtremeCloud IQ - Site Engine Server IP Address

To change the IP address of the ExtremeCloud IQ - Site Engine server, enter the following command at the login prompt in the **Console** tab: /opt/nac/configMgmtIP <IP address>

Enter the following command to start using the new ExtremeCloud IQ - Site Engine server: nacctl restart

Changing Web Service Credentials

The Web Service credentials provide access to the ExtremeControl engine Administration web page and the web services interface for the ExtremeControl engine. Engines are shipped with a preconfigured default password.

If you have changed the credentials on the Access Control tab (in the **Engine Settings** window) and then install a new engine that uses the default password, you will not be able to monitor or enforce to the new engine until you change the password on the engine using the command below. The credentials you enter on the engine must match the credentials specified on the Access Control tab in the **Engine Settings** window.

To change Web Service credentials, enter the following command at the login prompt in the **Console** tab:

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

Enter the following command to restart the engine:

nacctl 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 login prompt in the **Console** tab: /usr/postinstall/nacconfig

This will start the network configuration script and enable 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 login prompt in the **Console** tab: /usr/postinstall/dateconfig

This will start the date and time configuration script and enable you to change the settings.

Upgrading ExtremeControl Engine Software

Instructions for performing the software upgrade are available <u>here</u>.

Prior to performing an upgrade, you can create a snapshot of the engine that you can revert to in the event an upgrade fails. Refer to the vSphere client documentation for instructions on creating a snapshot.

Reinstalling ExtremeControl Engine Software

In the event that a software reinstall becomes necessary, restore an engine snapshot that you previously made using the vSphere client. Refer to the vSphere client documentation for instructions on restoring a snapshot.

If you do not have an engine snapshot to restore, you must re-deploy and reconfigure the ExtremeControl virtual engine following the instructions in <u>Engine Deployment</u> and this chapter.

Note: Be aware that a reinstall procedure reformats the hard drive, reinstalls all the ExtremeControl engine software, the operating system, and all related Linux packages.

ExtremeAnalytics Engine Configuration

After the ExtremeAnalytics virtual engine has been deployed on a VMware ESX or ESXi server, or a Hyper-V server using the instructions in <u>Engine Deployment</u>, you are ready to perform the initial engine configuration process described in this chapter.

This chapter also includes information on how to change your engine settings following your initial configuration, and how to upgrade or reinstall the engine software.

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
- Name Server IP address and domain name
- NIS (Network Information Services) Server IP address (optional)
- Network Time Protocol (NTP) server IP address

ExtremeCloud IQ - Site Engine And ExtremeAnalytics Licensing

If you are an existing Extreme Management Center customer, contact your representative to have your Extreme Management Center license migrated to an ExtremeCloud IQ - Site Engine license. The ExtremeCloud IQ - Site Engine license also includes licensing for ExtremeAnalytics.

NOTES: • ExtremeCloud IQ - Site Engine is a subscription-based -only licensing model.

• ExtremeCloud IQ - Site Engine is not compatible with ExtremeCloud IQ Connect level account. Either the Pilot or Navigator level is mandatory.

You can view ExtremeCloud IQ and ExtremeCloud IQ - Site Engine license information by accessing Administration > Licenses.

There are three tiers of licenses for ExtremeCloud IQ - Site Engine and devices:

- Pilot Extreme devices
- Navigator 3rd party devices
- No License Status-Only devices

As you begin to <u>onboard ExtremeCloud IQ - Site Engine</u> and your devices, ExtremeCloud IQ will determine if you meet or exceed the <u>license limits</u> for each license type.

NOTE: Devices that do not have serial numbers or MAC addresses in Extreme Management Center must be Rediscovered after you upgrade to ExtremeCloud IQ - Site Engine before they can be onboarded to ExtremeCloud IQ.

> For the first 90 days after ExtremeCloud IQ - Site Engine is released, license usage will not be enforced for devices onboarded to ExtremeCloud IQ. When ExtremeCloud IQ starts evaluating license usage, if your number of devices exceeds your licenses available, ExtremeCloud IQ - Site Engine transitions to a license violation state and your access to ExtremeCloud IQ - Site Engine features and functionality is locked. To resolve the license shortage you need to access the Extreme Networks portal or ExtremeCloud IQ to evaluate the quantities of available Pilot and Navigator licenses versus the number of licenses required by ExtremeCloud IQ - Site Engine.

Licensing for Devices

When ExtremeCloud IQ - Site Engine has been <u>onboarded</u>, it starts sending requests to add the devices from its database to ExtremeCloud IQ.

As devices are added and discovered in ExtremeCloud IQ - Site Engine, they are onboarded to ExtremeCloud IQ, with a request for a license of the appropriate tier (Navigator, Pilot or No License) that each device will require.

Devices can be marked as <u>Unmanaged</u> in ExtremeCloud IQ, which means they are not using a license and available features are very limited.

The following grid details the type of license required by each device and engine type:

Device Type	License Tier Type	Number of Licenses Per Device
Extreme-supported Device (Includes VOSS/Fabric Engine, SLX, Extreme Access, VDX, Fabric Manager, Unified Switching VOSS/Fabric Engine, Unified Switching EXOS/Switch Engine, Summit Series, ERS Series, 200 Series, 700 Series, A Series, B Series, C Series, ICX Series, Security Appliances, MLXe Series)	Pilot	1
Chassis	Pilot	1
ExtremeControlengine	Pilot	1
ExtremeAnalyticsengine	Pilot	1

ExtremeCloud IQ - Site Engine	Pilot	1
Extreme Management Center	Pilot	1
vSensor	Pilot	1
All Other Devices (Includes Non-Extreme Device)	Navigator	1
Devices with Ping-Only profile	No License	0
Devices Added with No Access Profile	No License (These are not onboarded to ExtremeCloud IQ)	0
Status-Only Devices	No License (These are not onboarded to ExtremeCloud IQ)	0

For HiveOS APs, a Pilot license is required, but currently not enforced in ExtremeCloud IQ - Site

NOTE: Engine Version 21.04.10. These are not onboarded to ExtremeCloud IQ through ExtremeCloud IQ - Site Engine.

License Limits and Violations

For each request to add a device to ExtremeCloud IQ - Site Engine, ExtremeCloud IQ determines if there are enough licenses of that type available.

As a result, one of the following actions happens:

- If there are enough licenses, device onboarding is successful.
- If there are not enough Navigator licenses, a Pilot license is used instead.
- If there are not enough Pilot licenses, the request is considered a license violation.

To correct a license limit violation, you must acquire more licenses (and, when the updated license is sent to ExtremeCloud IQ, it is used by ExtremeCloud IQ - Site Engine).

Devices Marked as Unmanaged

When devices are marked as Unmanaged in ExtremeCloud IQ, they are also Unmanaged in ExtremeCloud IQ - Site Engine.

Onboarded Unmanaged devices are indicated in the <u>XIQ Onboarded column</u> of the **Network >** Site > Device table by a red X.

are Archives Configuration Tem	plates Reports								
Devices ecconfig Site Summ	ary Endpoint Location	s FlexReports							
🗢 Add Device 🗋 Expertite CEV 🗮 👘 🖓								Π. α	
Pol Details	Device Type	Family	Firmware	flaterence	Connector	XIQ Onboarded	Upda	Archived	Config Changed
Up: 326 Down: 0	X#50-02-240-04	Summit Seri	\$1.1.1.5			×.			
Up: 196 Down: 0	V#3860/05	Summit Seri	30.4.0.483			20Q1	Ummanages		
Configuration staged for device.	vm386D105	Summit Seri	31.1.1.3		3.6.1.8	_		-	
Up 2 Down 162	2435-247-45	Summit Seri.	31.1.1.3	*	3.6.1.8			*	
Up: 2 Down: 162	2435-247-45	Summit Seri	21.1.1.3	*	3.6.1.8			*	
Up 0 Down: 198	Virtual Application A.	Extension	8.5.3.45						
Up: 0 Down: 196	Virtual Access Contr	Extreme Co	8.5.5.12						
Up: 2 Down: 162	PABRICIUSR	Fabric Man	1.5.3.25		3.6.1.6				
	S S LO LI	terr 1 61	Backmark						Construint 1 - 8 of 8
a class [] out		9 mm 64							Cobadia
									9

For more details on the Network > Site > Device table, visit Onboarding Unmanaged Devices.

Logging into ExtremeCloud IQ - Site Engine

Configuring the ExtremeAnalytics Engine

To configure the virtual engine to run the ExtremeAnalytics application:

1. In the **Console** tab of the vSphere client, login as root with no password, and then press **[Enter]**. **The following screen displays.**

```
_____
Extreme Networks, Inc. - Application Analytics Engine -
Welcome to the Application Analytics Engine 21.4.10.xx 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 displays:

Root Password Configuration There is currently no password set in the system administrator account (root). It is recommended that you set one that isactive the first time the machine is rebooted. Would you like to set a root password (y/n) [y]?

Note: You must set a new root password. This new root password will be used by the initial user when logging in to the ExtremeAnalytics application.

3. Press [Enter] to set a new root password.The following text displays where you can enter the new password:

Enter new UNIX password: Retype new UNIX password:

 From the ExtremeAnalytics Appliance (Engine) Deployment Modes screen, select the deployment mode that matches your network environment.

The default deployment mode is 2.

ExtremeAnalytics Appliance Deployment Modes

```
This appliance supports multiple deployment modes to suit different
network environments and connectivity characteristics. Please select a
deployment mode below that best fits your requirements.
```

0. Single Interface

A single interface is used for both management and monitoring traffic.

Suitable for feeds from XOS/VOSS/SLX switches.

1. Single Interface With Tunnel

A single interface is used for both management and monitoring traffic.

A GRE Tunnel will be configured for traffic monitoring. Suitable for feeds from Coreflow switches.

2. Interface Mirrored Separate interfaces are configured for management and monitoring

traffic.
The monitoring interface will put into tap mode for traffic
monitoring.
Suitable for feeds from XOS/VOSS/SLX switches.
3. Interface Tunnel Mirrored
Separate interfaces are configured for management and monitoring
traffic.
The monitoring interface will get its own IP Address and GRE Tunnels
will be configured for traffic monitoring.
Suitable for feeds from Coreflow switches.
4. Manual Mode
The interface and tunneling configurations will not be modified by
this script, leaving them to be manually edited by the user instead.
Please select a deployment mode [2]:

Note: If you select deployment mode 4, refer to the *ExtremeAnalytics Deployment Guide* for information on how to configure your deployment manually.

5. If you selected deployment mode 1, 2, or 3, the Appliance (Engine) Network Configuration for ethO screen displays. For each line, enter the requested configuration information and press [Enter]. If you will be using DNS, the IP address of the name server should be provided. If you are using a name server then you must enter a domain name for the engine. The NIS server is used to authenticate users logging into the engine. If you are using an NIS server, make sure the NIS domain name is valid or users might not be able to log in to the ExtremeCloud IQ - Site Engine applications.

```
ExtremeAnalytics Appliance Network Configuration for eth0
Enter information below to configure eth0
Enter the hostname for the appliance (Required):
Enter the IP address for eth0 on 10.54.56.141 [10.54.56.141]:
Enter the IP netmask [255.255.255.0]:
Enter the gateway address [10.54.56.2]:
Enter the IP address of the name server (Optional):
Enter the domain name for 10.54.56.141 (Optional):
```

Enable NIS (y/n) [n]?

6. Continue as follows:

For deployment mode 1, go to step 10. For deployment mode 2, go to step 7. For deployment mode 3, go to step 9. 7. If you are using a VMware server, proceed to Step 8. If you are using a Hyper-V server, you need to change the configuration on the Windows Server system to promiscuous mode by running the set_promiscuous.ps1 script, included in the ZIP file containing the virtual engine. When the files are extracted, the script is saved in the directory to which you extracted the engine. The script enables the ExtremeAnalytics sensor to see all traffic coming into the interface.

From an Administrator PowerShell on the Windows Server system, enter the following command to run the script:

.\set_promiscuous.ps1 VM Nameeth1
VM Name - The name of the virtual machine as reported by Get-VM
eth1 - The default interface. This entry is optional.

8. On the ExtremeAnalytics Engine, specify one or more tap ports. For each line, enter the requested configuration information and press **[Enter]**.



Go to step 11.

9. Specify one or more GRE tunnel interfaces. For each line, enter the requested configuration information and press [Enter].

```
_____
ExtremeAnalytics Appliance Network Configuration for Tunnel Interfaces
_____
Enter the interface name for Tunnel Configuration [eth1]: eth4
Enter information below to configure eth4
Enter the IP address for eth4 on pv88 [10.54.211.116]:
Enter the IP netmask [255.255.255.0]:
Enter the gateway address [10.54.211.1]:
Would you like to add another interface for Tunnel Configuration (y/n)
[n]? y
Enter the interface name for Tunnel Configuration [eth1]: eth5
Enter information below to configure eth5
Enter the IP address for eth5 on pv88 [10.54.222.117]:
Enter the IP netmask [255.255.255.0]:
Enter the gateway address [10.54.222.1]:
Would you like to add another interface for Tunnel Configuration (y/n)
```

[n]? n

10. Enter the IP addresses for one or more GRE tunnels. For each line, enter the requested configuration information and press [Enter]

ExtremeAnalytics Appliance GRE Configuration
Remote mirroring can be configured in Coreflow Switches using GRE
tunnels.
This requires a specific mirroring configuration enabled on the switches.
Enter the SRC IP address for the GRE Tunnel [10.54.211.116]:
Enter the DST IP address for the GRE Tunnel [192.168.1.1]: 10.54.1.116
Add another GRE Tunnel (y/n) [n]? y
Enter the SRC IP address for the GRE Tunnel [10.54.222.117]:
Enter the DST IP address for the GRE Tunnel [192.168.1.1]: 10.54.2.117
Add another GRE Tunnel (y/n) [n]? n

11. A screen displays asking you to confirm your network setting. Enter 0 to accept the settings.

The following example shows the Confirm Network Settings screen for **deployment mode 2**.

```
______
Confirm Network Settings
_____
These are the settings you have entered. Enter 0 or any key other than a
valid selection to continue. If you need to make a change, enter the
appropriate number now or run the /usr/postinstall/dnetconfig script at a
later time.
_____
0. Accept settings and continue
1. Hostname: pv88
2. Deployment Mode:
                                    Dual Interface Mirrored
3. Management Interface Configuration (eth0):
     Address: 10.54.184.88
     Netmask: 255.255.255.0
     Gateway: 10.54.184.1
     Nameserver: 10.54.188.120
     Domain name: nac2003.com
4. NIS Server/Domain: Not Configured
5. Monitor Interface Configuration:
     Tap Mode Interfaces: eth4, eth5
```

The following example shows the Confirm Network Settings screen for **deployment mode 3**.

Confirm Network Settings								
These are the settings you have entered. Enter 0 or any key other than a								
valid selection to continue. If you need to make a change, enter the								
appropriate number now or run the /usr/postinstall/dnetconfig script at a								
later time.								
0 Accent settings and continue								
1 Hostname: pv88								
2. Deployment Mode: Dual Interface Tunnel Mirrored								
3. Management Interface Configuration (eth0):								
Address: 10.54.184.88								
Netmask: 255.255.255.0								
Gateway: 10.54.184.1								
Nameserver: 10.54.188.120								
Domain name: nac2003.com								
4. NIS Server/Domain: Not Configured								
5. Mirror Interface Configuration:								
Name: eth4								
Address: 10.54.211.116								
Netmask: 255.255.0								
Gateway: 10.54.211.1								
Name: eth5								
Address: 10.54.222.117								
Netmask: 255.255.0								
Gateway: 10.54.222.1								
6. GRE tunnels: 10.54.211.116/10.54.1.116								
10.54.222.11//10.54.2.11/								

12. The SNMP Configuration screen displays. For each line, enter the requested information 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 ExtremeCloud IQ	1
- Site Engine Console.	
Please enter the SNMP user name [snmpuser]:	

Please enter the SNMP authentication protocol - MD5 or SHA [MD5]: Please enter the SNMP authentication credential [snmpauthcred]: Please enter the SNMP privacy protocol - DES or AES [DES]: Please enter the SNMP privacy credential [snmpprivcred]:

13. A summary screen displays asking you to accept your SNMP Configuration settings. Enter **0** to accept the settings.

SNMP Configuration
These are the current SNMP V3 settings. To accept them and complete SNMP
configuration, enter 0 or any key other than the selection choices.
If you need to make a change, enter the appropriate number now or run the
/usr/postinstall/snmpconfig script at a later time.
0. Accept the current settings
1. SNMP User: snmpv3user
2. SNMP Authentication Protocol: SHA
3. SNMP Authentication: shaauthpassword
4. SNMP Privacy Protocol: AES
5. SNMP Privacy: aesprivpassword
6. Modify all settings
Enter selection [0]: 0

14. The Configure Date and Time Settings screen displays where you are asked if 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 16.

Note that your VMS server should be using the same NTP settings as those configured for your virtual engine (i.e., the same settings as the VMs that are hosted on the VMS server).

```
Configure Date And Time Settings

The appliance 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
```

15. The NTP validate selection screen displays. Enter **O** to accept the current settings and proceed to the Set Time Zone screen at step 17.

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

16. If you answered no to using an NTP server to set date and time, the following manual set date and time screen displays.

```
_____
Set Date And Time
_____
The current system date and time is: Thu 14 Nov 2018 04:34:08 PM EST
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
   - 2 digit minute of hour
mm
ss - 2 digit seconds
_____
Please enter the month [11]:
Please enter the day of the month [14]:
Please enter the year [2018]:
Please enter the hour of day [04]:
Please enter the minutes [34]:
Please enter the seconds [08]:
```

17. Enter **n** at the Use UTC screen.

				=====											
Use	UTC														
				=====							====		-		
The	syste	em c	lock	can b	e set	to u	ise	UTC.	Speci	ifying	no	for	using	UTC,	sets
the	hardw	vare	cloc	k usi	ng loo	calti	.me	•							
													-		
Do	you wa	ant	to us	e UTC	(y/n)	[n]	?								

18. The Set Time Zone screen displays. 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]:

19. The **Modify Settings** screen displays. This screen summarizes the settings you have entered and provides an opportunity to modify the settings, if desired. Enter **0** to accept the settings.

Modify Settings
All of the information needed to complete the installation of the
ExtremeAnalytics Appliance has been entered. 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 settings and continue
1. Set the root user password
2. Set the host and network settings
3. Set SNMP settings
4. Set the system time
5. Modify all settings

Enter selection [0]:

The ExtremeAnalytics application software is automatically installed. This could take a few minutes. When the installation is complete, you'll see the following screen.

```
Extreme Networks - ExtremeAnalytics Appliance - Setup Complete
Setup of the ExtremeAnalytics Appliance is now complete.
The appliance is now operational and ready to accept remote connections.
Details of the installation are located in the /var/log/install
directory.
```

Note: After you have completed the configuration, it is important to take a snapshot of your engine configuration to be used in the event an engine image reinstall is required. For instructions on how to take a snapshot, see your vSphere client documentation.

Launching the ExtremeAnalytics Application

Now that you have configured the ExtremeAnalytics appliance, you are ready to access the ExtremeCloud IQ - Site Engine Launch Page and run ExtremeAnalytics from a remote client machine.

- Open a browser window on the remote client machine and enter the ExtremeCloud IQ Site Engine Launch page URL in the following format: http://<servername>:8080/.
 where <servername> is the ExtremeCloud IQ - Site Engine server IP address or hostname, and 8080 is the required port number. For example: http://10.20.30.40:8080/.
- On the ExtremeCloud IQ Site Engine Launch Page, select OneView.
 Note: The first time you attempt to launch an ExtremeCloud IQ Site Engine application, you will be prompted for the license text you received when you generated your ExtremeCloud IQ Site Engine product license.
- 3. At the login window, enter your ExtremeCloud IQ Site Engine user name and password.
- 4. On the ExtremeCloud IQ Site Engine screen, select Analytics at the top of the screen.
- Select Dashboard.
 The <u>Dashboard tab</u> displays.

Adding the ExtremeAnalytics Engine

To add the ExtremeAnalytics engine to ExtremeAnalytics:

- 1. Select the Analytics Configuration tab Analytics Configuration tab
- 2. Open the drop-down list below Overview and select Add Engine.
- 3. Enter the following information:
 - IP address of the ethO interface
 - Name of the ExtremeAnalytics engine
- 4. From the **Profile** list, select the appropriate <u>SNMP profile</u>.
- 5. Select OK.
- 6. Open the drop-down list below Overview and select Enforce Engine.

Changing ExtremeAnalytics Engine Settings

Use these steps if you need to change your ExtremeAnalytics virtual engine settings following your initial engine configuration. Perform these steps in the vSphere client Console tab.

Changing Basic Network Configuration

To change basic network configuration settings such as hostname and engine IP address, enter the following command at the login prompt in the **Console** tab: /usr/postinstall/dnetconfig

This will start the network configuration script and enable you to make the required changes. You must reboot the engine for the new settings to take effect.

Changing SNMP Configuration

To change SNMP configuration settings such as SNMP Trap Community String, SNMP User, SNMP Authentication, and SNMP Privacy credentials, enter the following command at the login prompt in the **Console** tab: /usr/postinstall/snmpconfig

This will start the SNMP configuration script and enable you to make the required changes.

Changing Date and Time Settings

To enable or disable using NTP to configure the engine date and time, or to manually set the date and time on the engine, enter the following command at the login prompt in the **Console** tab:

/usr/postinstall/dateconfig

This will start the date and time configuration script and enable you to change the settings.

Changing the ExtremeAnalytics Server IP Address

To change the IP address of the ExtremeAnalytics server, enter the following command at the login prompt in the **Console** tab: /opt/appid/configMgmtIP <IP address>

Then, start using the new ExtremeAnalytics server by typing: appidctl restart.

Changing the Web Service Credentials

The Web Service credentials provide access to the ExtremeAnalytics Appliance Administration web page and the web services interface for the ExtremeAnalytics engine. Engines are shipped with a preconfigured default password.

If you have changed the credentials in the **Analytics** tab and then install a new engine that is using the default password, you will not be able to monitor or enforce to the new engine until you change the password on the engine using this command. The credentials you enter on the engine must match the credentials specified in the Web Credentials section in **Analytics > Configuration > Configuration**.

To change Web Service credentials, enter the following command at the login prompt in the **Console** tab: /opt/appid/configWebCredentials <username> <password>

Then, restart the engine by typing: appidctl restart

Upgrading ExtremeAnalytics Engine Software

Upgrades to the ExtremeCloud IQ - Site Engine engine software will be made available from the Network Management Suite (NMS) Download webpage.

Prior to performing an upgrade, you can create a snapshot of the engine that you can revert to in the event an upgrade fails. Refer to the vSphere client documentation for instructions on creating a snapshot.

- 1. On a system with an Internet connection, go to the Network Management Suite (NMS) Download web page: <u>http://extranet.extremenetworks.com/downloads/pages/NMS.aspx</u>.
- 2. After entering your email address (username) and password, follow this path to the download page: Visibility & Control > Network Management Suite (NMS) > Software > select a version.
- 3. Download the following ExtremeAnalytics virtual engine file from the NMS Downloads section:

purview_appliance_upgrade_to_<version>.bin

- 4. Use FTP, SCP, or a shared mount point, to copy the file to the ExtremeAnalytics virtual engine.
- 5. SSH to the engine.
- 6. Cd to the directory where you downloaded the files.

7. Change the permissions on the upgrade file by entering the following command:

chmod 777 purview_appliance_upgrade_to_<version>.bin

8. Run the install program by entering the following command:

./purview_appliance_upgrade_to_<version>.bin

The upgrade automatically begins. You are notified when the upgrade completes.

Reinstalling ExtremeAnalytics Engine Software

In the event that a software reinstall becomes necessary, it is recommended that you restore an engine snapshot that you previously made using the vSphere client. Refer to the vSphere client documentation for instructions on restoring a snapshot.

If you do not have an engine snapshot to restore, you will need to re-deploy and reconfigure the ExtremeAnalytics virtual engine following the instructions in <u>Engine Deployment</u> and this section.

Note: The re-installation procedure reformats the hard drive, reinstalls all the ExtremeAnalytics engine software, the operating system, and all related Linux packages.