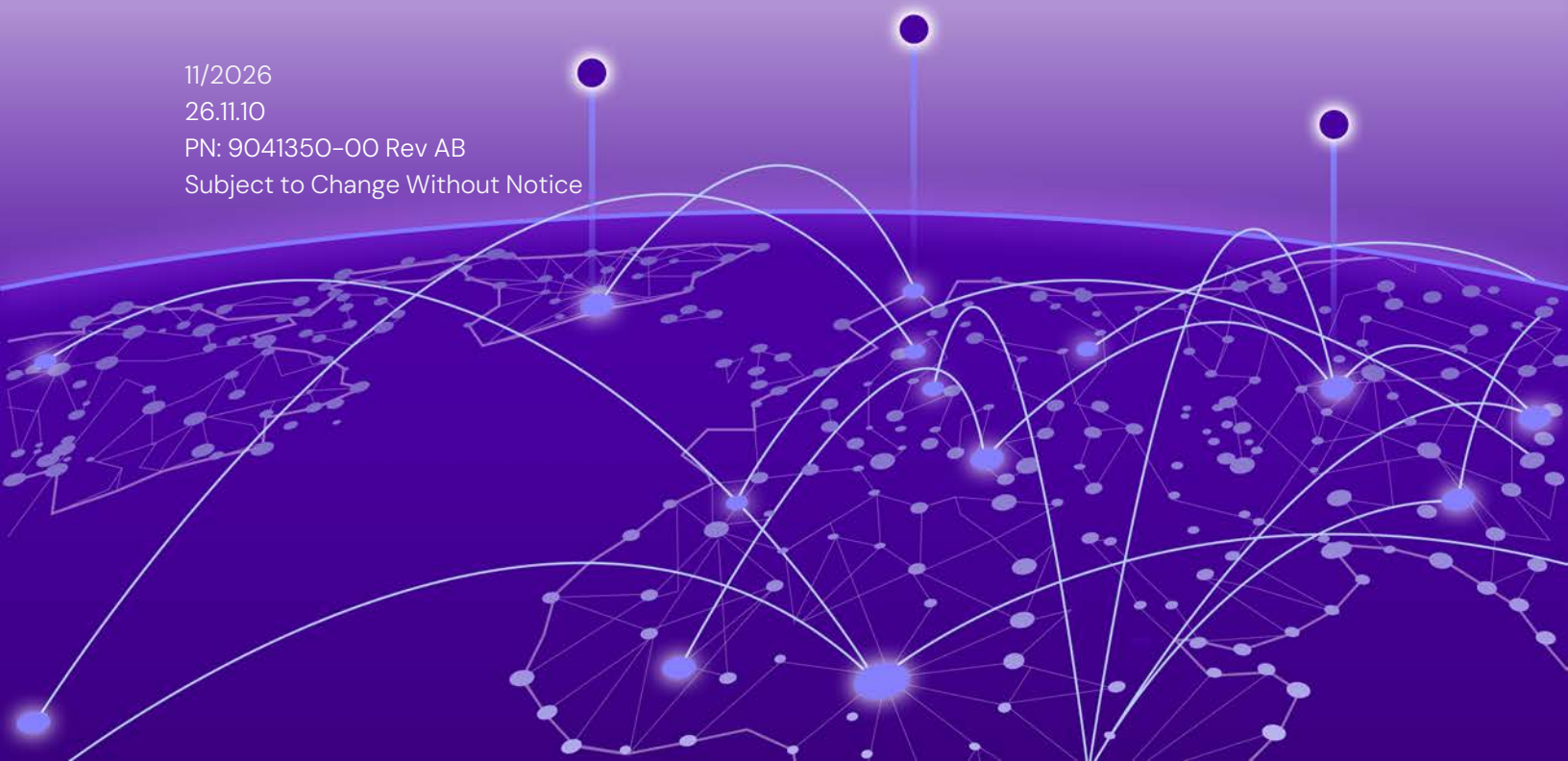
ExtremeCloud™ IQ Site Engine v26.11.10 Virtual Engine Installation Guide:

Deployment, Configuration, and Management for ExtremeCloud IQ Site Engine, ExtremeControl and ExtremeAnalytics

11/2026
26.11.10
PN: 9041350-00 Rev AB
Subject to Change Without Notice



Abstract

This Virtual Engine Installation Guide provides detailed instructions for deploying and configuring the ExtremeCloud IQ Site Engine, Access Control, and ExtremeAnalytics virtual engines on VMware ESX/ESXi, Microsoft Hyper-V, Nutanix, and Extreme Networks Universal Compute Platform servers. The guide outlines system requirements, including network configuration, licensing, and initial setup tasks. This guide includes step-by-step procedures for deploying virtual engines, configuring network settings, SNMP, NTP, and managing engine-specific configurations for optimal performance. The 26.11.10 Release adds support for deploying and configuring Application Analytics Traffic Sensor on UCP-3150C. Additionally, this guide covers the process for upgrading and reinstalling the virtual engine software, as well as detailed troubleshooting tips to ensure a smooth deployment. This guide is intended for IT professionals with advanced knowledge in network management and virtualization.

Copyright © 2026 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:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- **GTAC Knowledge** — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- **The Hub** — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- **Support Portal** — Manage cases, downloads, service contracts, product licensing, and training and certifications.

Table of Contents

ExtremeCloud™ IQ Site Engine v26.11.10 Virtual Engine Installation Guide: 1

Deployment, Configuration, and Management for ExtremeCloud IQ Site Engine, ExtremeControl and ExtremeAnalytics 1

Abstract 2

Table of Contents 4

Engine Deployment 7

Deploying the Virtual Engine on a VMware ESX Server 7

Deployment Requirements 7

Deploying the Virtual Engine 7

Shutting Down the Engine 11

Deploying the Virtual Engine on a Hyper-V Server 11

Deployment Requirements 11

Deploying the Virtual Engine 11

Deploying the Virtual Engine on a Nutanix Server 16

Deployment Requirements 16

Deploying the Virtual Engine 17

Deploying the Virtual Engine on an Extreme Networks Universal Compute Platform Server 25

Deployment Requirements 25

Deploying the Virtual Engine 26

ExtremeCloud IQ Site Engine Engine Configuration 29

Pre-Configuration Tasks 29

Configuring the ExtremeCloud IQ Site Engine Engine 29

Launching ExtremeCloud IQ Site Engine 36

Onboarding ExtremeCloud IQ Site Engine to ExtremeCloud IQ 36

After Initial Installation of ExtremeCloud IQ Site Engine 36

Onboarding Devices 38

ExtremeCloud IQ Onboarded Status for Devices 38

Changing ExtremeCloud IQ Site Engine Engine Settings 40
Changing Basic Network Configuration 40
Changing SNMP Configuration 40
Changing Date and Time Settings 41
Upgrading ExtremeCloud IQ Site Engine Engine Software 41
Reinstalling ExtremeCloud IQ Site Engine Appliance Software 42
ExtremeControl Engine Configuration 43
Pre-Configuration Tasks 43
Configuring the ExtremeControl Engine 43
Changing ExtremeControl Engine Settings 49
Using the Access Control tab 49
Changing DNS, NTP, SSH, and SNMP Settings 49
Changing Hostname, Gateway, and Static Routes 49
Using the Console 50
Changing the ExtremeCloud IQ Site Engine Server IP Address 50
Changing Web Service Credentials 50
Changing the Engine IP Address and Basic Network Settings 50
Changing Date and Time Settings 51
Upgrading ExtremeControl Engine Software 51
Reinstalling ExtremeControl Engine Software 51
ExtremeAnalytics Engine Configuration 52
Pre-Configuration Tasks 52
Configuring the ExtremeAnalytics Engine 52
Launching the ExtremeAnalytics Application 61
Adding the Application Analytics Engine 62
Changing ExtremeAnalytics Engine Settings 62
Changing Basic Network Configuration 62
Changing SNMP Configuration 62
Changing Date and Time Settings 62
Changing the ExtremeAnalytics Server IP Address 63

Changing the Web Service Credentials 63
Upgrading ExtremeAnalytics Engine Software 63
Reinstalling ExtremeAnalytics Engine Software 64
Configuring the Application Analytics Traffic Sensor 64
Launching the ExtremeAnalytics Application 68
Adding the Application Analytics Traffic Sensor Engine 68
Changing Application Analytics Traffic Sensor Engine Settings 68
Changing Basic Network Configuration 69
Changing SNMP Configuration 69
Changing Date and Time Settings 69
Changing the Application Analytics Traffic Sensor Server IP Address 69
Changing the Web Service Credentials 69
Upgrading Application Analytics Traffic Sensor Engine Software 70
Reinstalling Application Analytics Traffic Sensor Engine Software 70

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® ESXi server, a Microsoft® Hyper-V server, a Nutanix server, or an Extreme Networks Universal Compute Platform.

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, 7.0, or 8.0 server using the web client.

For information about the different ExtremeCloud IQ Site Engine, ExtremeControl, and ExtremeAnalytics virtual engine configurations, and supported Operating System versions, 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:

   a. Access the Extreme Portal at: https://extreme-networks.my.site.com/ExtrLogin?startURL=%2FExtrDownloadLanding.

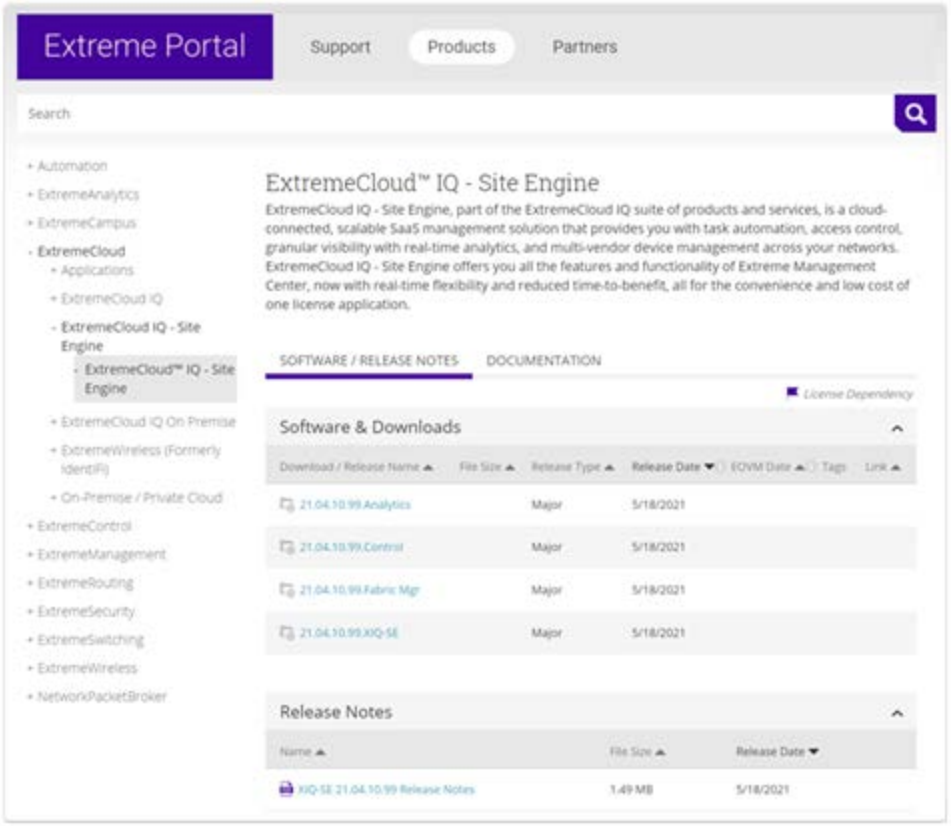
   b. Login with your email address and password.

   c. Select the **Products** tab and select ExtremeManagement.

   d. Select **ExtremeCloud IQ Site Engine** in the right-panel.

   e. Select a version.

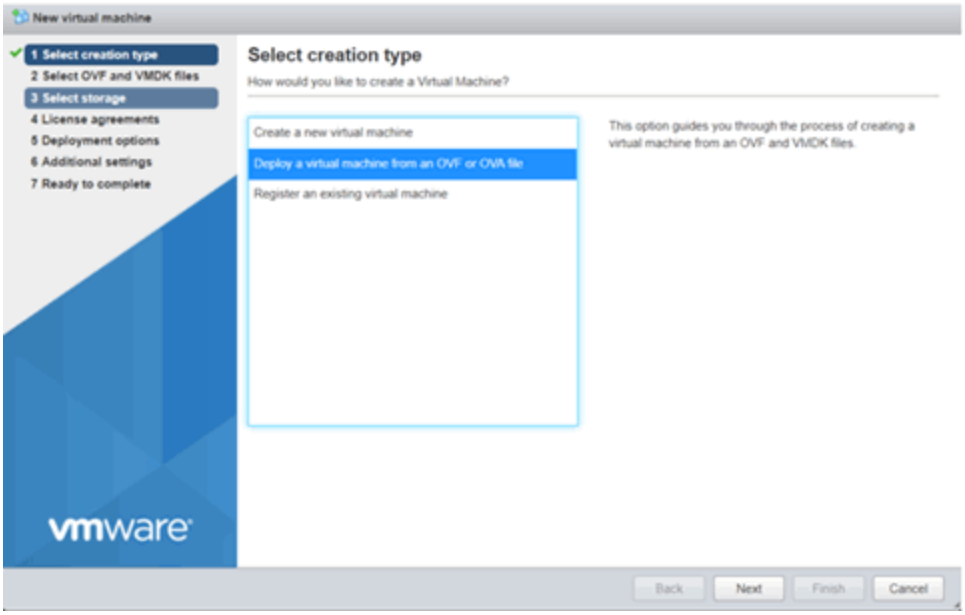
   f. Download the ExtremeCloud IQ Site Engine, ExtremeControl, or ExtremeAnalytics virtual engine (appliance) image from the appropriate section.



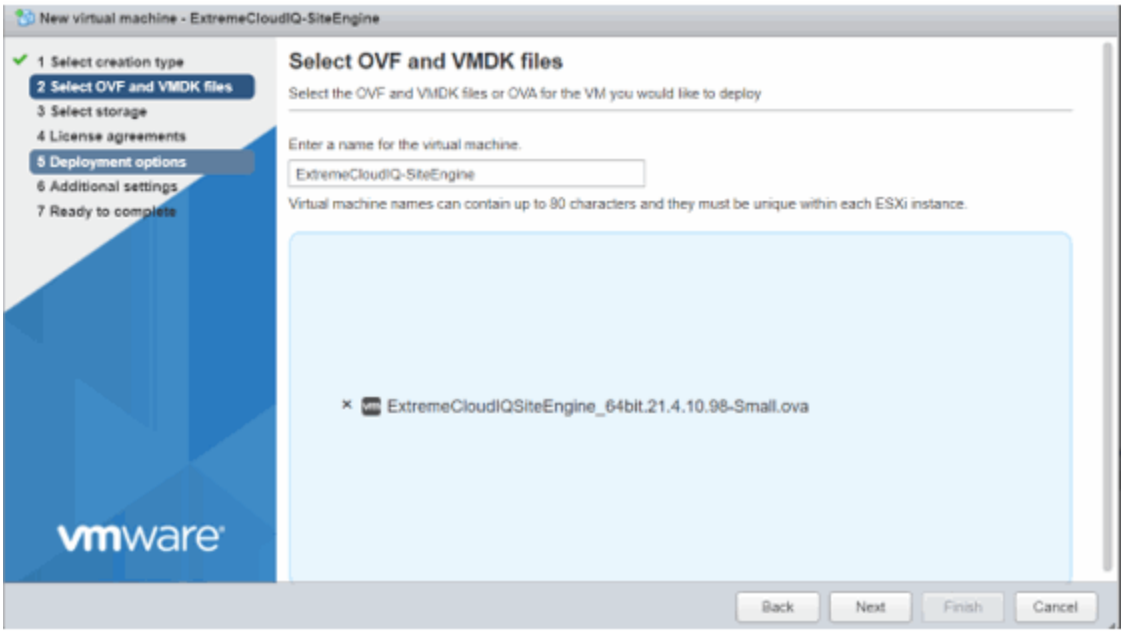
2. Open the VMWare software. From the **Host** menu, select **Create/Register VM.**



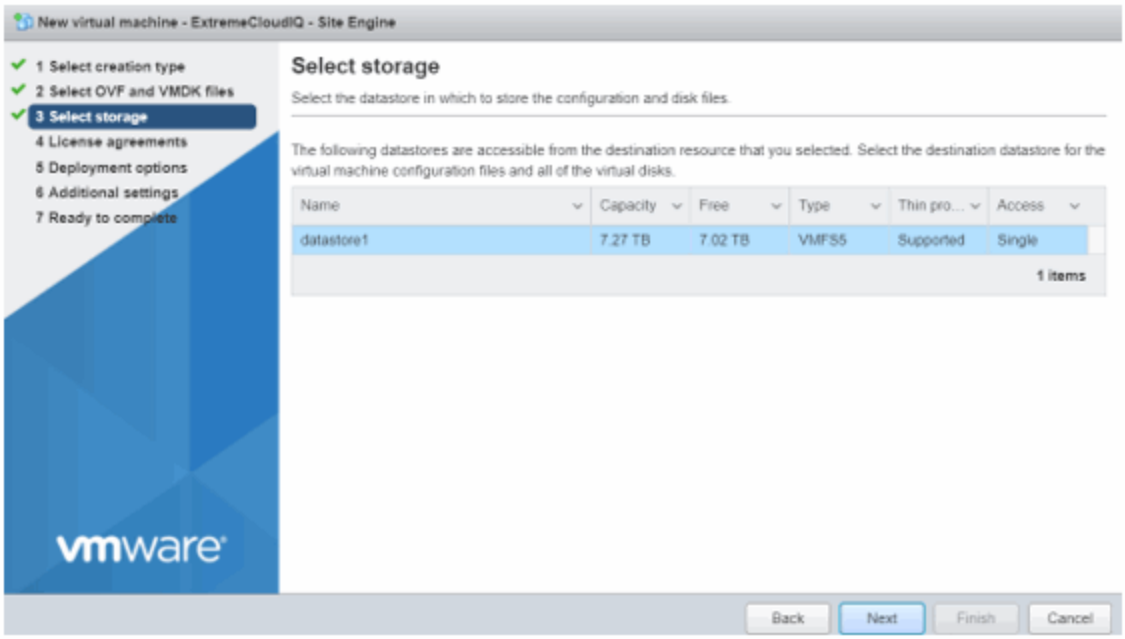
3. From the **Select creation type** panel, select **Deploy a virtual machine from an .OVF or .OVA file**. Select **Next**.



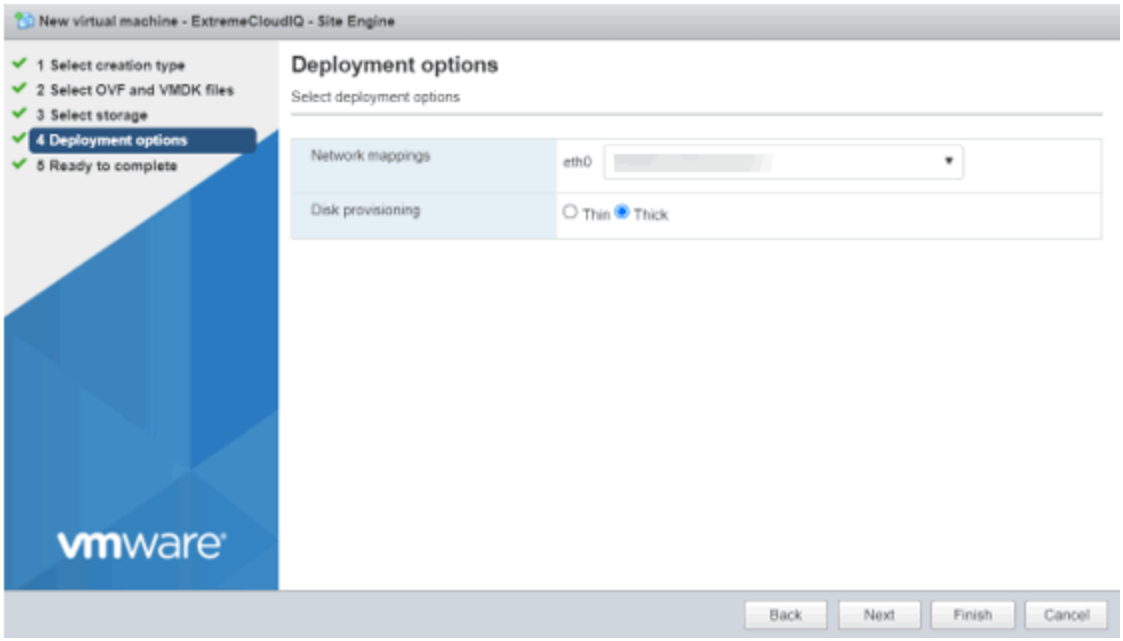
4. Enter the name of the virtual machine and select the .OVA file. Select **Next** to continue.



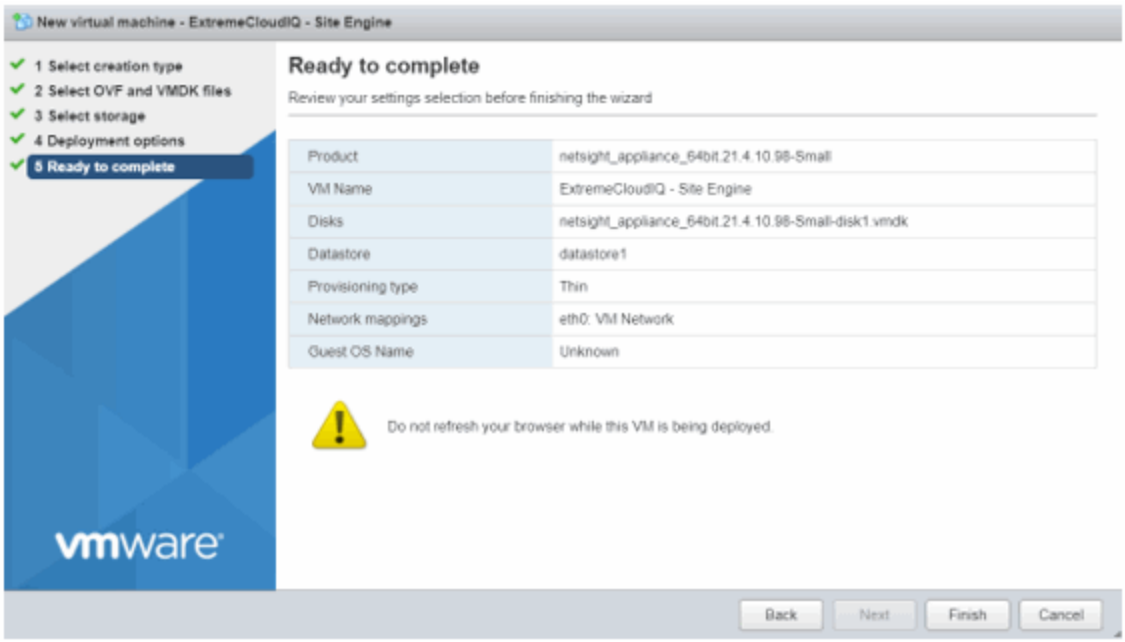
5. Select your datastore. Select **Next** to continue.



6. Select your deployment options and select **Next**.



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



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

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 Hyper-V server.

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

   To download an engine image:

   a. Access the Extreme Portal at: https://extreme-networks.my.site.com/ExtrLogin?startURL=%2FExtrDownloadLanding.

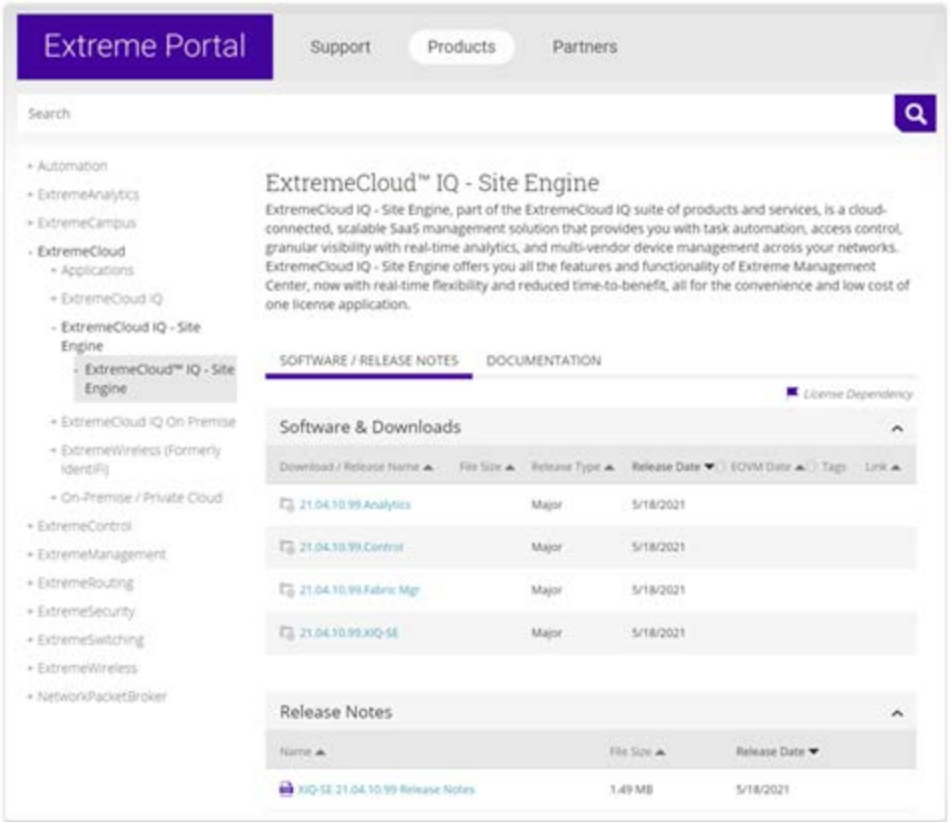
   b. Login with your email address and password.

   c. Select the **Products** tab and select ExtremeCloud IQ Site Engine.

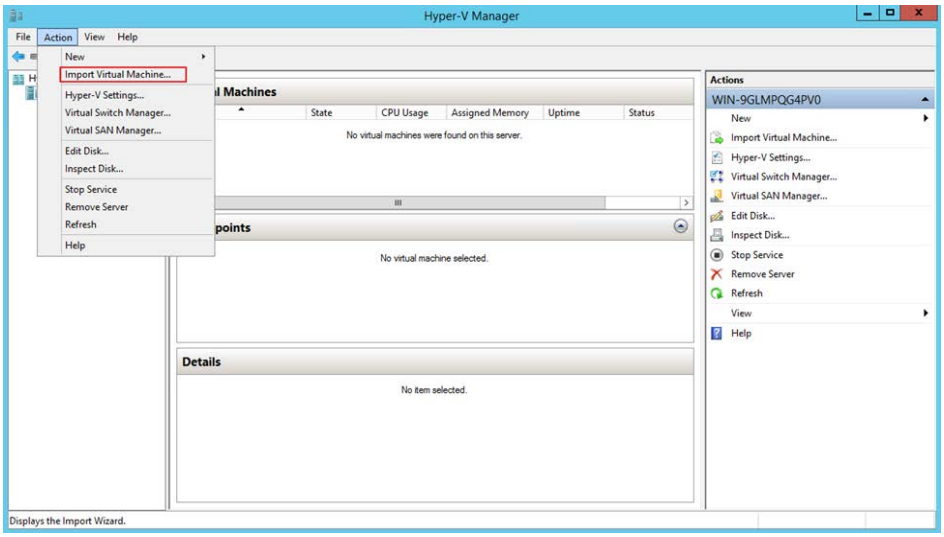
   d. Select **ExtremeCloud IQ Site Engine** in the right-panel.

   e. Select a version.

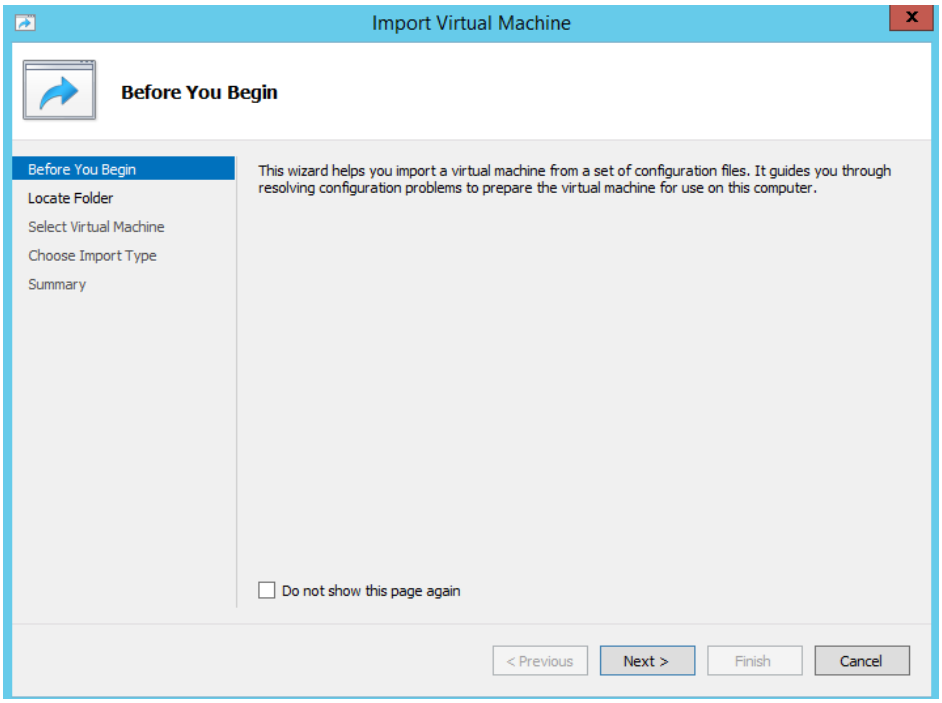
   f. Download the ExtremeCloud IQ Site Engine, ExtremeControl, or ExtremeAnalytics virtual engine (appliance) image from the appropriate section.



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**.

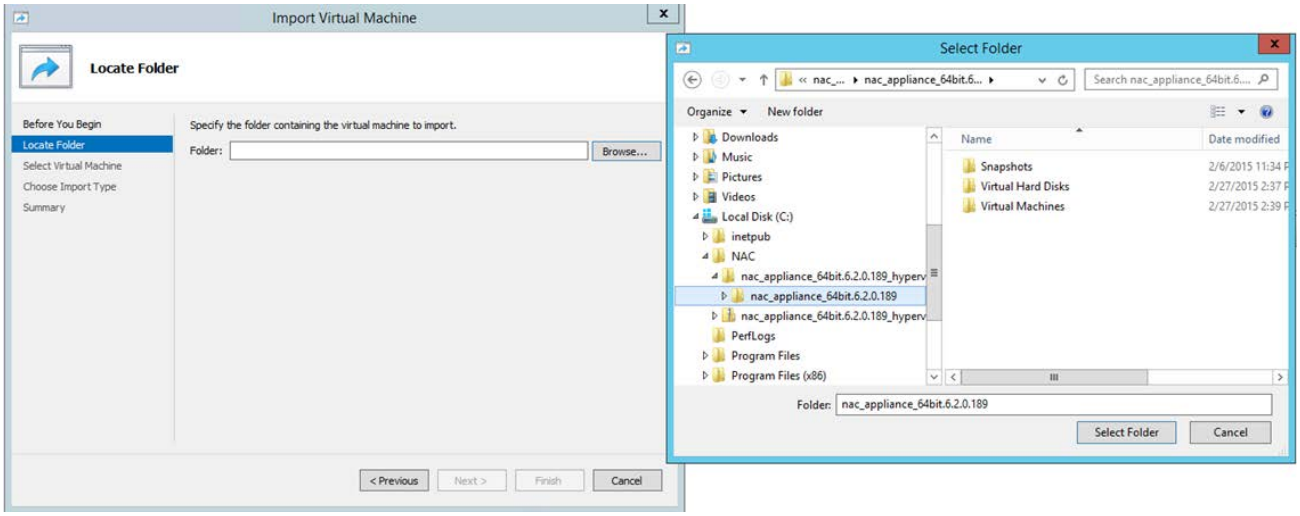


The **Import Virtual Machine** wizard opens to the Before You Begin panel.



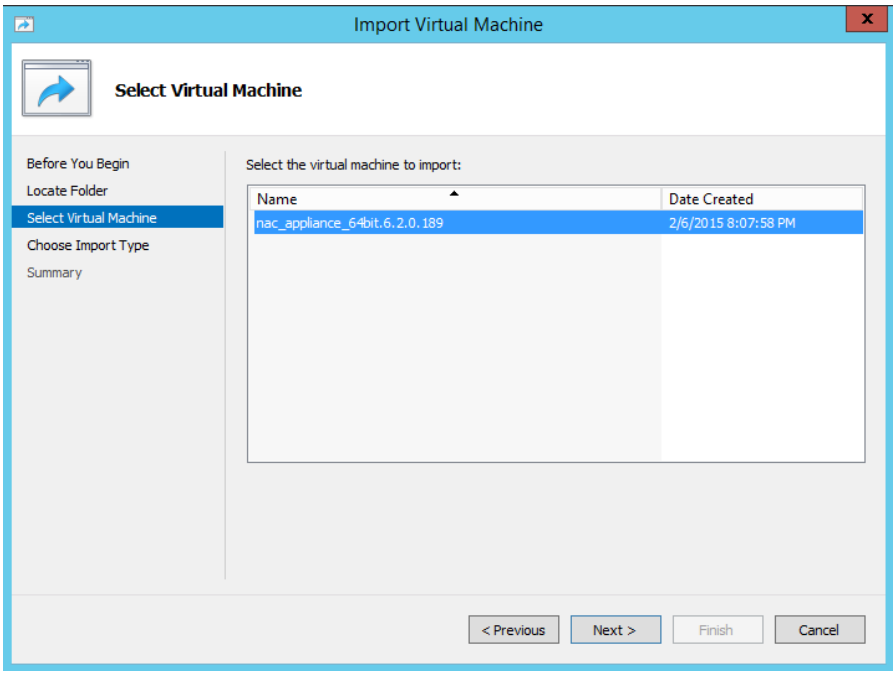
Select **Next**.

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**.

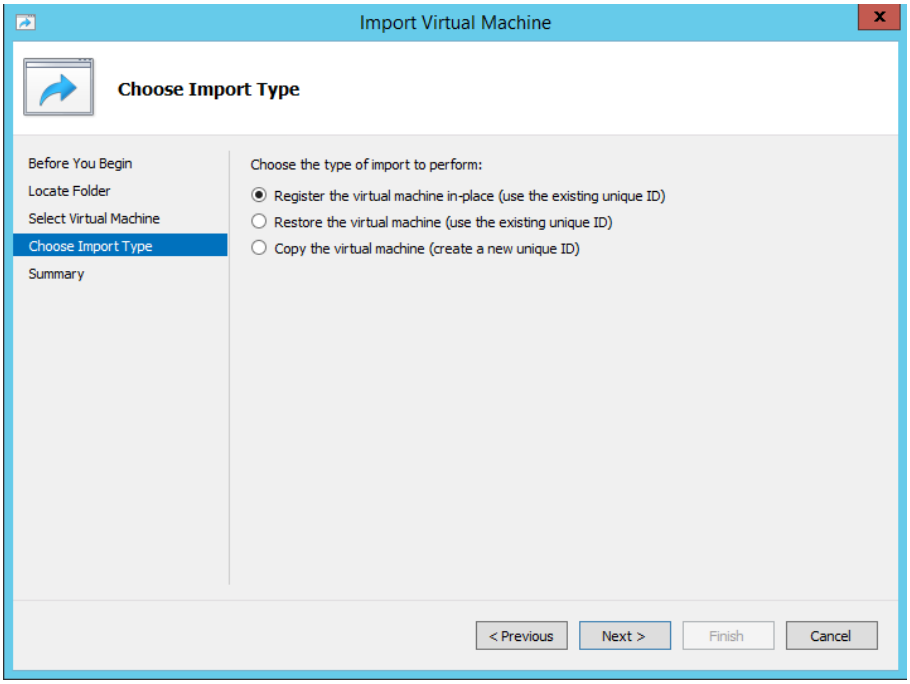


The Select Virtual Machine panel opens.

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

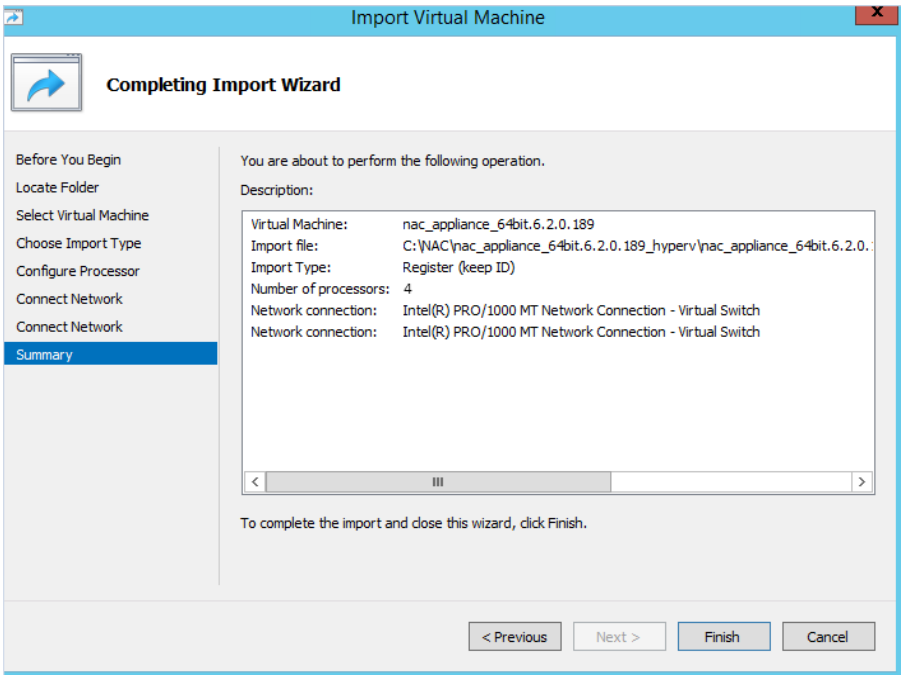


The Choose Import Type panel opens.



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.



You are now ready to begin configuring the engine.

- If you are configuring an ExtremeCloud IQ Site Engine virtual engine, see ExtremeCloud IQ Site 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 ExtremeAnalytics Engine Configuration.

Deploying the Virtual Engine on a Nutanix 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 enhanced with Nutanix extensions, and can be deployed on a Nutanix server with Prism Central.

For information about the different ExtremeCloud IQ Site Engine, ExtremeControl, and ExtremeAnalytics virtual engine configurations and supported Operating System versions, 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 Nutanix server.

1. Download the ExtremeCloud IQ Site Engine, ExtremeControl, or ExtremeAnalytics virtual engine software image to a local machine where Nutanix Prism Central is reachable.

   To download an engine image:

   a. Access the Extreme Portal at: https://extreme-networks.my.site.com/ExtrLogin?startURL=%2FExtrDownloadLanding.

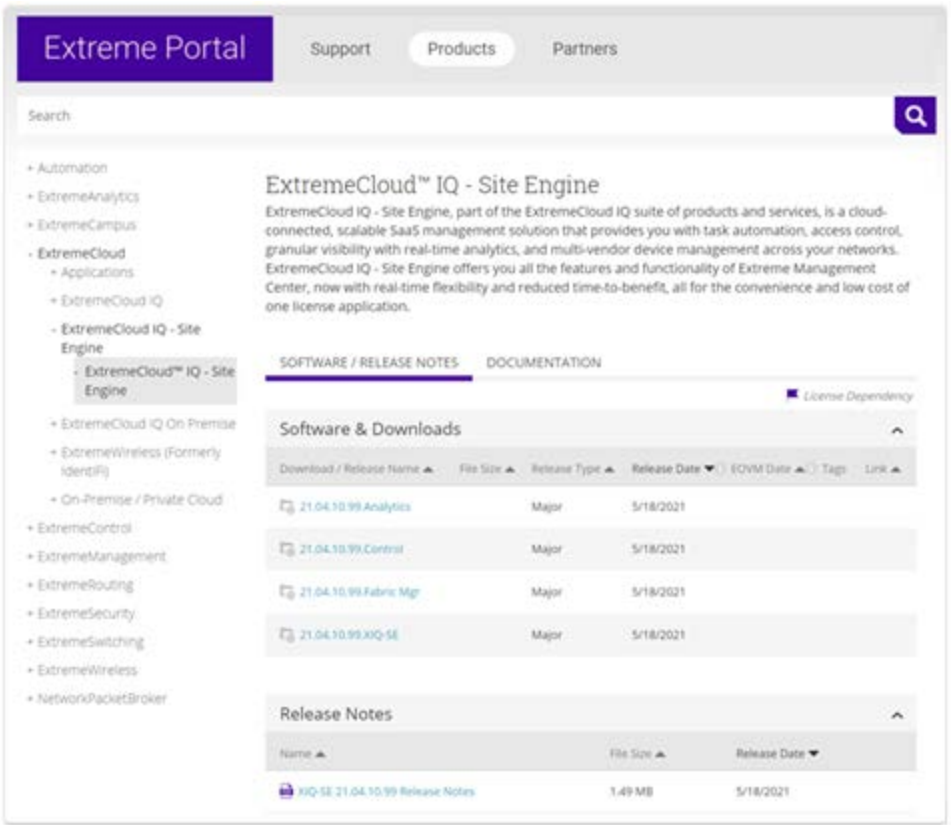
   b. Login with your email address and password.

   c. Select the **Products** tab and select ExtremeCloud IQ Site Engine.

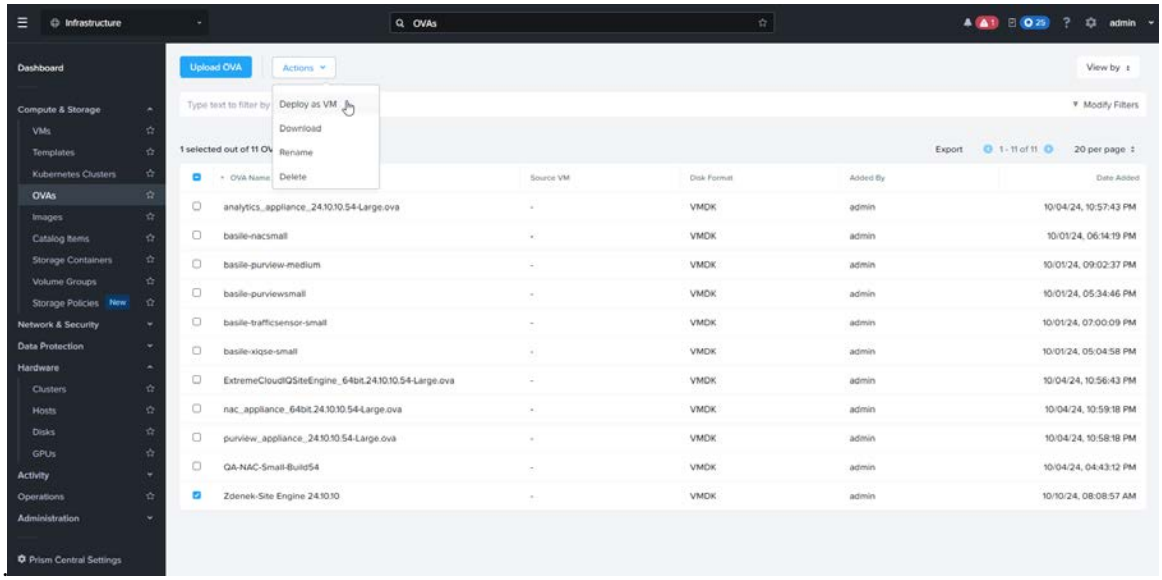
   d. Select **ExtremeCloud IQ Site Engine** in the right-panel.

   e. Select a version.

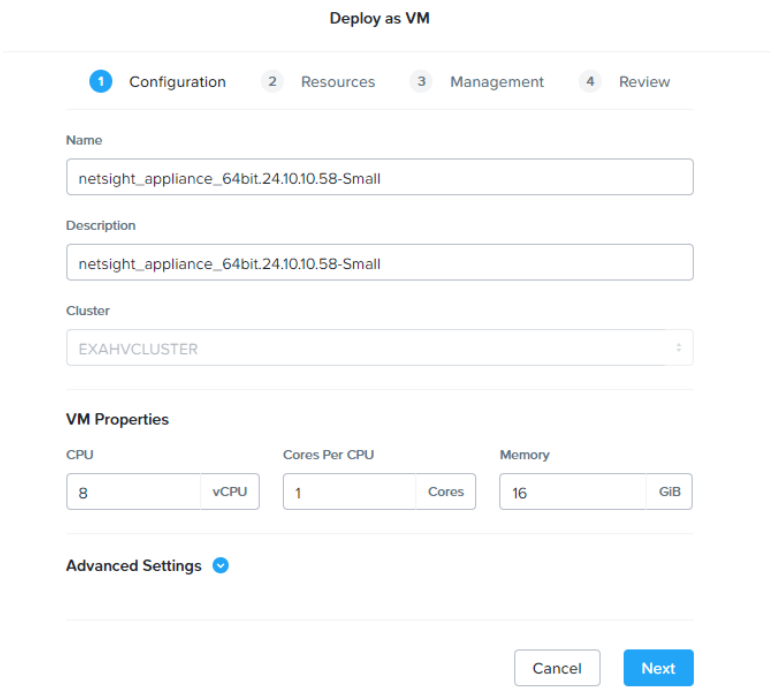
   f. Download the ExtremeCloud IQ Site Engine, ExtremeControl, or ExtremeAnalytics virtual engine (appliance) image from the appropriate section.



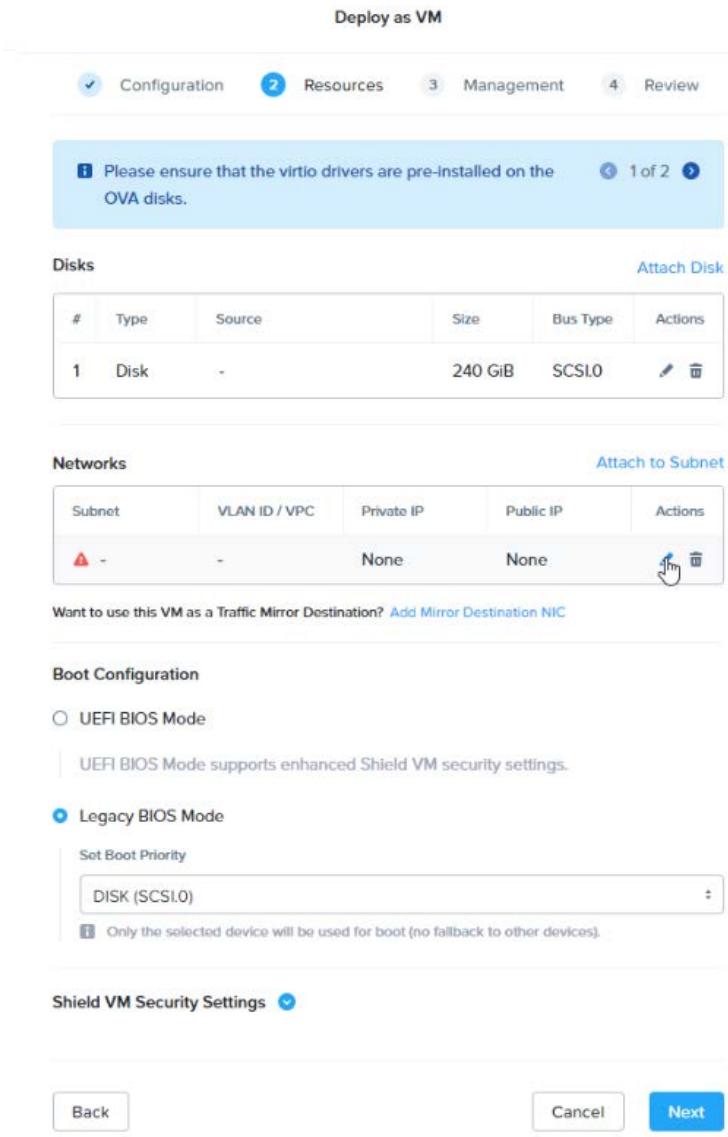
2. In a browser, connect to **Nutanix Prism Central** and navigate to **Infrastructure**.
3. Select the **Upload OVA** button.
4. Enter a **name**, select the **Select File** button, choose the downloaded virtual engine OVA file, and select **Upload**.
5. When the upload has completed, select **Close**. Wait for the validation process to complete.
6. In Prism Central select the uploaded OVA, then from the **Actions** menu select **Deploy as VM.**

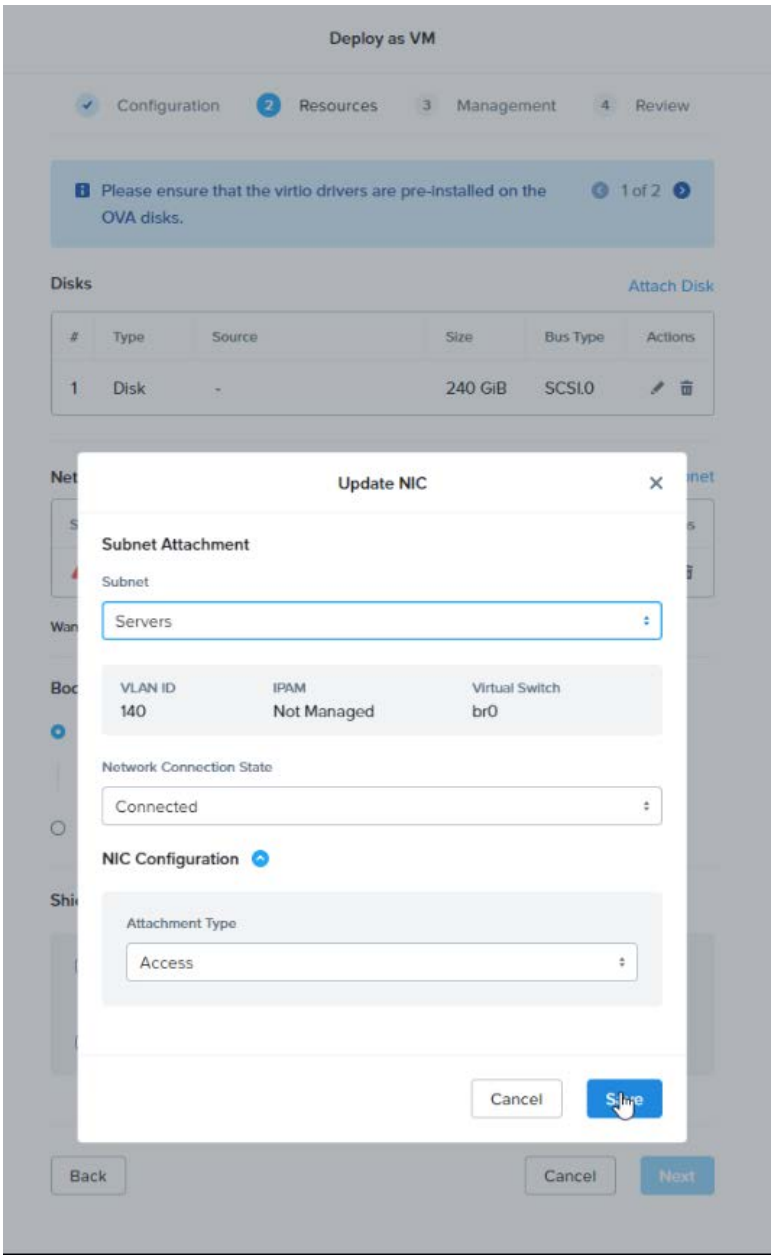


   a. In the **Configuration** tab, enter a **Name** and **Description**, and select **Next**. The best practice is to not change the default VM properties.

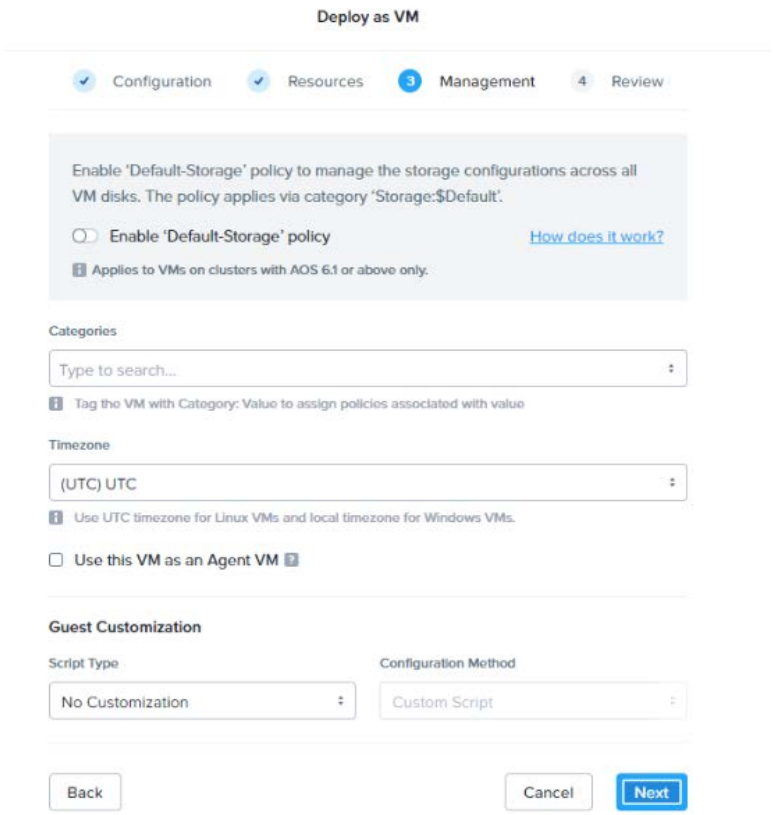


b. In the **Resources** tab, configure **Networks** by selecting the edit icon in the Actions column. Configure the network, then select **Save** and **Next**.

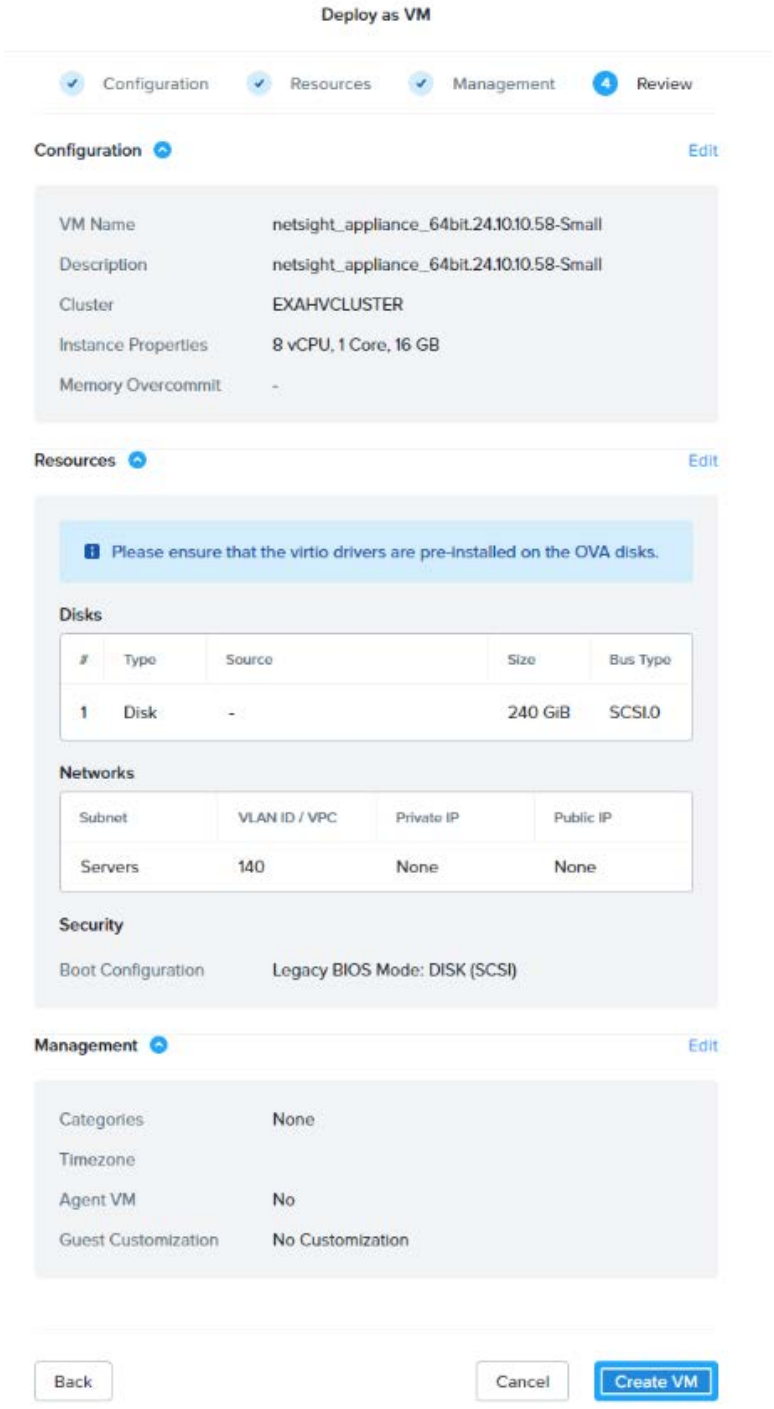

Deploy as VM
Configuration
2
Resources
3
Management
4
Review
Please ensure that the virtio drivers are pre-installed on the OVA disks.
1 of 2
Disks
Attach Disk
Type Source Size Bus Type Actions
1 Disk - 240 GiB SCSI.0
Networks
Attach to Subnet
Subnet VLAN ID / VPC Private IP Public IP Actions
- - None None
Want to use this VM as a Traffic Mirror Destination? Add Mirror Destination NIC
Boot Configuration
UEFI BIOS Mode
UEFI BIOS Mode supports enhanced Shield VM security settings.
Legacy BIOS Mode
Set Boot Priority
DISK (SCSI.0)
Only the selected device will be used for boot (no fallback to other devices).
Shield VM Security Settings
Back
Cancel
Next


Deploy as VM
Configuration
2
Resources
3
Management
4
Review
Please ensure that the virtio drivers are pre-installed on the OVA disks.
1 of 2
Disks
Attach Disk
#
Type
Source
Size
Bus Type
Actions
1
Disk
-
240 GiB
SCSI.0
Update NIC
Subnet Attachment
Subnet
Servers
VLAN ID
140
IPAM
Not Managed
Virtual Switch
br0
Network Connection State
Connected
NIC Configuration
Attachment Type
Access
Cancel
Save
Back
Cancel
Next

c. In the **Management** tab, select **Next**.

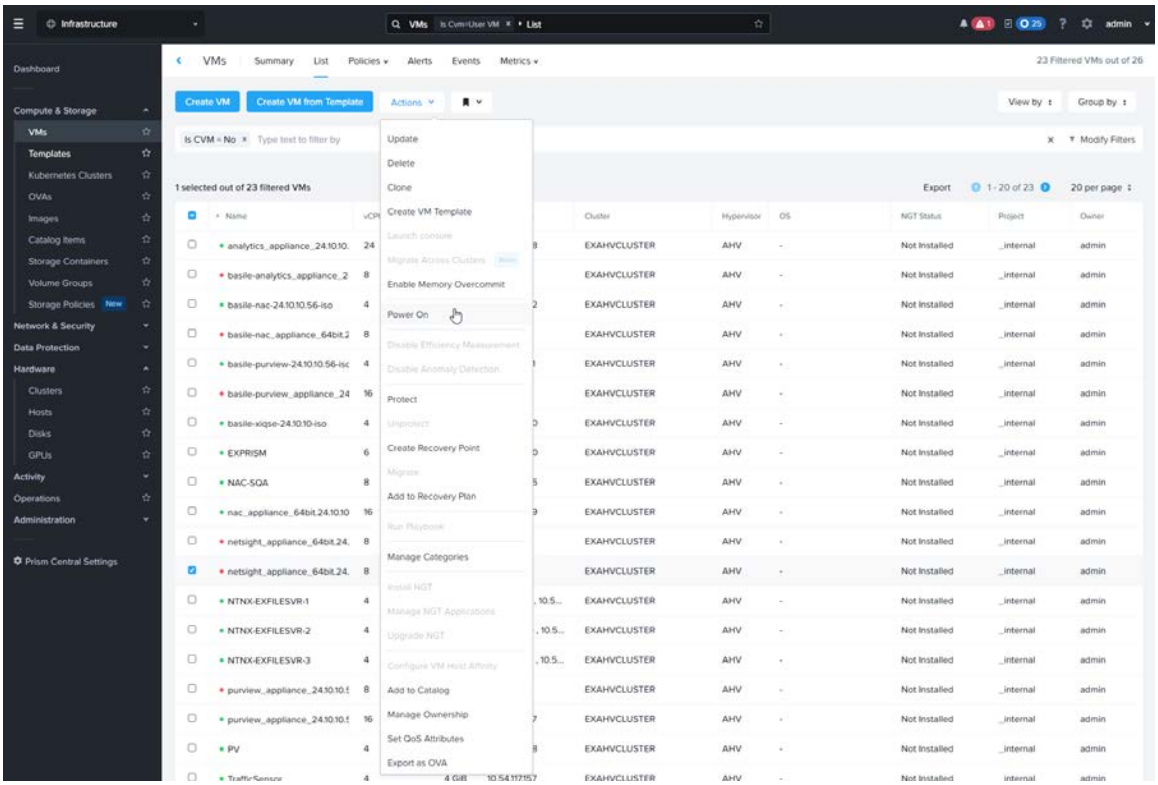


d. In the **Review** tab, select **Create VM**.

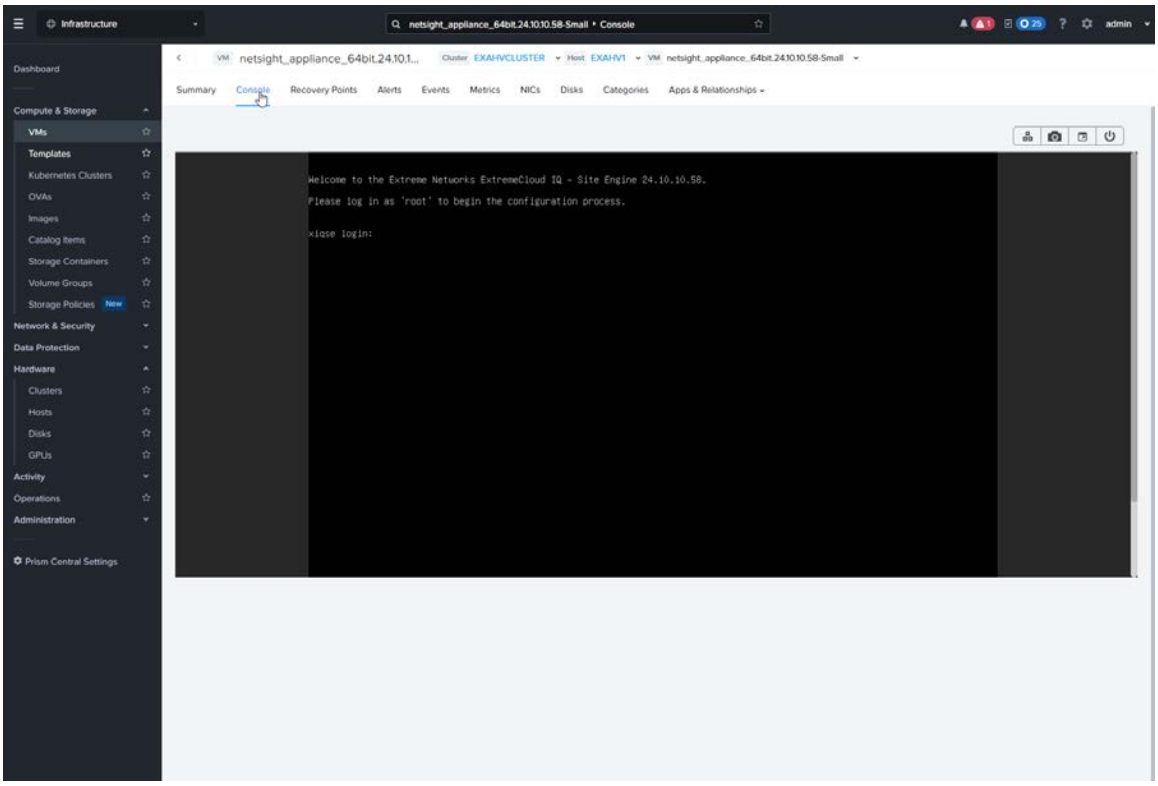


.

7. In the **Computer & Storage** menu, select **VMs**.
    a. Select the VM you deployed, then in the **Actions** menu, select **Power On**.



b. Select the VM you powered on. Select **Console** and follow the installation wizard.



You are now ready to begin configuring the engine.

- If you are configuring an ExtremeCloud IQ Site Engine virtual engine, see ExtremeCloud IQ Site 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 ExtremeAnalytics Engine Configuration.

Deploying the Virtual Engine on an Extreme Networks Universal Compute Platform Server

Deployment Requirements

A virtual engine is a software image that runs on a virtual machine. The ExtremeCloud IQ Site Engine, ExtremeControl, ExtremeAnalytics, and Application Analytics Traffic Sensor virtual engines are packaged in the `.TAR` file format and can be deployed on an Extreme Networks Universal Compute Platform.

For information about the different ExtremeCloud IQ Site Engine, ExtremeControl, ExtremeAnalytics, and Application Analytics Traffic Sensor virtual engine configurations and supported Operating System versions, see the latest ExtremeCloud IQ Site Engine Release Notes.

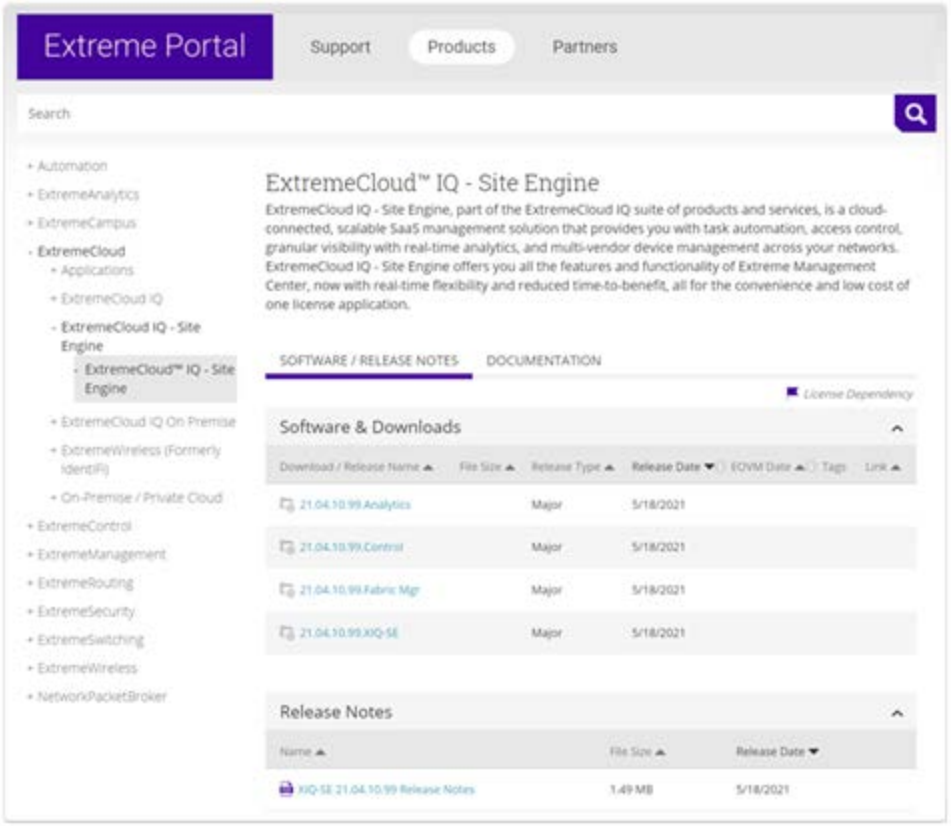
Deploying the Virtual Engine

Use the following steps to deploy an ExtremeCloud IQ Site Engine, ExtremeControl, ExtremeAnalytics, or Application Analytics Traffic Sensor virtual engine on an Extreme Networks Universal Compute Platform (UCP).

1. Download the ExtremeCloud IQ Site Engine, ExtremeControl, ExtremeAnalytics, or Application Analytics Traffic Sensor virtual engine software image to a local machine where the UCP is reachable.

   To download an engine image:

   a. Access the Extreme Portal at: https://extreme-networks.my.site.com/ExtrLogin?startURL=%2FExtrDownloadLanding.
   b. Login with your email address and password.
   c. Select the **Products** tab and select ExtremeCloud IQ Site Engine.
   d. Select **ExtremeCloud IQ Site Engine** in the right-panel.
   e. Select a version.
   f. Download the ExtremeCloud IQ Site Engine, ExtremeControl, ExtremeAnalytics, or Application Analytics Traffic Sensor virtual engine (appliance) image from the appropriate section.



2. Ensure the UCP is installed and running the supported version. For more information, see the UCP documentation.
3. In a browser, connect to UCP (`https://<IP-of-UCP>:5825/`) and log in. From the navigation menu navigate to **Cluster Settings > Cluster Configuration.**
    a. In **Deployment Type** choose **ExtremeCloud Edge – Self Orchestration**, and select **Next**.
    b. In **Cluster Node Information** select **Standalone**, provide the **ICC IP Address**, and select **Next**.
    c. In **Pod Network Configuration** define the **Pod Network IP Address**, **Pod Network CIDR**, **Service Network IP Address**, **Service Network CIDR**, and select **Create Cluster**. After the cluster creation process finishes, select **Done**.

    NOTE: The Pod and Service IPs are internal reserved address spaces within the UCP. Keep the default values unless the defined ranges overlap with the infrastructure address space in use. If that scenario occurs you can change to any other non-overlapping IP range.
4. In the navigation menu navigate to **Engines > Image Management >** upload the .TAR file you downloaded from the Extreme Portal either by drag and drop into the **Image File** pane, or by selecting the **Choose Image File** pane and navigate to the file.

5. In the navigation menu navigate to **Engines > Installation >** select the engine you uploaded, select **Install**, and select **Ok**.
6. Select the **engine** you want to deploy, confirm the port mapping, and select **Deploy**.

   NOTE: Keep the default port mapping unless GTAC tells you to change values. The default mapping uses VF01 in deployments with a single application for each UCP.
7. Wait until the Node and Port Information displays below the Instance, then select **Console**, and select **Attach**.

   NOTE: The deployment may take a few minutes. If you attach the console too early, the error "Can't connect to websocket" displays, which means the VM is not fully deployed yet.

You are now ready to begin configuring the engine.

- If you are configuring an ExtremeCloud IQ Site Engine virtual engine, see ExtremeCloud IQ Site Engine Engine Configuration.
- If you are configuring an ExtremeControl virtual engine, see ExtremeControl Engine Configuration.
- If you are configuring an ExtremeAnalytics virtual engine, see ExtremeAnalytics Engine Configuration.
- If you are configuring an Application Analytics Traffic Sensor virtual engine, see Configuring the Application Analytics Traffic Sensor.

ExtremeCloud IQ Site Engine Engine Configuration

After the ExtremeCloud IQ Site Engine virtual engine has been deployed on a supported server using the instructions in Engine Deployment, 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:

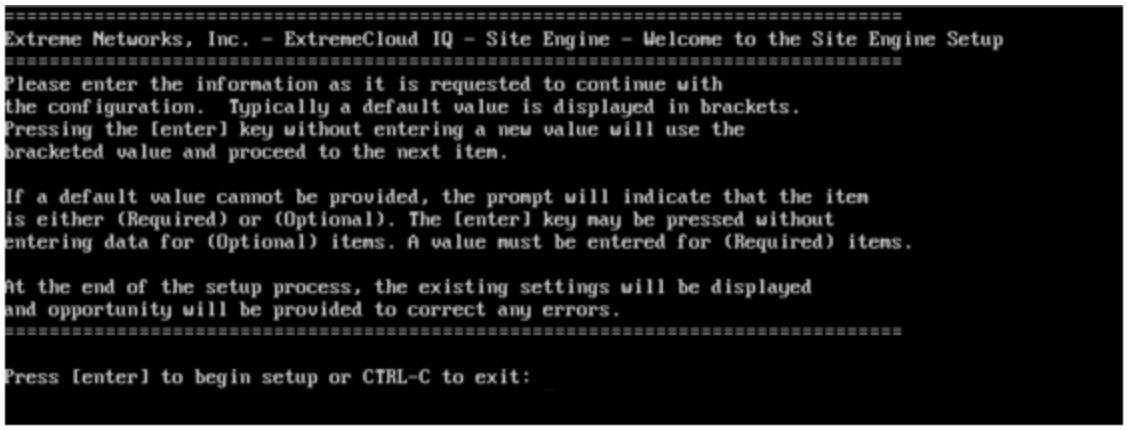
- Engine hostname, IP address, and netmask
- Default Gateway IP address
- Name Server IP address and domain name
- NIS (Network Information Services) Server IP address *(optional)*
- Network Time Protocol (NTP) server IP address
- Licensing for ExtremeCloud IQ Site Engine

For more information about Licensing for ExtremeCloud IQ Site Engine and ExtremeAnalytics, see ExtremeCloud IQ Site Engine Licensing.

Configuring the ExtremeCloud IQ Site Engine Engine

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

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

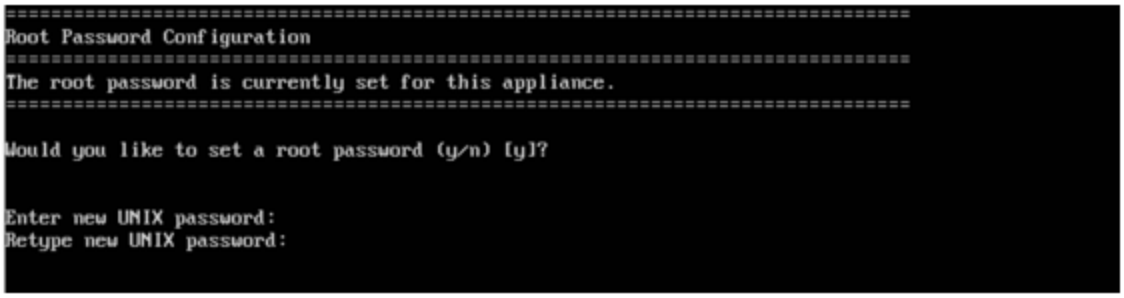


2. Press **[Enter]** to begin the setup.
   The **Root Password Configuration** screen displays:

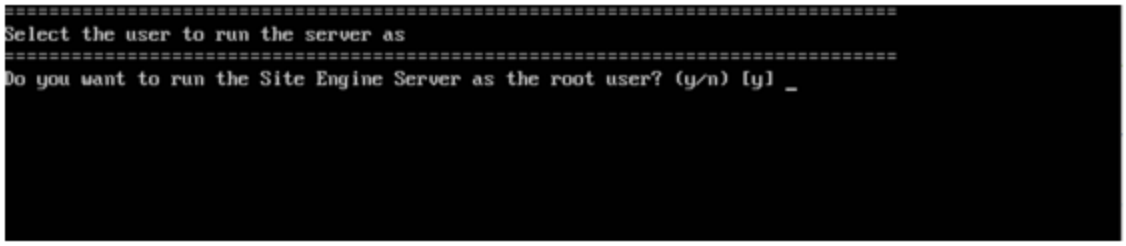


   Note: You must set a new root password. The root password will be used to access the CLI of the ExtremeCloud IQ Site Engine VM.

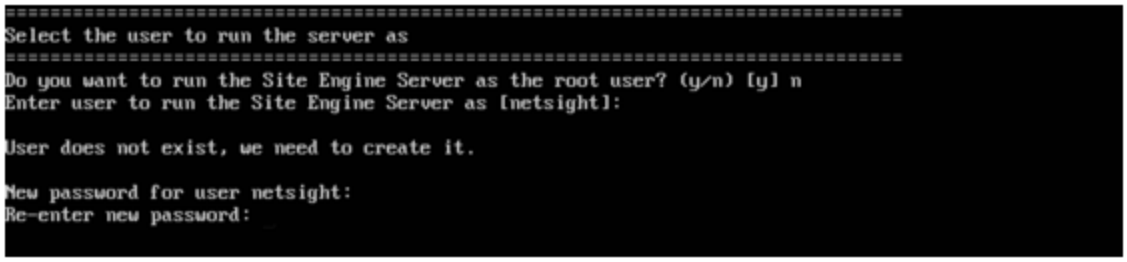
3. Press **[Enter]** to set a new root password. Enter the new password as prompted.



   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).



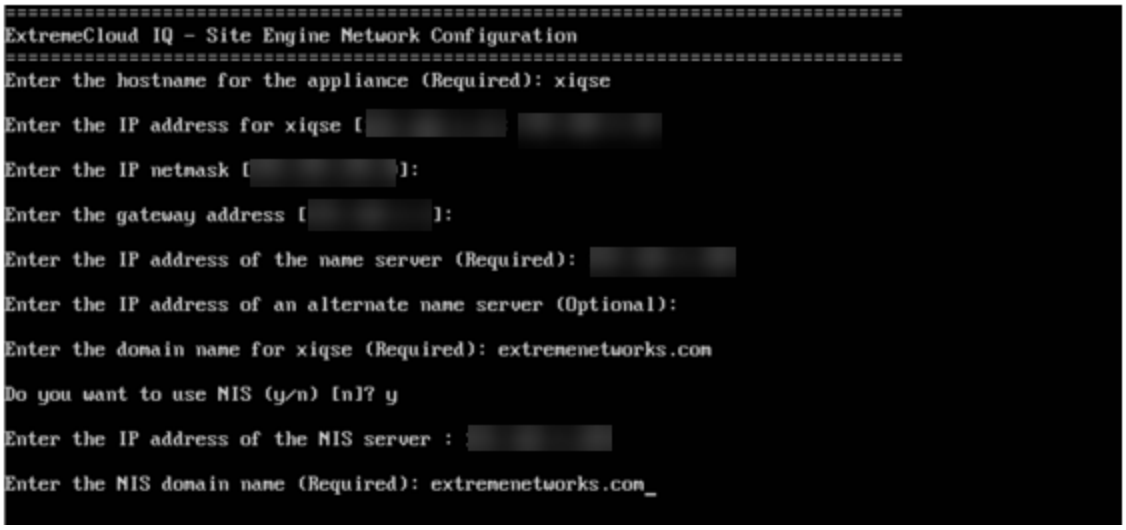
4. Enter **y** to use the root user. Accept your selection.
   Enter **n** to either use the "netsight" user or to specify a different user. Re-enter the password and then accept your selection.



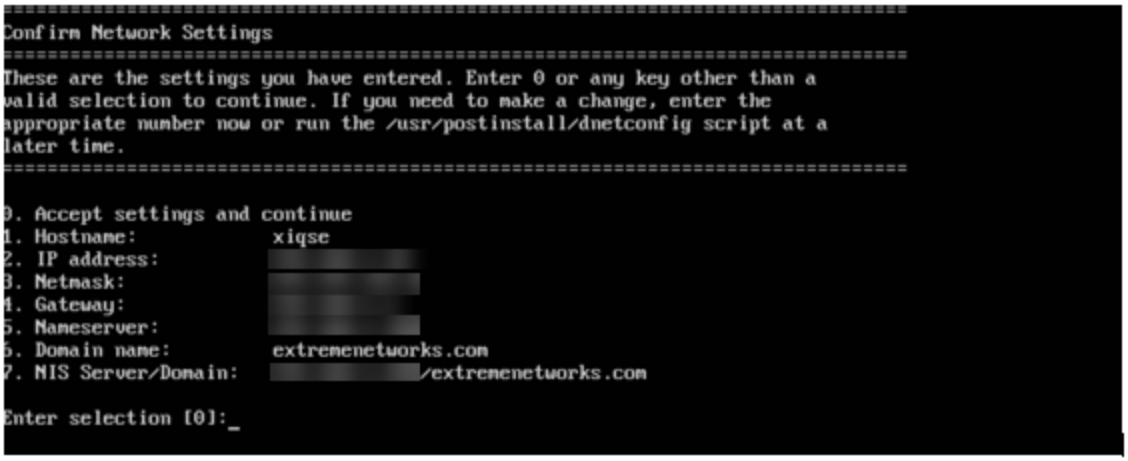
5. In the **Provide settings for the SCP/SFTP server** screen, enter the requested information for each line and press **[Enter]**.
   The default transfer method for modern devices is SCP or SFTP instead of TFTP. Enter the username for the SCP and SFTP transfers. Enter and confirm the password for the user. The directory structure is created with appropriate permissions.

```
================================================================
Provide settings for the SCP/SFTP server
================================================================
Would you like to provide settings for the SCP/SFTP server (y/n) [y]

Enter the user name to be used for SCP/SFTP transfers [sftp]:
New password for user sftp:
Re-enter new password:

You have provided these SCP/SFTP server settings:

 User Name : sftp
 Firmware Path : /home/sftp/firmware/images
 Root Path : /home/sftp

Do you accept (y/n) [y]
```

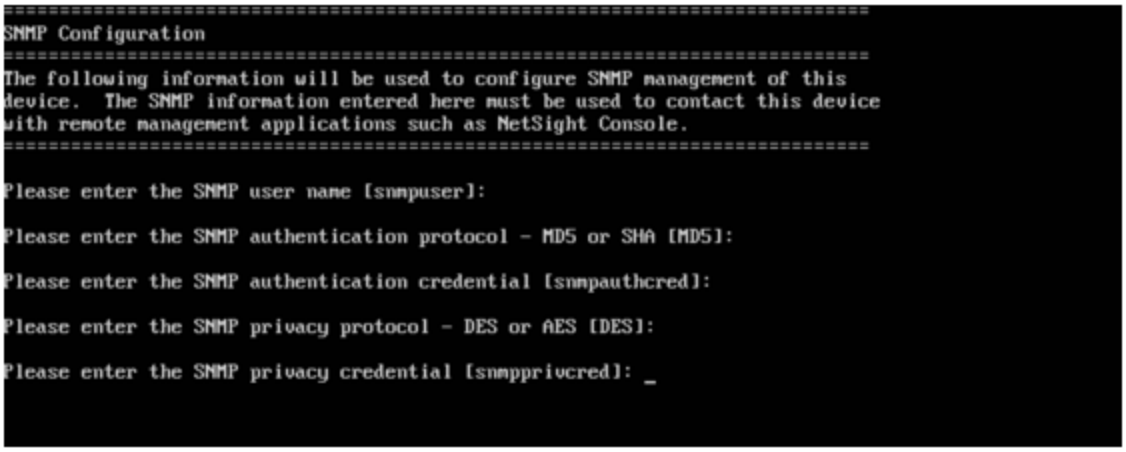
6. In the **Suite Network Configuration** screen, enter the requested configuration information for each line and press **[Enter]**.
   Enter the IP address of the name server. If you are using a name server, you must enter a domain name for the engine (appliance). If you are using an NIS server to authenticate 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.



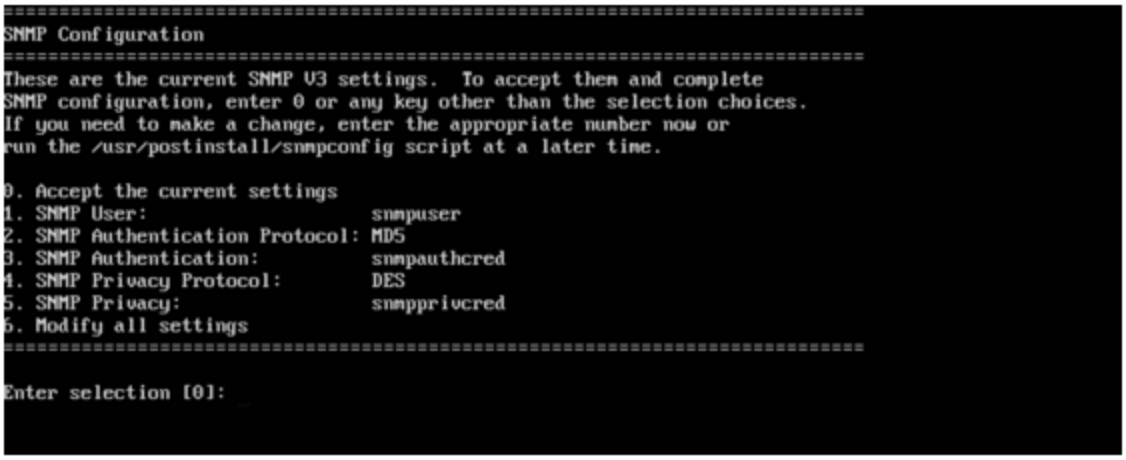
7. In the **Confirm Network Settings** screen, you can accept the current configuration or modify the settings.



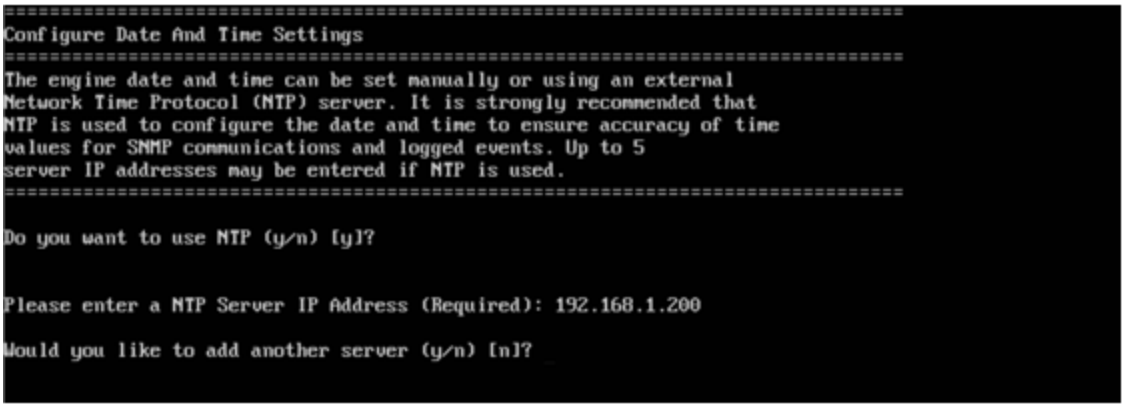
8. In the **SNMP Configuration** screen, enter the requested information for each line and press [Enter].



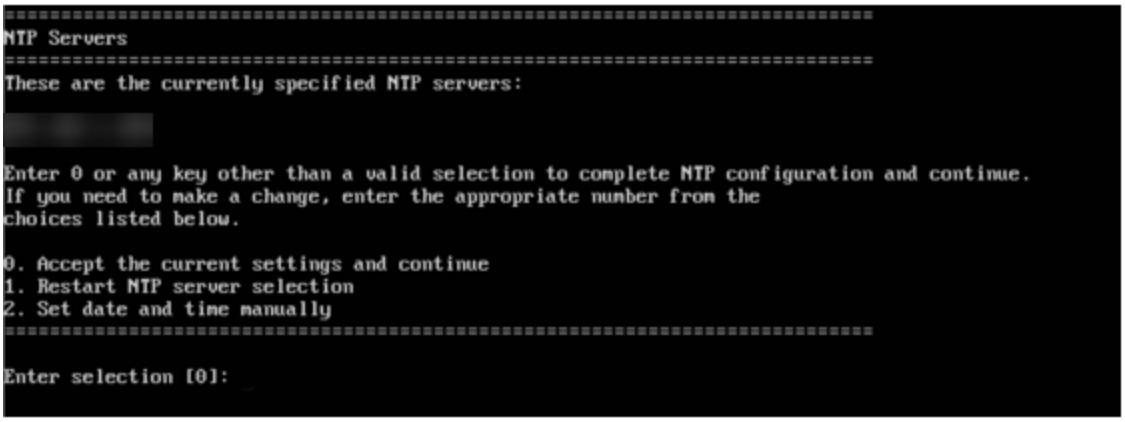
9. In the **SNMP Configuration summary** screen, enter **0** to accept the settings.



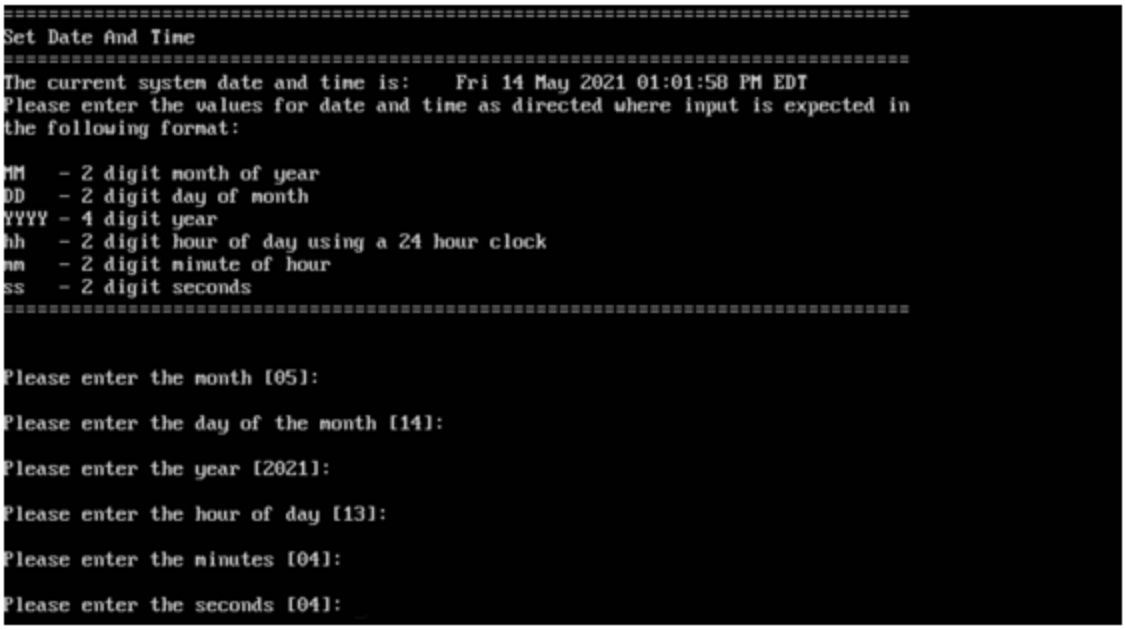
10. In the **Configure Date and Time Settings** screen, select whether you want to use an external Network Time Protocol (NTP) server. Enter **y** to use NTP, and enter your NTP server IP address (es). Or enter **n** to configure the date and time manually and proceed to step 12.
Note that your NTP server 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).



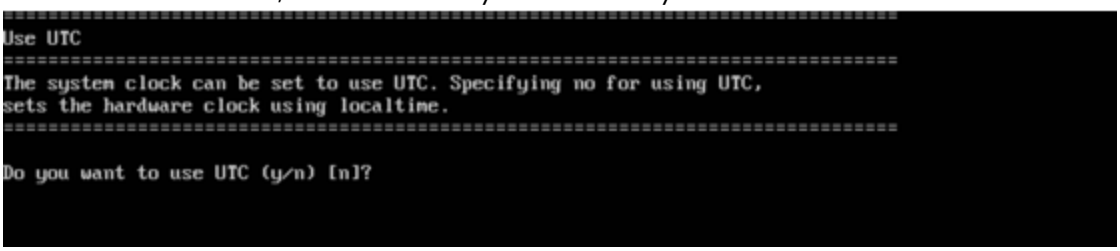
11. In the **NTP Servers validate selection** screen, enter **0** to accept the current settings and proceed to the Set Time Zone screen at step 14.



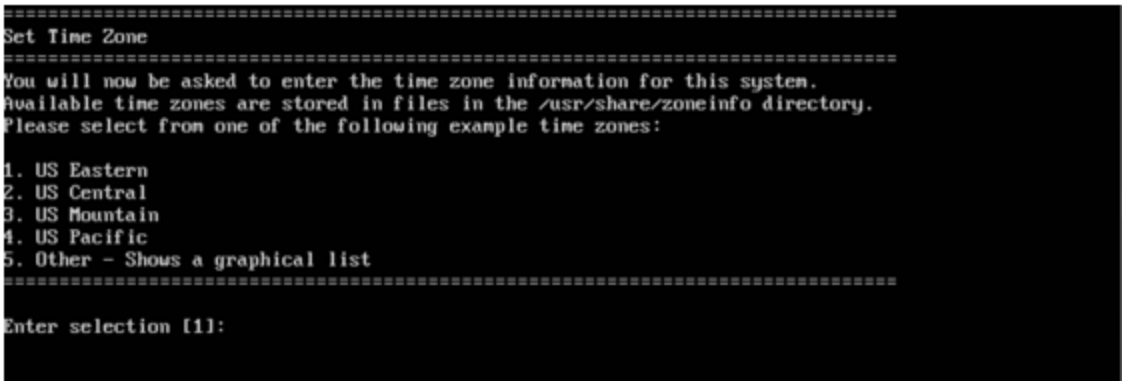
12. If you answered no to using an NTP server to set date and time, set the date and time in the **Set Date and Time** screen.



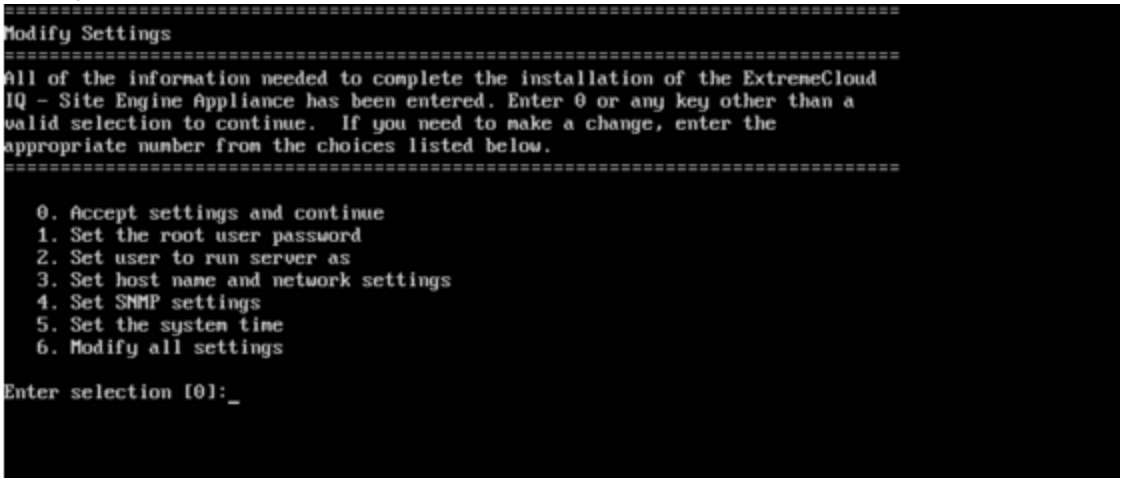
13. In the **Use UTC** screen, select whether you want the system clock to be set to use UTC.



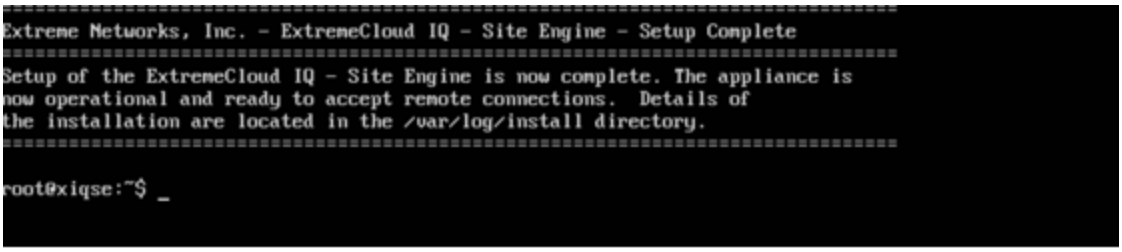
14. In the **Set Time Zone** screen, type the number that corresponds to the appropriate time zone and press **[Enter]**.



15. 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, refer to your Hypervisor 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 8443 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 step 3 or as the user you specified in 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 ExtremeCloud IQ

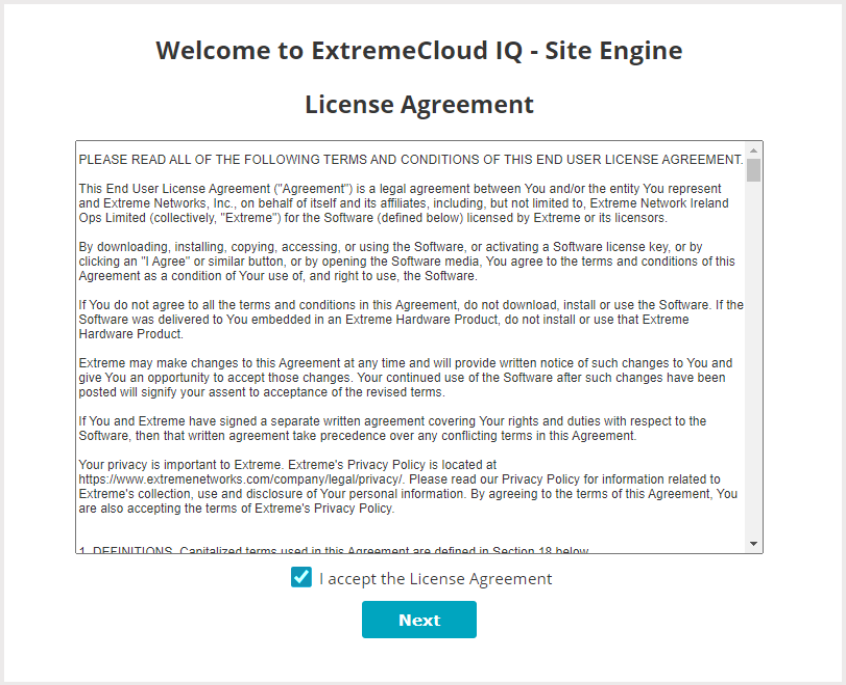
To access ExtremeCloud IQ Site Engine, you must first complete the steps to onboard ExtremeCloud IQ Site Engine to ExtremeCloud IQ.

- After Initial Installation of ExtremeCloud IQ Site Engine

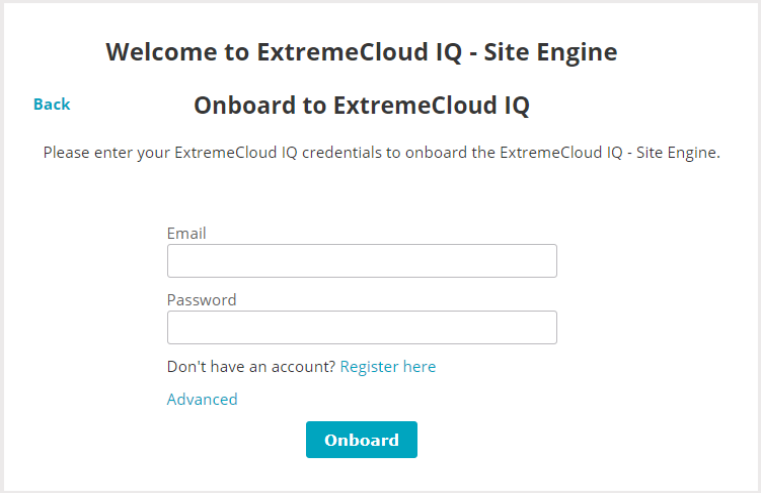
After Initial Installation of ExtremeCloud IQ Site Engine

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.



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



   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.

   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.

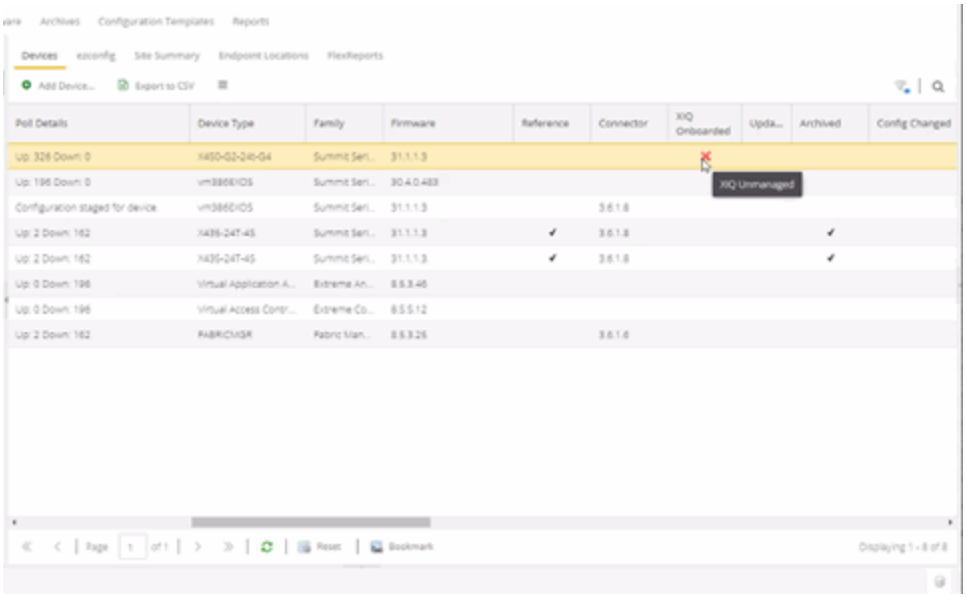
NOTES: Devices with IPv6 addresses in ExtremeCloud IQ Site Engine will not be onboarded as locally-managed devices in ExtremeCloud IQ. Only devices with IPv4 addresses qualify.

As devices are added and discovered in ExtremeCloud IQ Site Engine, they are onboarded to ExtremeCloud IQ, with a request for a license of the appropriate tier 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.

ExtremeCloud IQ 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.



- 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 26.11.10, 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 license limit violation, 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.

.

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 Console 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:
`/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:
`/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**:
`/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 your Hypervisor documentation for instructions on creating a snapshot.

1. On a system with an internet connection, go to the ExtremeCloud IQ Site Engine web page: https://extreme-networks.my.site.com/ExtrProductDetail?id=01t2T000004yHvgQAE.
2. 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`

   Run the command with root privileges (either login as root or use sudo). If the server is running as non-root then add `--user` attribute followed by the username.

   The upgrade automatically begins.

The ExtremeCloud IQ Site Engine Server is 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. Refer to your Hypervisor 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 Engine Deployment 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 Engine Deployment, 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

For more information about licensing for ExtremeControl, see ExtremeCloud IQ Site Engine Licensing.

Configuring the ExtremeControl Engine

To configure the virtual engine to run the ExtremeControl software:

1. In the **Console**, 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

Press CTRL-C to skip configuration for now
================================================================
Now extracting the Access Control Engine. This may take a few moments...



================================================================
```

```
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:
```

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 is active the first time the machine is rebooted.
================================================================
Would you like to set a root password (y/n) [y]?
```

2. 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.
```

3. 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):
```

4. In the **Provide settings for the SCP/SFTP server** screen, enter the requested information for each line and press **[Enter]**.
   The default transfer method for modern devices is SCP or SFTP instead of TFTP. Enter the

username for the SCP and SFTP transfers. Enter and confirm the password for the user. The directory structure is created with appropriate permissions.

```
================================================================
Provide settings for the SCP/SFTP server
================================================================
Would you like to provide settings for the SCP/SFTP server (y/n) [y]

Enter the user name to be used for SCP/SFTP transfers [sftp]:
New password for user sftp:
Re-enter new password:

You have provided these SCP/SFTP server settings:

 User Name : sftp
 Firmware Path : /home/sftp/firmware/images
 Root Path : /home/sftp

Do you accept (y/n) [y]
```

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 step 8.

```
================================================================
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
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
============================================================
Configuration of the appliance network settings is now complete. Enter 0 or any key other than a
valid selection to continue. If you need to make a change, enter the appropriate number from the
choices listed below. ============================================================
0. Accept the current settings
1. Edit NAC Appliance settings
2. Edit SNMP settings
3. Edit date and time
4. Modify all settings
============================================================
Enter selection [0]:
```

When you see the following screen, configuration is complete.

```
============================================================
Extreme Networks - 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, refer to your Hypervisor 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 **Console** to make the changes.

Using the Access Control tab

Use the **Access Control** tab to easily change Access Control Engine Settings 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 Network Settings 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 **Interfaces** window 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 **Static Route Configuration** window where you can add or edit the static routes used for advanced routing configuration.

Using the Console

Use the **Console** 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** 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 Using the Access Control tab).

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**:

```
/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**:

```
/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**:

```
/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**:

```
/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 here.

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 your Hypervisor 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. Refer to your Hypervisor 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 Engine Deployment 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 Engine Deployment, 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
- Licensing for ExtremeCloud IQ Site Engine

For more information about Licensing for ExtremeCloud IQ Site Engine and ExtremeAnalytics, see ExtremeCloud IQ Site Engine Licensing.

Configuring the ExtremeAnalytics Engine

To configure the virtual engine to run the ExtremeAnalytics application:

1. In the **Console**, 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:
```

4. 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 eth0 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]**.

```
============================================================
ExtremeAnalytics Appliance Network Configuration for Tap Mode
============================================================
Enter the interface name for Tap Mode [eth1]:  eth4
Would you like to add another interface for Tap Mode (y/n) [n]? y
Enter the interface name for Tap Mode [eth2]:  eth5
Would you like to add another interface for Tap Mode (y/n) [n]? n
```

   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. Accept 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:    255.255.255.0
       Gateway:    10.54.211.1
       Name:       eth5
       Address:    10.54.222.117
       Netmask:    255.255.255.0
       Gateway:    10.54.222.1
6. GRE tunnels:    10.54.211.116/10.54.1.116
                   10.54.222.117/10.54.2.117
```

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
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 **0** to accept the current settings and proceed to the Set Time Zone screen on step 18.

```
============================================================
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
mm   - 2 digit minute of hour
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 system clock can be set to use UTC. Specifying no for using UTC, sets
the hardware clock using localtime.
============================================================

Do you want to use UTC (y/n) [n]?
```

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, refer to your Hypervisor 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.

1. 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>:8443/`.
   where *<servername>* is the ExtremeCloud IQ Site Engine server IP address or hostname, and 8443 is the required port number.
2. 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.
5. Select **Dashboard**.
   The Dashboard tab displays.

Adding the Application Analytics Engine

To add the Application Analytics Engine to ExtremeAnalytics:

1. Select the **Analytics Configuration** tab, see Analytics Configuration tab
2. Open the drop-down list below Overview and select **Add Engine**.
3. Enter the following information:
    - IP address of the eth0 interface
    - Name of the Application Analytics Engine
4. From the **Profile** list, select the appropriate SNMP profile.
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 Console.

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:

```
/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:

```
/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:

```
/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**:
`/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**:
`/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 your Hypervisor 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: https://extreme-networks.my.site.com/ExtrProductDetail?id=01t2T000004yHvgQAE.
2. After entering your email address (username) and password, follow this path to the download page: **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. Refer to your Hypervisor 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 Engine Deployment 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.

Configuring the Application Analytics Traffic Sensor

To configure the virtual engine to run the Application Analytics Traffic Sensor Engine application, complete the following procedure.

1. In the **Console**, log in as root with no password, and then press **[Enter]**.
   The following screen displays.

```
============================================================
Extreme Networks, Inc. - Traffic Sensor Appliance -
Welcome to the Traffic Sensor Engine xx.xx.xx.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 is active 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 password will be used by the initial user when logging in to the Application Analytics Traffic Sensor Engine application.

3. Press **[Enter]** to set a new root password. Enter and confirm the password when prompted:

```
New UNIX password:
Retype new password:
```

4. For each line, enter the requested configuration information and press **[Enter]**.

```
============================================================
Network Configuration Settings
============================================================
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]?
```

   Note: If you use DNS, provide the name server IP address and enter a domain name for the engine. If you use NIS to authenticate users, ensure the NIS domain name is valid.

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

```
============================================================
SNMP Configuration
============================================================
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. On the **SNMP Configuration** summary screen, enter **0** to accept the settings.

```
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
```

7. On the **Configure Date and Time Settings** screen, choose whether to use an external NTP server. Enter **y** to use NTP and provide one or more NTP server IP addresses. Enter **n** to configure the date and time manually, then proceed to step 9.

```
============================================================
Configure Date And Time Settings
============================================================
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
```

Note: The UCP server should use the same NTP settings as the virtual engine.

8. On the **NTP Servers** validation screen, enter **0** to accept the current settings and proceed to the Set Time Zone screen on step 11.

```
============================================================
NTP Servers
============================================================
144.131.10.120
0. Accept the current settings
1. Restart NTP server selection
2. Set date and time manually
Enter selection [0]: 0
```

9. If you chose not to use an NTP server, set the date and time manually on the **Set Date And Time** screen.

```
============================================================
Set Date And Time
============================================================
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 [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]:
```

10. Enter **n** on the **Use UTC** screen.

```
============================================================
Use UTC
============================================================
Do you want to use UTC (y/n) [n]?
```

11. On the **Set Time Zone** screen, select the appropriate time zone and press **[Enter]**.

```
============================================================
Set Time Zone
============================================================
1. US Eastern
2. US Central
3. US Mountain
4. US Pacific
5. Other - Shows a graphical list
Enter selection [1]:
```

12. On the **Modify Settings** screen, review the settings. Enter **0** to accept them and continue.

```
============================================================
Modify Settings
============================================================
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 Application Analytics Traffic Sensor Engine application software is installed automatically. When installation is complete, the following message displays:

```
============================================================
Extreme Networks - Traffic Sensor Appliance - Setup Complete
============================================================
Setup of the Traffic Sensor Engine 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.
============================================================
The Web Credentials are configured in
OneView -> Analytics -> Configuration -> Engines -> Configuration
If the Web Credentials have been modified from defaults, execute the
following
command and set the same values before re-adding this engine to Extreme
Analytics:
```

```
Execute: /opt/appid/configWebCredentials <username> <password>
============================================================
```

Launching the ExtremeAnalytics Application

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

1. 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>:8443/`.
   where *<servername>* is the ExtremeCloud IQ Site Engine server IP address or hostname, and 8443 is the required port number.
2. 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.
5. Select **Dashboard**.
   The **Dashboard** tab displays.

Adding the Application Analytics Traffic Sensor Engine

To add the Application Analytics Traffic Sensor Engine to ExtremeAnalytics:

1. Select the **Analytics Configuration** tab, see Analytics Configuration tab
2. Open the drop-down list below Overview and select **Add Engine**.
3. Enter the following information:
   - IP address of the eth0 interface
   - Name of the Application Analytics Traffic Sensor Engine
4. From the **Profile** list, select the appropriate SNMP profile.
5. Select **OK**.
6. Open the drop-down list below Overview and select **Enforce Engine**.

Changing Application Analytics Traffic Sensor Engine Settings

Use these steps if you need to change your Application Analytics Traffic Sensor virtual engine settings following your initial engine configuration. Perform these steps in the Console.

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**:
`/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**:
`/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**:
`/usr/postinstall/dateconfig`

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

Changing the Application Analytics Traffic Sensor Server IP Address

To change the IP address of the Application Analytics Traffic Sensor server, enter the following command at the login prompt in the **Console**:
`/opt/appid/configMgmtIP <IP address>`

Then, start using the new Application Analytics Traffic Sensor 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 Application Analytics Traffic Sensor 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**:
`/opt/appid/configWebCredentials <username> <password>`

Then, restart the engine by typing: `appidctl restart`

Upgrading Application Analytics Traffic Sensor Engine Software

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

1. On a system with an Internet connection, go to the Network Management Suite (NMS) Download web page: https://extreme-networks.my.site.com/ExtrProductDetail?id=01t2T000004yHvgQAE.
2. After entering your email address (username) and password, follow this path to the download page: **Select a version**.
3. Download the following Application Analytics Traffic Sensor Engine file from the NMS Downloads section:

   `Analytics/analytics_appliance_upgrade_to_<version>.bin`
4. Use FTP, SCP, or a shared mount point, to copy the file to the Application Analytics Traffic Sensor 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 analytics_appliance_upgrade_to_<version>.bin`
8. Run the install program by entering the following command:

   `./analytics_appliance_upgrade_to_<version>.bin`

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

Reinstalling Application Analytics Traffic Sensor Engine Software

In the event that a software reinstall becomes necessary, you will need to re-deploy and reconfigure the ExtremeAnalytics virtual engine following the instructions in Engine Deployment and this section.

Note: The re-installation procedure reformats the hard drive, reinstalls all the Application Analytics Traffic Sensor Engine software, the operating system, and all related Linux packages.