Extreme

Extreme Management Center®, ExtremeControl®, and ExtremeAnalytics® Virtual Engine Installation Guide

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

Engine Deployment

This chapter provides an overview of Extreme Management Center, ExtremeControl, and ExtremeAnalytics virtual engine deployment requirements and provides instructions for deploying a virtual engine on a VMware® and Hyper-V server.

Deploying the Virtual Engine on a VMware ESX Server

Deployment Requirements

A virtual engine is a software image that runs on a virtual machine. The Extreme Management Center, ExtremeControl, and ExtremeAnalytics virtual engines are packaged in the `.OVA` file format defined by VMware and must be deployed on a VMware ESXi™ 6.0 server with a vSphere™ client, or on a VMware ESXi™ 6.5, 6.7, or 7.0 server using the web client.

For information about the different Extreme Management Center, ExtremeControl, and ExtremeAnalytics virtual engine configurations, see the latest Extreme Management Center *Release Notes*.

Deploying the Virtual Engine

Use the following steps to deploy an Extreme Management Center, ExtremeControl, or ExtremeAnalytics virtual engine on a VMware ESX or ESXi server.

1. Download the Extreme Management Center, ExtremeControl, or ExtremeAnalytics virtual engine software image to your local machine where the client is installed and running.

   To download an engine image:

   1. Access the Extreme Portal at: https://extremeportal.force.com/.
   2. After entering your email address and password, you are on the Support page.
   3. Select the **Products** tab and select ExtremeManagement.

4. Select **Extreme Management Center** in the right-panel.

5. Select a version.

6. Download the Extreme Management Center, ExtremeControl, or ExtremeAnalytics virtual engine (appliance) image from the appropriate section.

2. Open the VMWare software. From the **Host** menu, select **Create/Register VM.**
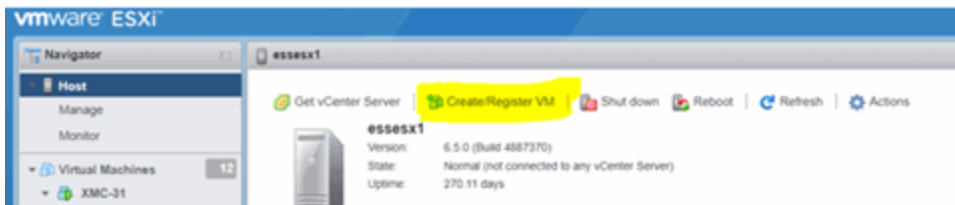
3. From the **Select creation type** panel, select **Deploy a virtual machine from an .OVF or .OVA file**. Select **Next**.
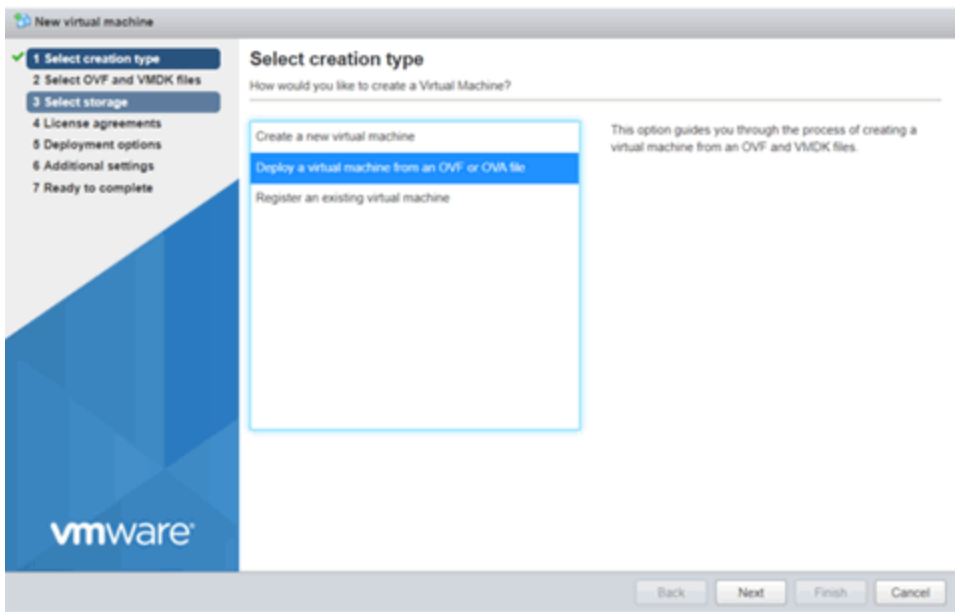
4. Enter the name of the virtual machine and select the .OVA file. Select **Next** to continue.
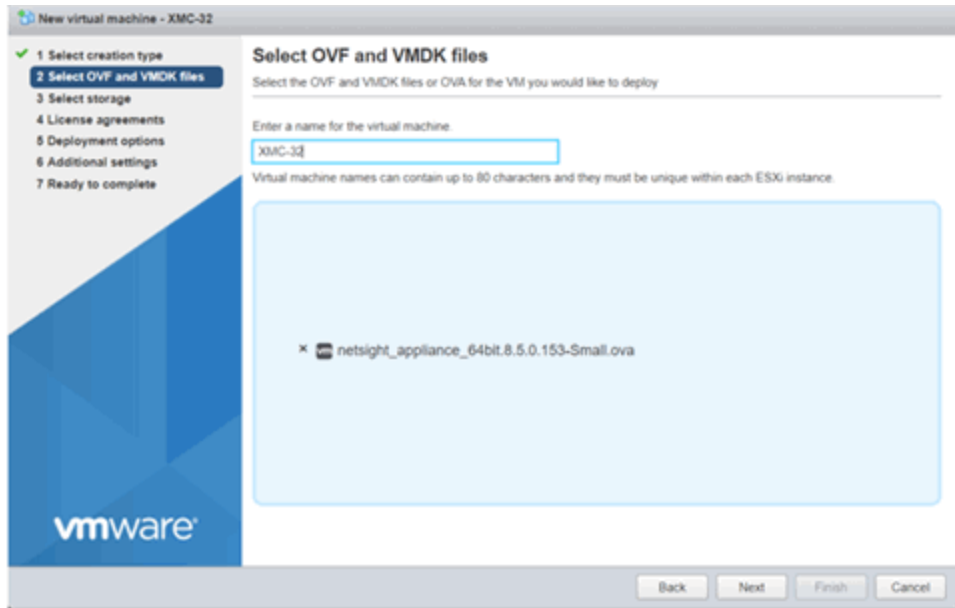
5. Select your datastore. Select **Next** to continue.
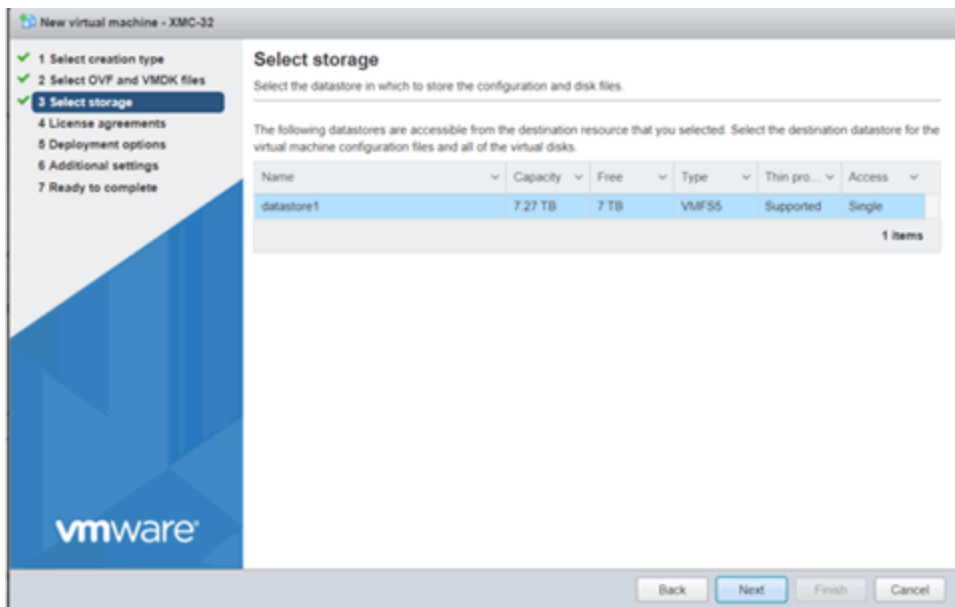
6. Select your deployment options and select **Next**.
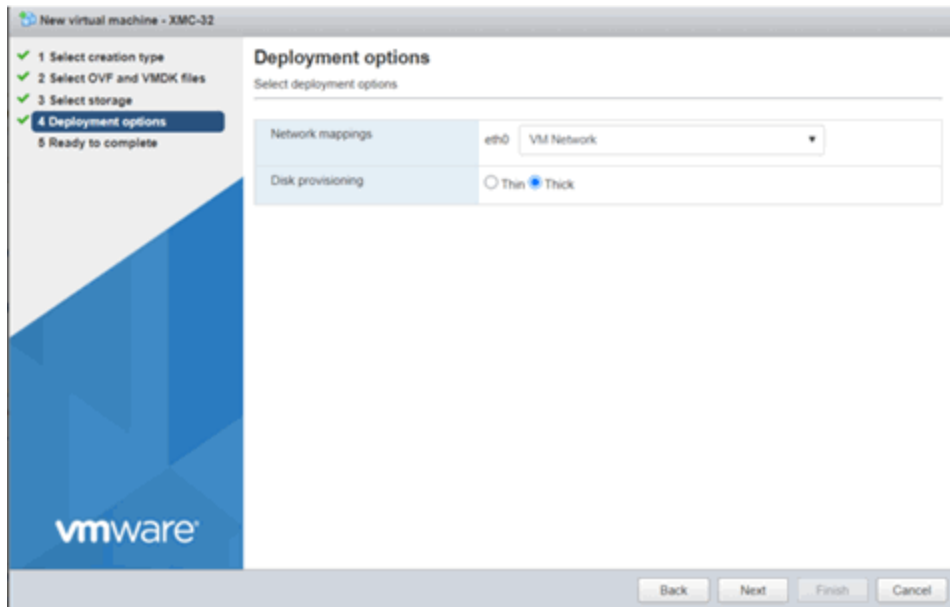
7. Review and select **Finish** to start the deployment.
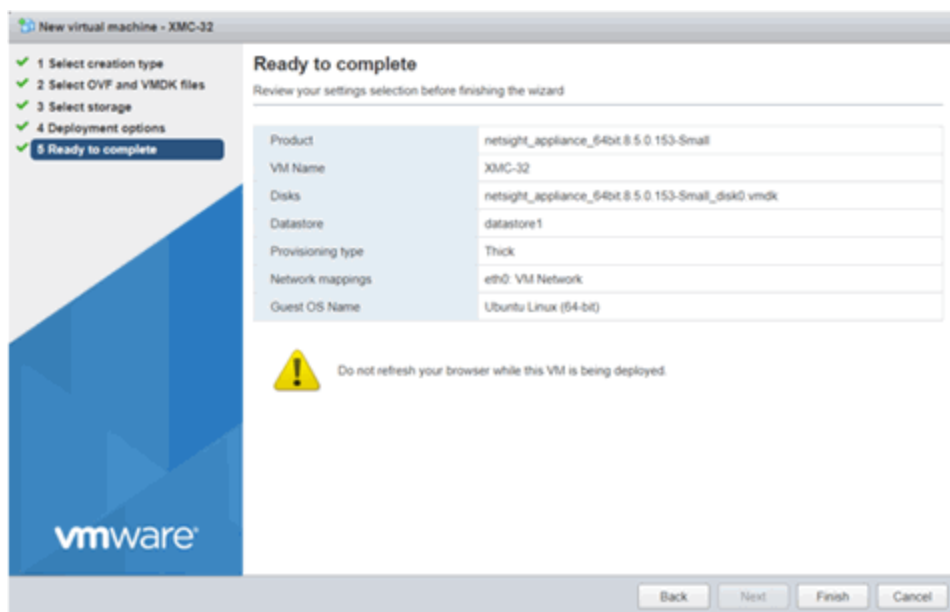
After the .OVA file has finished uploading and importing, you are now ready to begin configuring the engine.

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 , Extreme Management Center, 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 Extreme Management Center, ExtremeControl, or ExtremeAnalytics virtual engine on a VMware ESX or ESXi server.

1. Download the Extreme Management Center, ExtremeControl, or ExtremeAnalytics virtual engine software image to your local machine where the vSphere client is installed and running.

   To download an engine image:

   1. Access the Extreme Portal at: https://extremeportal.force.com/.
   2. After entering your email address and password, you are on the Support page.
   3. Click the **Products** tab and select ExtremeManagement.
   4. Click **Extreme Management Center** in the right-panel.
   5. Select a version.
   6. Download the Extreme Management Center, 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**.
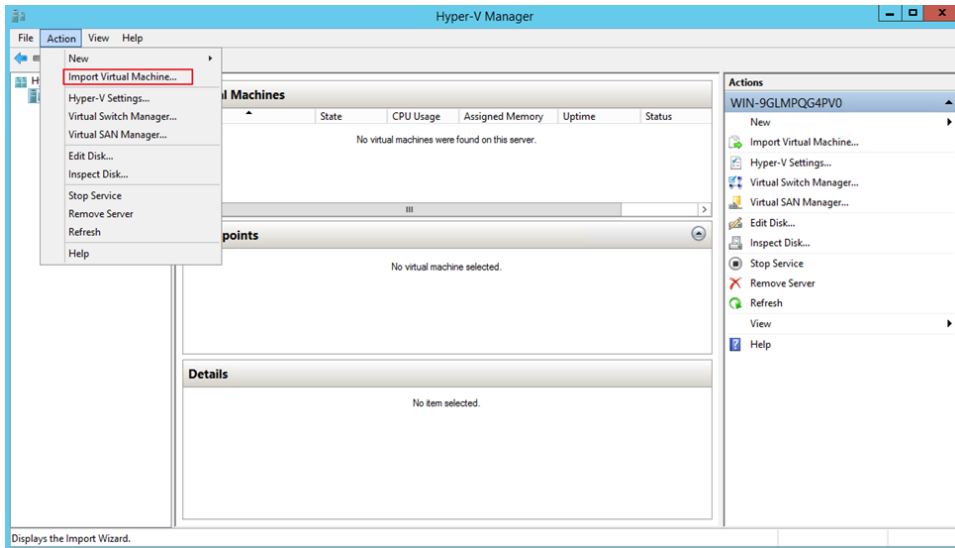
The **Import Virtual Machine** wizard opens to the Before You Begin
panel.
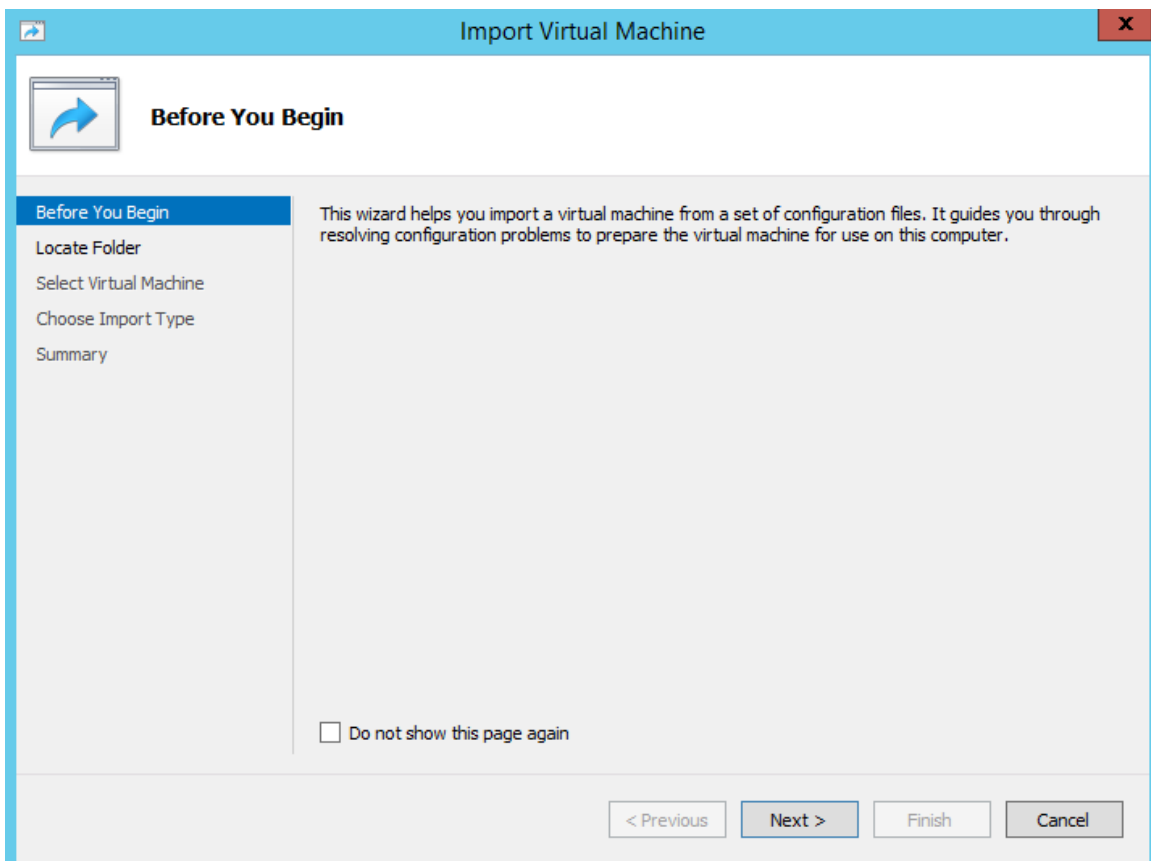
Select **Next**.

5. **The Locate Folder panel opens.**

6. Click the **Browse** button and navigate to the folder where you saved the engine image.

7. Click **Select Folder**, and then **Next**.
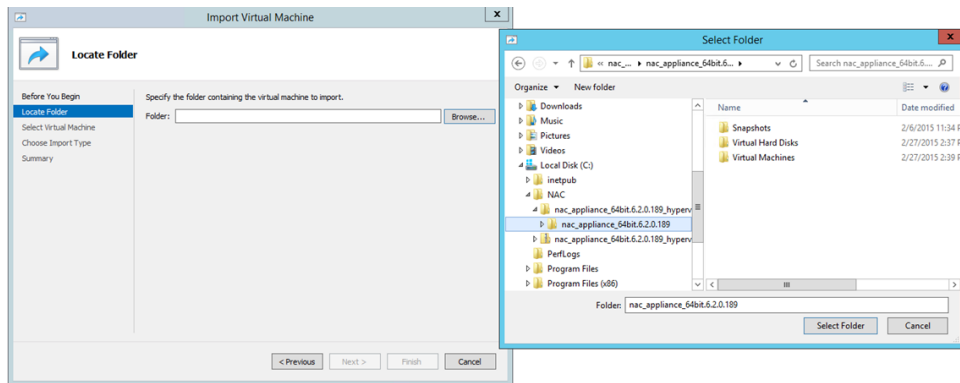
The Select Virtual Machine panel opens.

8. Select the virtual machine you are importing, and then click **Next**.
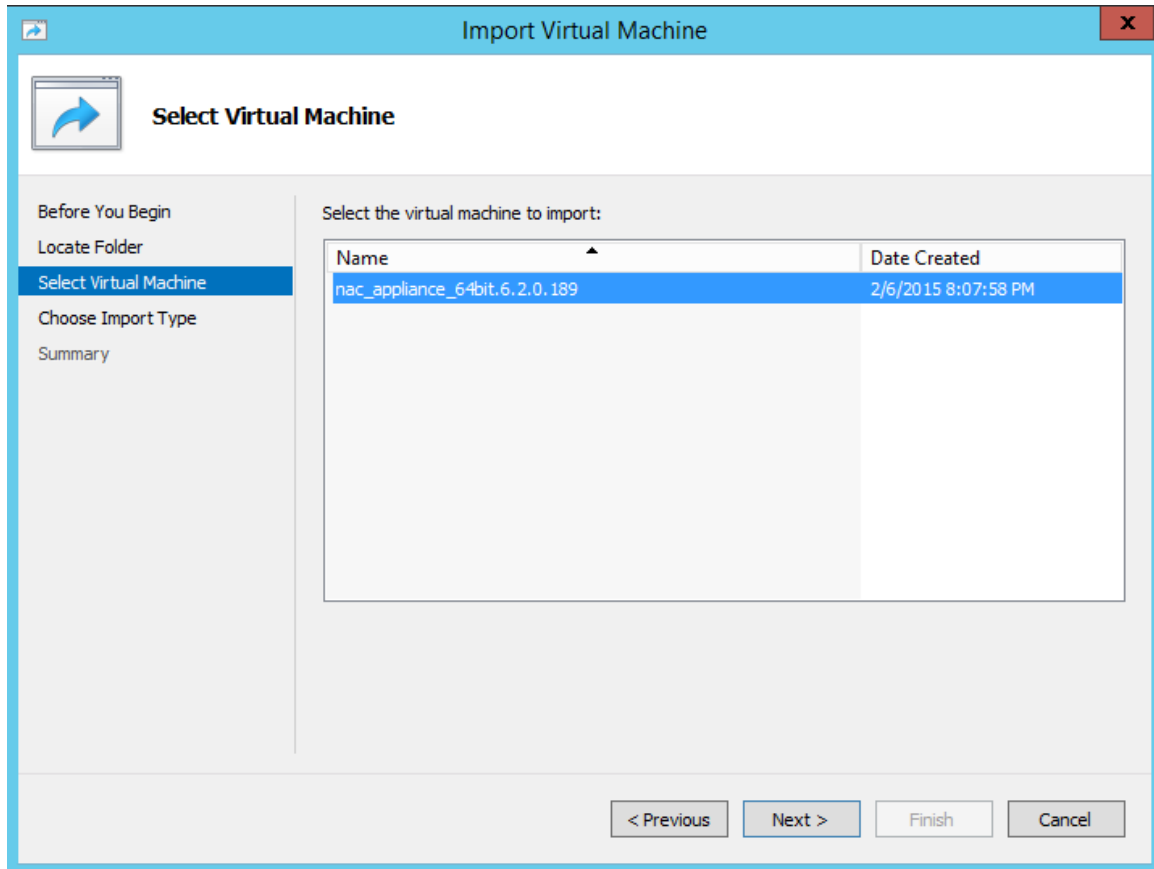
The Choose Import Type panel opens.
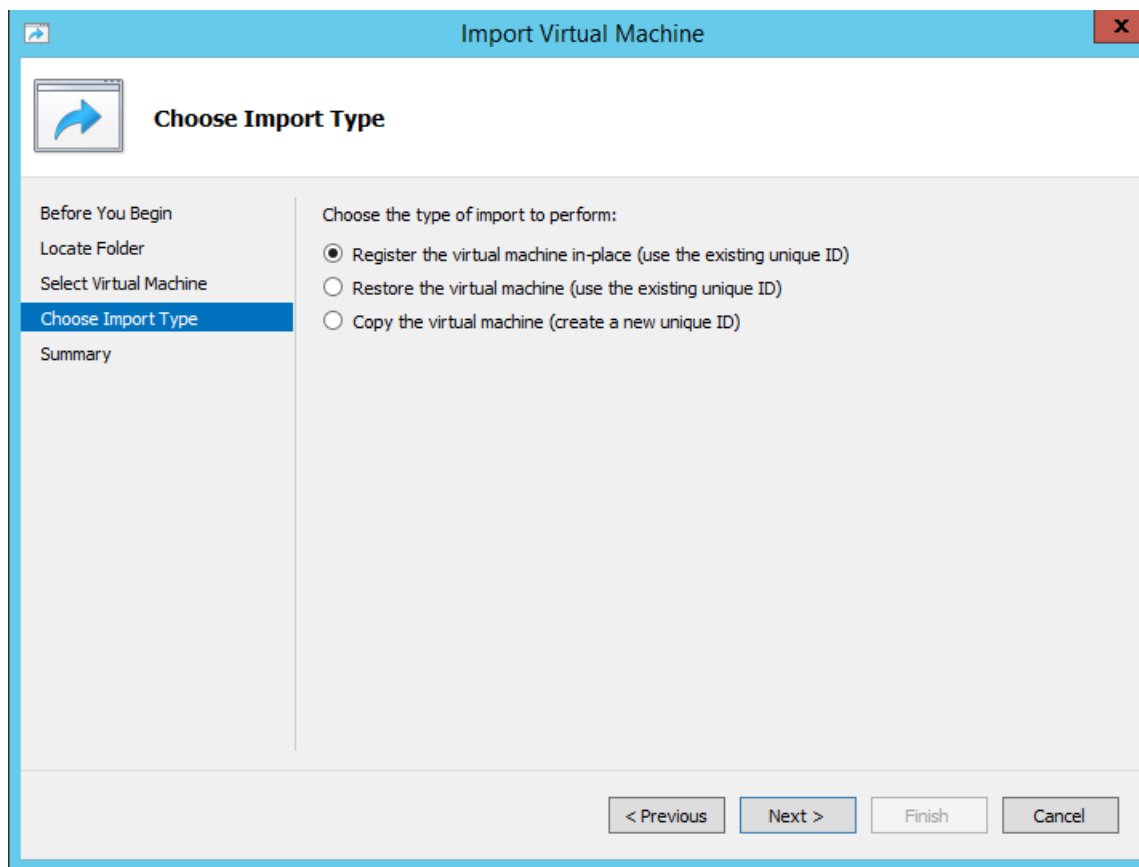
9. Select the radio button that corresponds to the appropriate type for your machine.

   - **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.
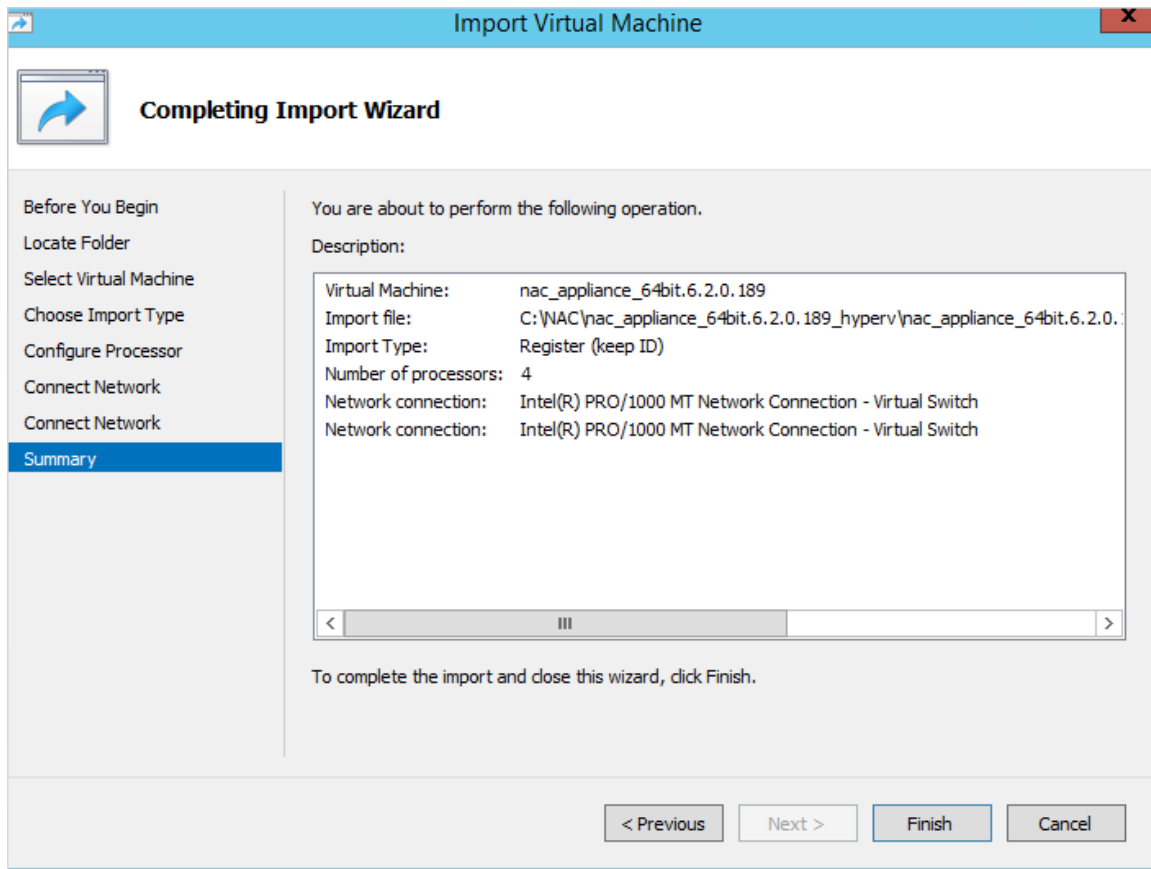
You are now ready to begin configuring the engine.

- If you are configuring an Extreme Management Center virtual engine, see Extreme Management Center 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.

Extreme Management Center Engine Configuration

Once the Extreme Management Center 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

In addition, you must obtain the appropriate Extreme Management Center software license(s) prior to launching the Extreme Management Center applications. You will be prompted to enter a license for any unlicensed application that is launched. (When you purchased Extreme Management Center, 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.)

Configuring the Extreme Management Center Engine

To configure the virtual engine to run the Extreme Management Center applications:

1. In the **Console** tab of the vSphere client, login as root with no password, and then press **[Enter]**.
   The following screen appears.
   ```
   ===============================================================
   ======
   Extreme Networks - Extreme Management Center
   Welcome to the Extreme Management Center Appliance Setup
   ===============================================================
   ======
   Please enter the information as it is requested to continue with the
   configuration.
   Typically a default value is displayed in brackets. Pressing the [enter]
   key without entering a new value will use the bracketed value and
   proceed to the next item.
   If a default value cannot be provided, the prompt will indicate that the
   item is either (Required) or (Optional). The [enter] key may be
   pressed without entering data for (Optional) items. A value must be
   entered for (Required) items.
   At the end of the setup process, the existing settings will be displayed
   and opportunity will be provided to correct any errors.
   ===============================================================
   ======
   Press [enter] to begin setup or CTRL-C to exit:
   ```

2. Press **[Enter]** to begin the setup.
   The Root Password Configuration screen appears:
   ```
   ===============================================================
   ======
   Root Password Configuration
   ===============================================================
   ======
   There is currently no password set on the system administrator
   account (root). It is recommended that you set one so that it 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. The root password will be used to access the CLI of the Extreme Management Center VM.

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

Enter new UNIX password:
Retype new UNIX password:
Password updated successfully.

After you create the new root password, a screen appears where you can specify a user other than root to run the Extreme Management Center server, if desired. This user becomes the admin user for the server. (Use the root user account when performing upgrades and accessing CLI).

===
======
Select the user to run the server as
===
======
Do you want to run the Management Center Server as the root user?
(y/n) [y]

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.

===
======
Select the user to run the server as
===
======
Do you want to run the Management Center Server as the root user?
(y/n) [n]
Enter user to run the Management Center Server as [netsight]:

User does not exist, we need to create it.

New password for user netsight:
Re-entr new password:_

5. In the **Suite Network Configuration** screen, enter the requested configuration information for each line and press **[Enter]**.
If you plan to use DNS, 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 may not be able to log in to the Extreme Management Center applications.

```
================================================================
======
Management Center Suite Network Configuration
================================================================
======
Enter the hostname for the appliance (Required):
Enter the IP address for <hostname> [192.168.1.10]:
Enter the IP netmask [255.255.255.0]:
Enter the gateway address [192.168.1.1]:
Enter the IP address of the name server (Optional):
Enter the domain name for <hostname> (Optional):
Do you want to use NIS (y/n) [n]? y
Enter the IP address of the NIS server:
Enter the NIS domain name (Required):
```

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

```
================================================================
======
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: <hostname>
2. IP address:   192.168.1.10
```

3. Netmask: 255.255.255.0
4. Gateway: 192.168.1.1
5. Nameserver: <IP address>
6. Domain name: <domain name>
7. NIS Server/Domain:

Enter selection [0]:

7. 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.
================================================================
======
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]:
```

8. In the **SNMP Configuration summary** screen, 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: [snmpuser]
2. SNMP Authentication Protocol: [MD5]:
```

```
3. SNMP Authentication: [snmpauthcred]
4. SNMP Privacy Protocol: [DES]
5. SNMP Privacy: [snmpprivcred]
5. Modify all settings
===================================================================
======
Enter selection [0]: 0
```

9. In the **Configure Date and Time Settings** screen, select whether you want to use an external Network Time Protocol (NTP) server. Enter **y** to use NTP, and enter your NTP server IP address(es). Enter **n** to configure the date and time manually and proceed to step 11.
   Note that your NTP server should be using the same NTP settings as those configured for your virtual engine (i.e., the same settings as the VMs that are hosted on the NTP server).

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

10. In the **NTP Servers validate selection** screen, enter **0** to accept the current settings and proceed to the Set Time Zone screen at step 13.

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

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

```
===============================================================
======
Set Date And Time
===============================================================
======
The current system date and time is: Thu Oct 28 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 [10]:
Please enter the day of the month [28]:
Please enter the year [2018]:
Please enter the hour of day [09]:
Please enter the minutes [34]:
Please enter the seconds [08]:
```

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

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

13. In the **Set Time Zone** screen, type the number that corresponds to 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]:
```

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

```
===============================================================
======
Modify Settings
```

```
================================================================
======
All of the information needed to complete the installation of the
Extreme Management Center 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 user to run server as
3. Set hostname and network settings
4. Set SNMP settings
5. Set the system time
6. Modify all settings

Enter selection [0]:
```

The Extreme Management Center application software is automatically installed.
This could take a few minutes. When you see the following screen, configuration
is complete.

```
================================================================
===
Extreme Networks - Management Center Suite - Setup Complete
================================================================
===
Setup of the Extreme Management Center 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
recovery is required. For instructions on how to take a snapshot, see your
vSphere client documentation.

Launching Extreme Management Center

Now that you have configured the Extreme Management Center virtual engine, you are ready to access Extreme Management Center from a remote client machine.

Open a browser window on the remote client machine and enter the Extreme Management Center Launch page URL in the following format:

```
https://<servername>:8443/
```

where *<servername>* is the Extreme Management Center virtual engine IP address or hostname, and 8080 is the required port number. For example,
`https://10.20.30.40:8443/`
Extreme Management Center 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 Extreme Management Center Server has a single pre-defined user, which is the user who performed the Extreme Management Center installation. Once the initial user has logged in, additional users (with usernames valid for Ubuntu) can log in.

The first time you attempt to launch Extreme Management Center, you are prompted for the license text you received when you generated your Extreme Management Center product license.

For more information on the Extreme Management Center Launch page, access the Extreme Management Center Online Help by clicking the **?** icon in the top-right corner of Extreme Management Center.

Restoring a Database from a Windows Server to the Engine

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

Changing Console

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

Changing Syslog Location

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

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

Changing Traps Location

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

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

Changing Inventory Settings

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

1. Select **Administration** > **Options**.

2. Expand the **Inventory Manager** options folder and select **Directory Path** in the Data Storage section.

3. Change the path to the correct new location.
   On a default installation, the path would be :/usr/local/Extreme_ Networks/NetSight/appdata/InventoryMgr/

4. Click **OK**.

Changing Extreme Management Center Engine Settings

Use these steps if you need to change your Extreme Management Center virtual engine settings following your initial engine configuration. Perform these steps in the vSphere client **Console** tab or login using an ssh session to Extreme Management Center CLI..

Changing Basic Network Configuration

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

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

Changing SNMP Configuration

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

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

Changing Date and Time Settings

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

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

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

Upgrading Extreme Management Center Engine Software

Upgrades to the Extreme Management Center engine software are available on the Extreme Management Center web page.

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

1. On a system with an internet connection, go to the Extreme Management Center web page: http://extranet.extremenetworks.com/downloads/pages/NMS.aspx.
2. Enter your email address and password.
   You will be on the Extreme Management Center page.
3. Click on the **Software** tab and select a version of Extreme Management Center.
4. Download the Extreme Management Center virtual engine image from the Extreme Management Center Virtual Appliance (engine) section.
5. Use FTP, SCP, or a shared mount point, to copy the file to the Extreme Management Center 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 ExtremeManagementCenter_Suite_<version number>_
   64bit_install.bin
   ```

9. Run the install program by entering the following command:
   ```
   ./ExtremeManagementCenter_Suite_<version number>_64bit_
   install.bin
   ```
   The upgrade automatically begins.

The Extreme Management Center Server are restarted automatically when the upgrade is complete. Because your Extreme Management Center engine settings were migrated, you are not required to perform any configuration on the engine following the upgrade.

Reinstalling Extreme Management Center Appliance Software

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

If you do not have an engine snapshot to restore, you must re-deploy and reconfigure the Extreme Management Center 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 Extreme Management Center engine software, the operating system, and all related Linux packages. We recommend backing up your hard drive before reinstalling.

ExtremeControl Engine Configuration

Once 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
- Extreme Management Center Server IP address
- Name Server IP address and domain name
- Network Time Protocol (NTP) server IP address

In addition, you must obtain the appropriate virtual ExtremeControl engine license prior to adding the engine on the Control > **Access Control** tab of Extreme Management Center. When you add the virtual engine, you 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.)

Configuring the ExtremeControl Engine

To configure the virtual engine to run the ExtremeControl software:

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

    The following screens display:

```
===============================================================
======
Welcome to Extreme Networks Access Control Engine 8.5.0.xxx
controlengine login: root
===============================================================
======
Extreme Networks Access Control Engine 8.5.0.xxx 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:
```

2. Press [Enter] to begin the setup.

   The **Root Password Configuration** screen appears:

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

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

3. Press [Enter] to set a new root password. Enter the new password as prompted.
Enter new UNIX password:
Retype new UNIX password:
Password updated successfully.

4. In the 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.O]:
Enter the gateway address [192.168.2.1]:
Enter the IP address of the name server (Optional):
Enter the domain name for <hostname> (Optional):
Enter the IP address of the   Server (Required):

5. In the **SNMP Configuration** screen, enter the requested information for each line and
   press **[Enter]**.
**===
======**
SNMP Configuration
**===
======**
**The following information will be used to configure SNMP
management of this device. The SNMP information entered here must**

be used to contact this device with remote management applications
such as Extreme Management Center 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:
Extreme Management Center 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, see your vSphere client documentation.

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

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

Note:

When you add the virtual engine to Extreme Management Center, 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 Extreme Management Center, and cannot be enforced. You can view the engine license status in the **Administration > Diagnostics > Server > Server Licenses** tab in Extreme Management Center.

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 Extreme Management Center or the vSphere client

Console tab to make the changes.

Using the Access Control tab

Use the **Access Control** tab to easily change 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. Click 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. Click the ExtremeControl engine
3. Select the right-panel **Details** tab.
4. In the Interface Summary section, click **Edit** to open the **Interfaces window** where you can change the engine hostname and default gateway.

5. Click **Save**.

6. In the Interface Summary section, click **Static Routes** to open the <u>**Static Route**</u> <u>**Configuration** window</u> where you can add or edit the static routes used for advanced routing configuration.

Using the vSphere Client Console Tab

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

Changing the Extreme Management Center Server IP Address

To change the IP address of the Extreme Management Center server, enter the following command at the login prompt in the **Console** tab:
```
/opt/nac/configMgmtIP <IP address>
```

Enter the following command to start using the new Extreme Management Center server:
```
nacctl restart
```

Changing Web Service Credentials

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

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

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

Enter the following command to restart the engine:
```
nacctl restart
```

Changing the Engine IP Address and Basic Network Settings

To change the engine IP address, as well as basic network settings such as hostname and SNMP configuration (including system contact, system location, trap server, SNMP trap community string, SNMP user, SNMP authentication, and SNMP privacy credentials), enter the following command at the login prompt in the **Console** tab:
```
/usr/postinstall/nacconfig
```

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

Changing Date and Time Settings

To enable or disable NTP for engine date and time, or to manually set the date and time on the engine, enter the following command at the login prompt in the **Console** tab:
```
/usr/postinstall/dateconfig
```

This will start the date and time configuration script and allow 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 the vSphere client documentation for instructions on creating a snapshot.

Reinstalling ExtremeControl Engine Software

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

If you do not have an engine snapshot to restore, you must re-deploy and reconfigure the ExtremeControl virtual engine following the instructions in 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

Once 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

In addition, you must obtain the appropriate Extreme Management Center software license(s) prior to launching the Extreme Management Center applications. You will be prompted to enter a license for any unlicensed application that is launched. (When you purchased Extreme Management Center, 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.)

Configuring the ExtremeAnalytics Engine

To configure the virtual engine to run the ExtremeAnalytics application:

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

   ```
   ============================================================
   Extreme Networks, Inc. - Application Analytics Engine -
   Welcome to the Application Analytics Engine 8.5.0.xxx
   Setup
   ============================================================
   Please enter the information as it is requested to
   continue with the configuration. Typically a default value
   is displayed in brackets.
   Pressing the [enter] key without entering a new value will
   use the bracketed value and proceed to the next item.
   If a default value cannot be provided, the prompt will
   indicate that the item is either (Required) or (Optional).
   The [enter] key may be pressed without
   entering data for (Optional) items. A value must be
   entered for (Required) items.
   At the end of the setup process, the existing settings
   will be displayed and opportunity will be provided to
   correct any errors.
   ============================================================
   Press [enter] to begin setup or CTRL-C to exit:
   ```

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

   ```
   ============================================================
   Root Password Configuration
   ============================================================
   There is currently no password set in the system
   administrator account (root). It is recommended that you
   set one that 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 appears 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 appears. 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 may not be able to log in to the Extreme Management Center 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 appears 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 appears. 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  Extreme Management Center
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 appears 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 appears 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 at step 17.

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

```
================================================================
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 appears. 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 appears. This screen summarizes the settings you have
    entered and provides an opportunity to modify the settings, if desired. Enter **0** to
    accept the settings.

```
============================================================
Modify Settings
============================================================
All of the information needed to complete the installation
of the ExtremeAnalytics Appliance has been entered. Enter
0 or any key other than a valid selection to continue. If
```

```
you need to make a change, enter the appropriate number
from the choices listed below.
===========================================================
0. Accept settings and continue
1. Set the root user password
2. Set the host and network settings
3. Set SNMP settings
4. Set the system time
5. Modify all settings

Enter selection [0]:
```

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

```
===========================================================
Extreme Networks - ExtremeAnalytics Appliance - Setup
Complete
===========================================================
Setup of the ExtremeAnalytics Appliance is now complete.

The appliance is now operational and ready to accept
remote connections.

Details of the installation are located in the
/var/log/install directory.
===========================================================
```

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

Launching the ExtremeAnalytics Application

Now that you have configured the ExtremeAnalytics appliance, you are ready to access the Extreme Management Center Launch Page and run ExtremeAnalytics from a remote client machine.

1. Open a browser window on the remote client machine and enter the Extreme Management Center Launch page URL in the following format:
   `http://<servername>:8080/.`
   where *servername* is the Extreme Management Center server IP address or hostname, and 8080 is the required port number. For example: `http://10.20.30.40:8080/.`

2. On the Extreme Management Center Launch Page, click **OneView.**
   Note: The first time you attempt to launch an Extreme Management Center application, you will be prompted for the license text you received when you generated your Extreme Management Center product license.

3. At the login window, enter your Extreme Management Center user name and password.

4. On the **Management Center** screen, click **Analytics** at the top of the screen.

5. Click **Dashboard.**
   The Dashboard tab displays.

Adding the ExtremeAnalytics Engine

To add the ExtremeAnalytics engine to ExtremeAnalytics:

1. Select the **Analytics Configuration** tabAnalytics 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 ExtremeAnalytics engine

4. From the **Profile** list, select the appropriate SNMP profile.

5. Click **OK.**

6. Open the drop-down list below Overview and select **Enforce Engine**.

Changing ExtremeAnalytics Engine Settings

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

Changing Basic Network Configuration

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

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

Changing SNMP Configuration

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

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

Changing Date and Time Settings

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

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

Changing the ExtremeAnalytics Server IP Address

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

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

Changing the Web Service Credentials

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

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

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

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

Upgrading ExtremeAnalytics Engine Software

Upgrades to the Extreme Management Center engine software will be made available from the Network Management Suite (NMS) Download webpage.

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

1. On a system with an Internet connection, go to the Network Management Suite (NMS) Download web page:
   http://extranet.extremenetworks.com/downloads/pages/NMS.aspx.

2. After entering your email address (username) and password, follow this path to the download page: **Visibility & Control > Network Management Suite (NMS) > Software > select a version**.

3. Download the following ExtremeAnalytics virtual engine file from the NMS Downloads section:
   `purview_appliance_upgrade_to_version.bin`

4. Use FTP, SCP, or a shared mount point, to copy the file to the ExtremeAnalytics virtual engine.

5. SSH to the engine.

6. Cd to the directory where you downloaded the files.

7. Change the permissions on the upgrade file by entering the following command:
    `chmod 777 purview_appliance_upgrade_to_version.bin`

8. Run the install program by entering the following command:
    `./purview_appliance_upgrade_to_version.bin`
    The upgrade automatically begins. You are notified when the upgrade completes.

Reinstalling ExtremeAnalytics Engine Software

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

If you do not have an engine snapshot to restore, you will need to re-deploy and reconfigure the ExtremeAnalytics virtual engine following the instructions in 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.