Enterprise Secure Key Manager

virtual Enterprise Secure Key Manager v8.50.0

Deployment Guide

utimaco®

Imprint

Copyright 2022	Utimaco IS GmbH
	Germanusstr. 4
	D-52080 Aachen
	Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226)
	EMEA +49 800-627-3081
	APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	8.50.0
Date	2023-04-26
Status	
Document No.	2021-0048

Table of Contents

1 About this guide

This guide provides information about:

- Deploying a virtual Enterprise Secure Key Manager
- Configuring a virtual Enterprise Secure Key Manager
- Administering security keys
- Administering CA, server, and client certificates

1.1 Intended audience

This guide is intended for system administrators with knowledge of:

- Data security administration
- Network configuration

1.2 Related documentation

The following documents provide related information:

- Enterprise Secure Key Manager v8.50.0 User Guide
- Enterprise Secure Key Manager v8.50.0 Release Notes

1.3 Document conventions and symbols

Table 1: Document conventions and Symbols

Convention	Element
Blue text: Run the Setup utility (p. 32)	Cross-reference links and Email addresses
Blue, underlined text: https://www.utimaco.com	Website addresses

Bold text	Keys that are pressed Text typed into a GUI element, such as a box GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes
Italic text	Text emphasis
Monospace text	File and directory names System output Code Commands, their arguments, and argument values
Monospace, italic text	Code variables Command variables
Monospace, bold text	Emphasized monospace text

Indicates that failure to follow directions could result in bodily harm or death.

Indicates an action that can have consequences such as deletion of keys or changes to security settings.

Provides clarifying information or specific instructions.

Provides additional information.

1.4 Utimaco Technical Support

For technical questions, contact Utimaco Technical Support:

- E-mail: support-atalla@utimaco.com[1]
- Telephone: 800-500-7858 (U.S.A.) +1-916-414-0216 (International)
- Website: https://support.utimaco.com/

Before contacting Utimaco, collect the following information:

- Product model names and numbers
- Service Agreement ID number (SAID)/Subscription
- Product serial numbers
- Error messages
- Software version number
- Detailed questions

24-hour emergency support is available to those customers who have valid service contracts. Use this service for product and system emergencies that occur after normal working hours or on weekends and U.S. holidays. Questions about product installation and setup are supported during normal working hours.

For 24-hour emergency support call: 800-500-7858 (U.S.A.), +1-916-414-0216 (International)

1.5 Utimaco websites

For additional information, see the following Utimaco websites: https://www.utimaco.com/

1.6 Documentation feedback

Utimaco welcomes your feedback. To make comments and suggestions about product documentation, please send an email message to: support-atalla@utimaco.com[2]

All submissions become the property of Utimaco.

1 mailto:support-atalla@utimaco.com
2 mailto:support-atalla@utimaco.com

2 Deploying vESKM

2.1 Introduction

Utimaco's virtual Enterprise Secure Key Manager (vESKM) is a versatile, trusted and scalable virtual key manager that securely manages encryption keys across the enterprise. The vESKM implements native protocol KMS (Key Management Service) or industry-standard OASIS KMIP (Key Management Interoperability Protocol) for its client integrations.

The more data you protect, the more dependent you are on encryption keys. True enterprise key management enables uniform, consistent key protection and policy management across mixed environments. A virtual key manager can be quickly deployed and integrated with a remote HSM, providing a secure root of trust for compliance.

This chapter explains how to deploy a virtual ESKM under different hypervisors (VMware via the vSphere client, HyperV and KVM).

2.1.1 Recommended minimum system configuration

- VMware vCenter version 6.5 or later
- 140 GB hard disk space
- 4GB RAM
- 2 vCPU
- Setup Virtual Network Adapter (Hyper V)

This configuration supports up to 100K KMS keys or 25K KMIP keys. To support more keys, the configuration must be updated by adding more resources (CPU or RAM).

2.2 Deploy OVF Template using VMware vSphere client

This section details the steps for deploying vESKM OVF Template via VMware vSphere client:

The version of vCenter used in the example below is 6.5.

Please perform the following steps to deploy an OVF template via vSphere web client:

1. Navigate to vSphere web client by entering the IP address (https:// IP address of the vCenter) and login with administrative credentials.

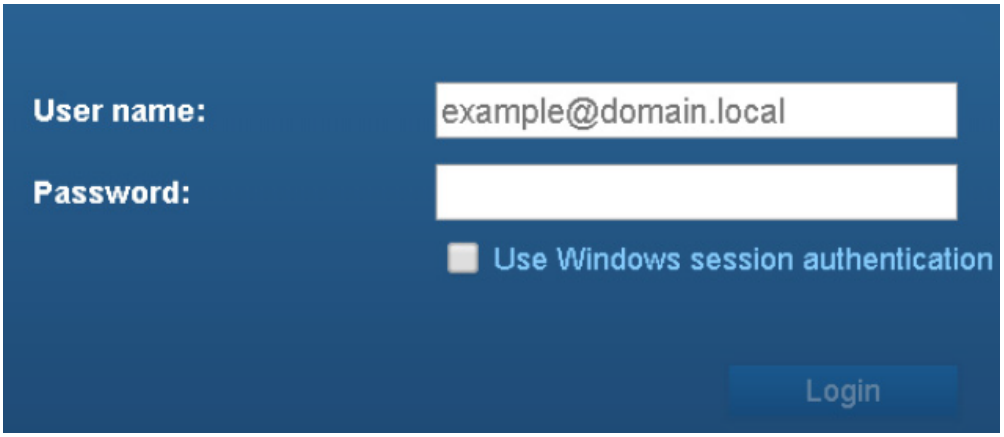


Figure 1 : Login to vSphere web client

2. Once logged in, click on **vCenter > vCenter Servers**.

3. Right-click on the **vCenter server**, highlight **All vCenter Actions** and click on **Deploy OVF Template**.

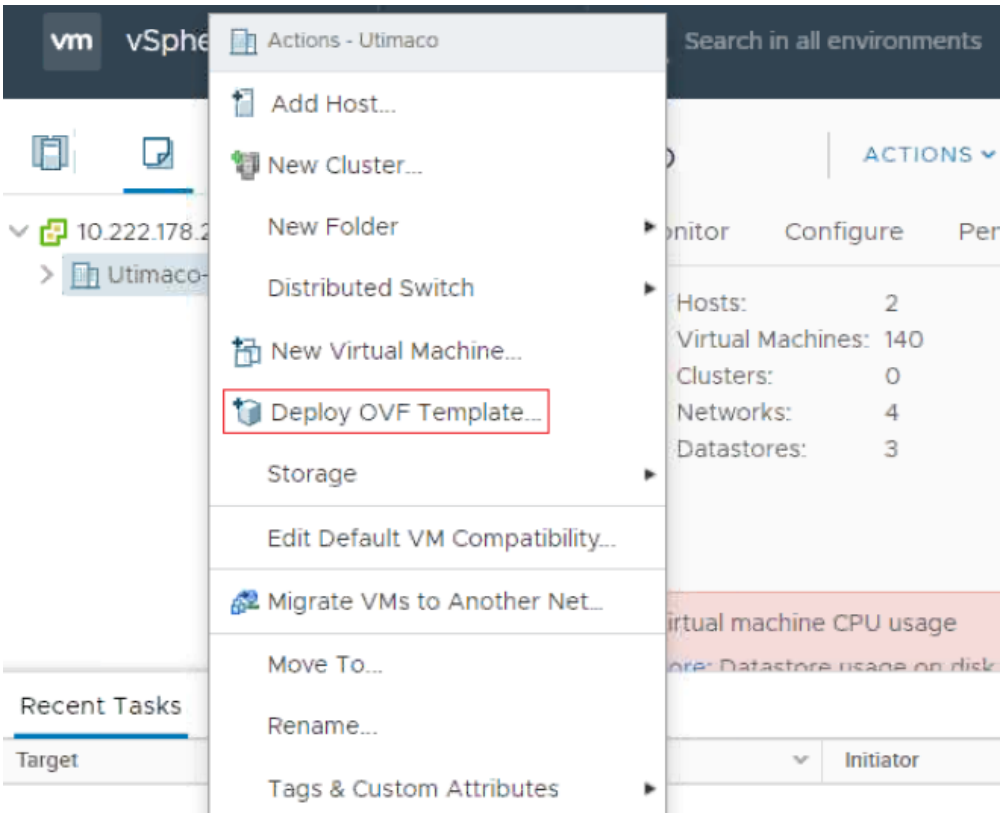


Figure 2 : Deploy OVF Template

4. If this is the first time you are running the VMware Client Integration Plug-In, a window will appear. Click **Allow**.

5. The next window will prompt you to select your OVA file. Click on **Browse** and select the **vESKM version 8.50.0** OVA file. Click **Next.**

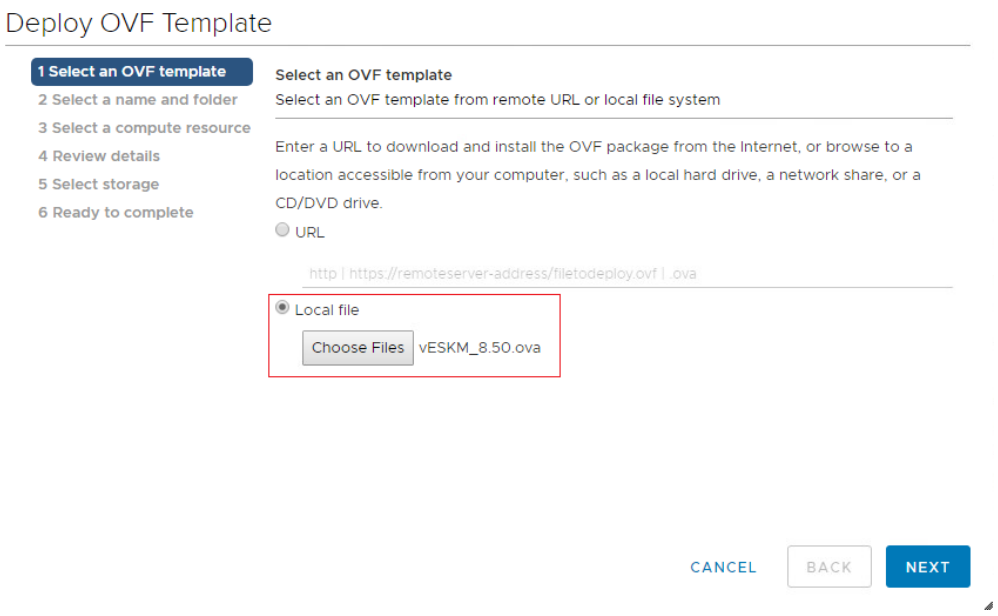


Figure 3 : Select an OVF Template

6. Now, you will be prompted to select a VMware folder and to name the virtual machine. Once done, Click **Next.**

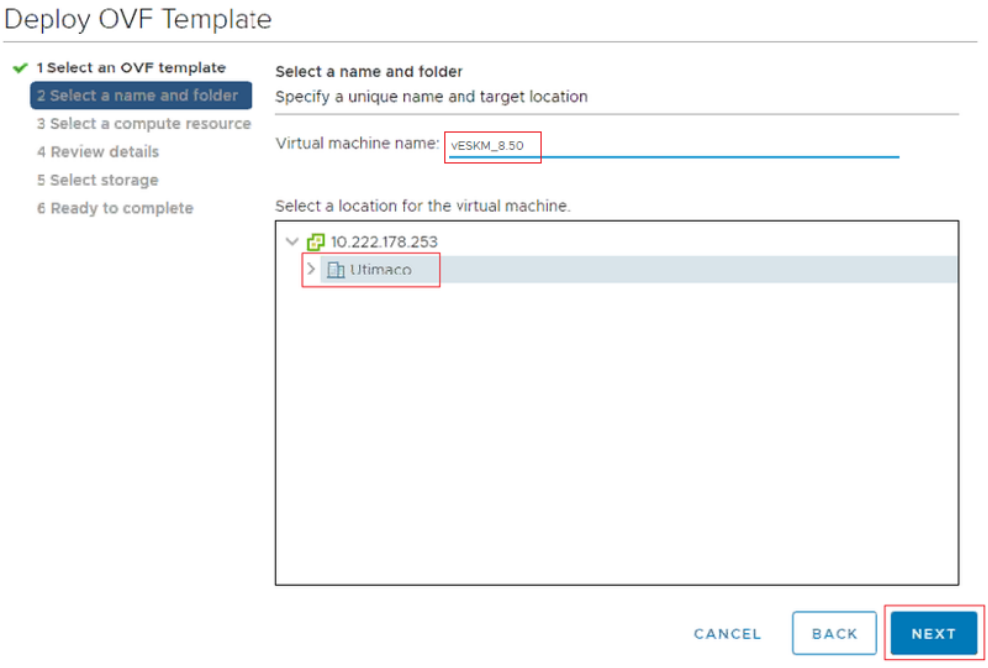


Figure 4 : Select VMware Folder

7. Select an ESXi host and click **Next.**

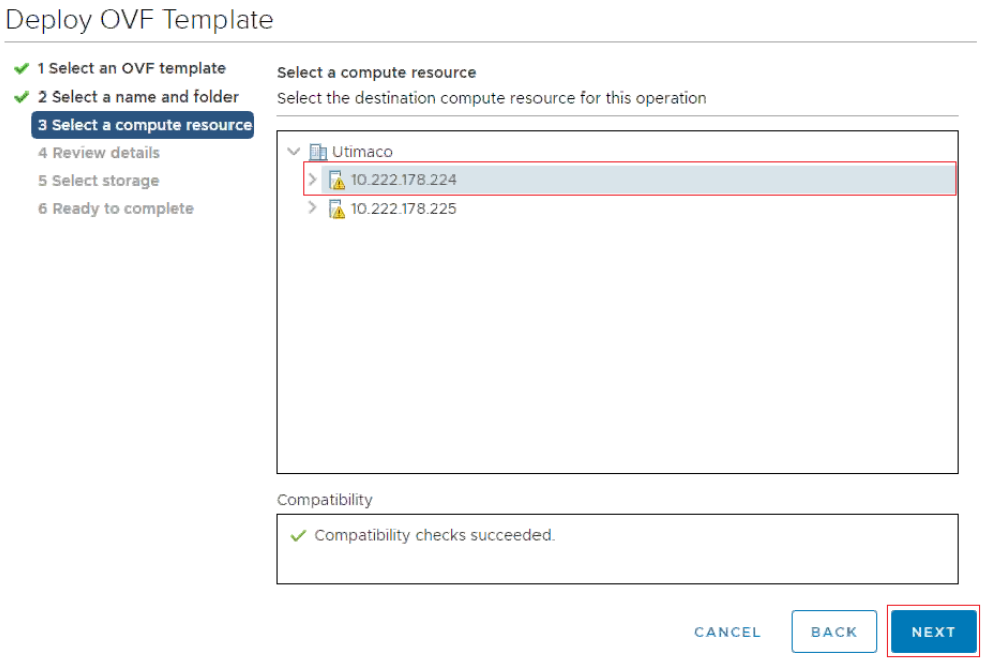


Figure 5 : Select the destination

8. The OVF template details will appear in the following window. Verify the details and click **Next**.

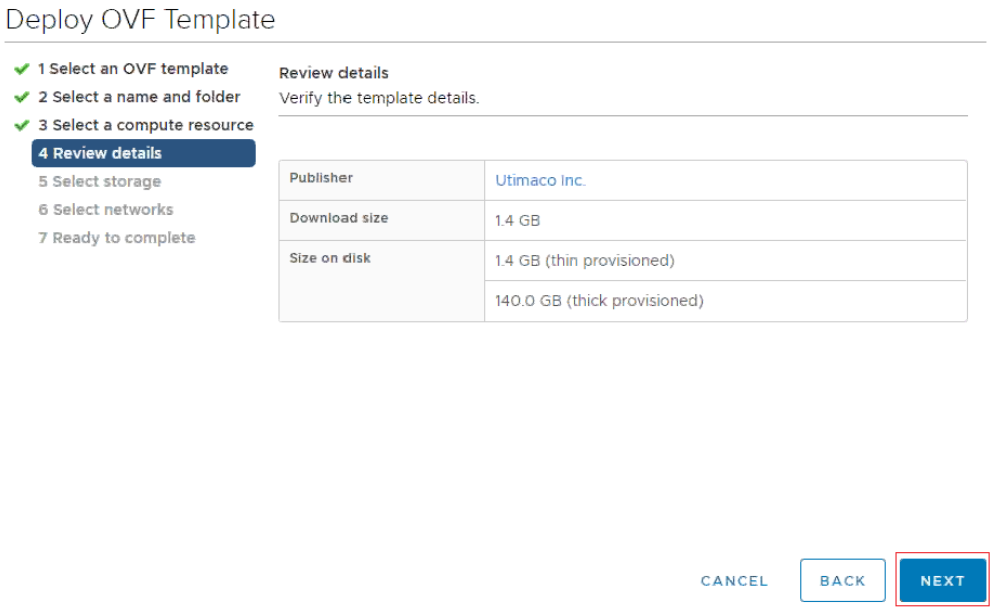


Figure 6 : Review Details

9. Select both the virtual disk format, and the Datastore for deployment. Click **Next**.

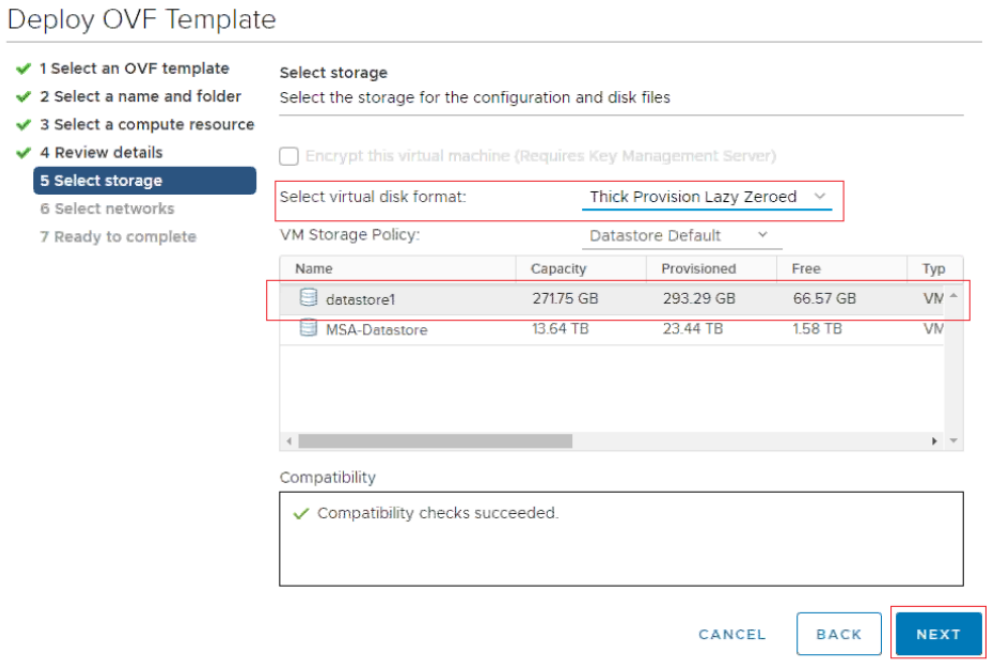


Figure 7 : Select storage

10. Select a network to manage the virtual appliance and click **Next**.

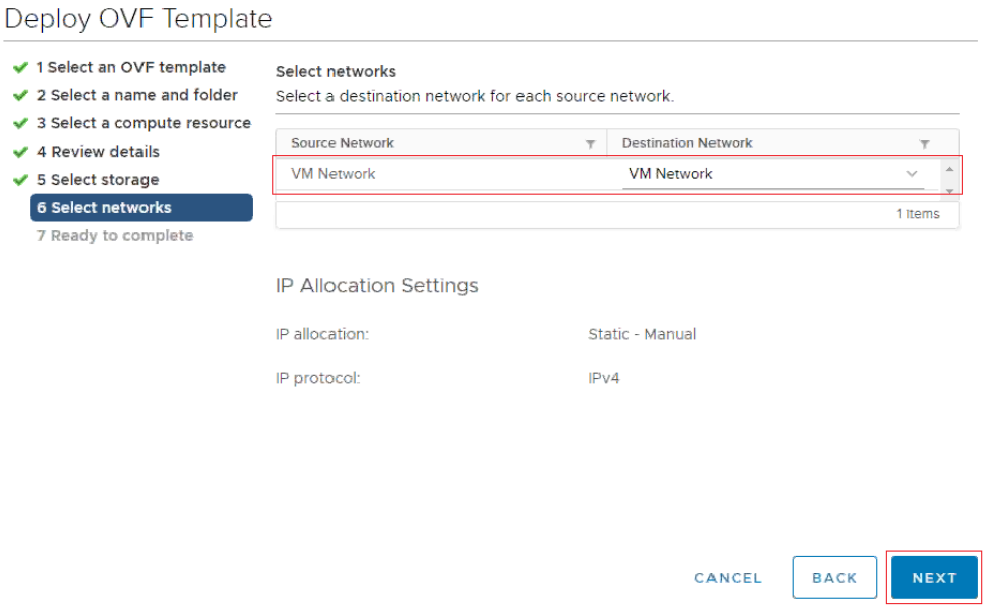


Figure 8 : Select networks

11. The Deploy OVF Template window will summarize all options selected for deployment. Click **Finish** to begin the deployment of the virtual appliance.

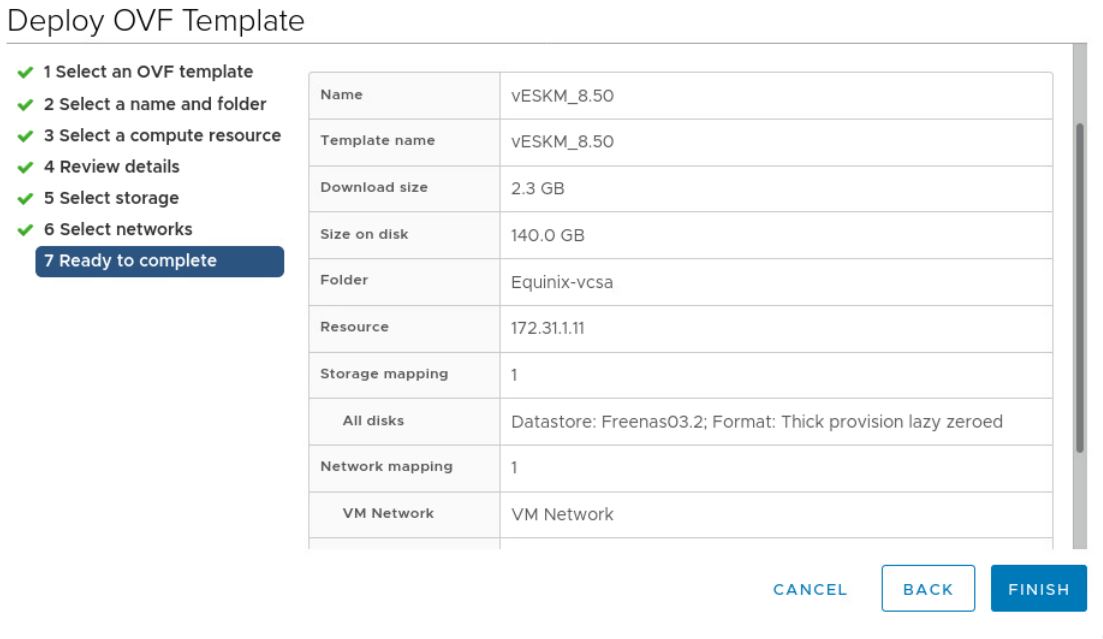


Figure 9 : Ready to complete

After the deployment has completed, vESKM can be configured. See Configuring the vESKM server (p. 8) for more details.

2.3 Deploy ESKM using Hyper V Manager

This section provides steps to deploy ESKM application via Hyper V manager.

Before deploying the ESKM machine, ensure that the Hyper V Manager is installed on the windows system and that the zipped ESKM application package has been unzipped and saved in the correct location.

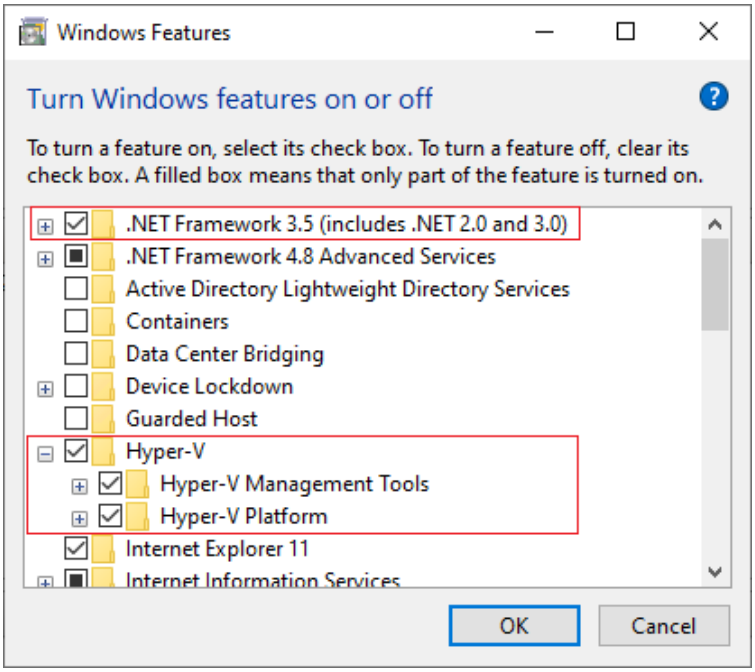
2.3.1 Enable the Hyper-V machine Settings

1. Right click on the windows button and select "**Apps and Features**".

2. Select "**Programs and Features**" on the right under related settings.

3. Select "**Turn Window feature on or off**".

4. Select **.NET Framework 3.5 (includes .NET 2.0 and 3.0) and Hyper-V**. Click **OK**.



Perform the following steps to deploy ESKM via Hyper V Manager:

1. From the **Actions** menu in the **Hyper V Manager**, select **Import Virtual Machine**.

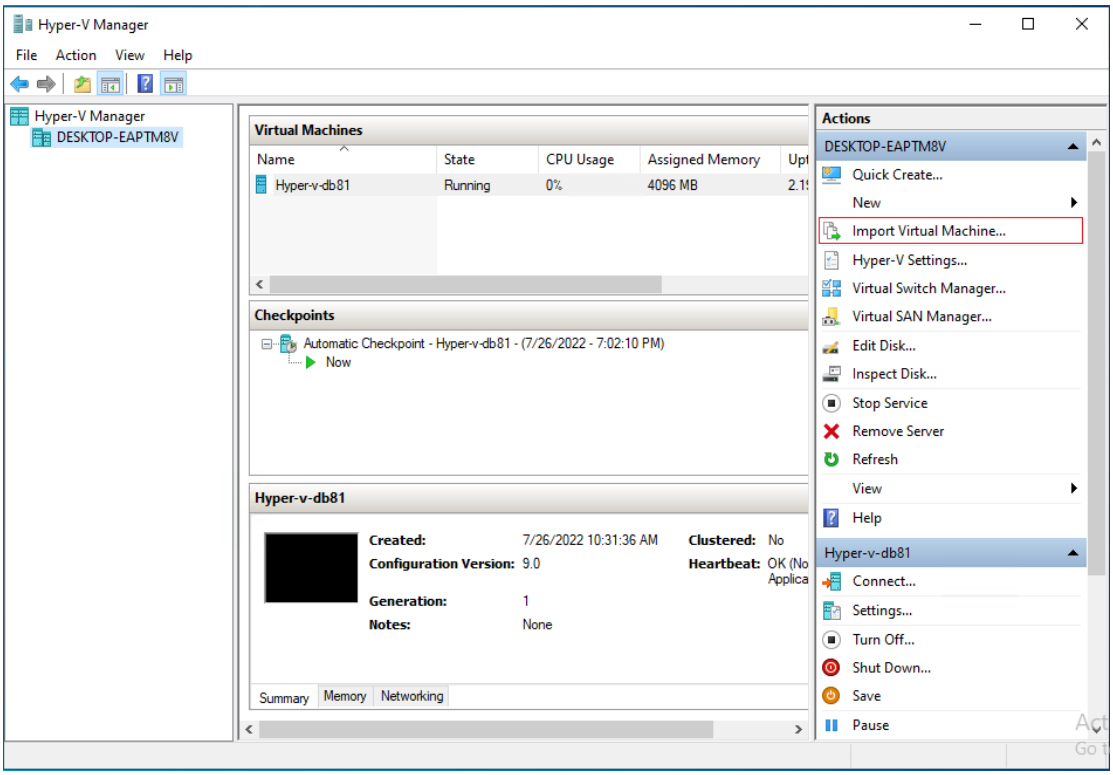


Figure 10 : Import Virtual Machine

2. The **Import Virtual Machine wizard** will appear. Click **Next**.

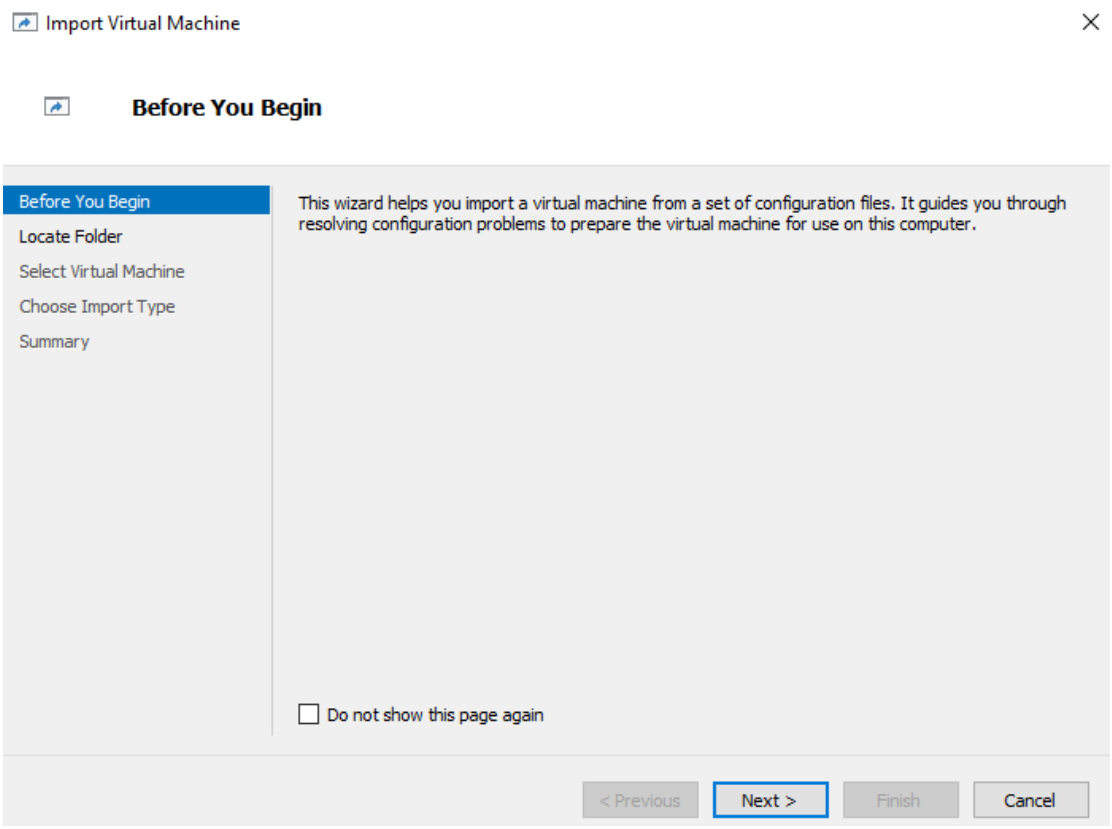


Figure 11 : Before you Begin

3. Now, you will be prompted to select the folder that contains unzipped ESKM application package. Click **Next**.

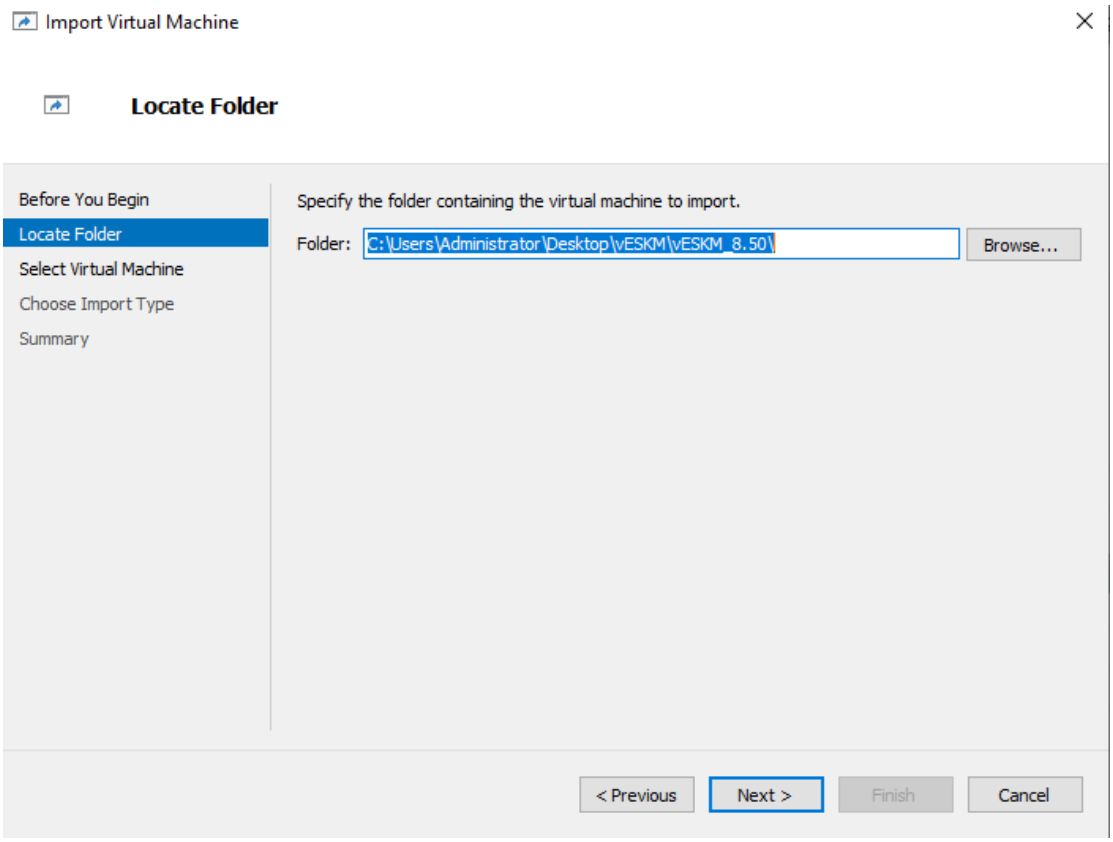


Figure 12 : Locate Folder

4. In the **Select Virtual Machine** wizard, the selected virtual machine is displayed. Click **Next**.

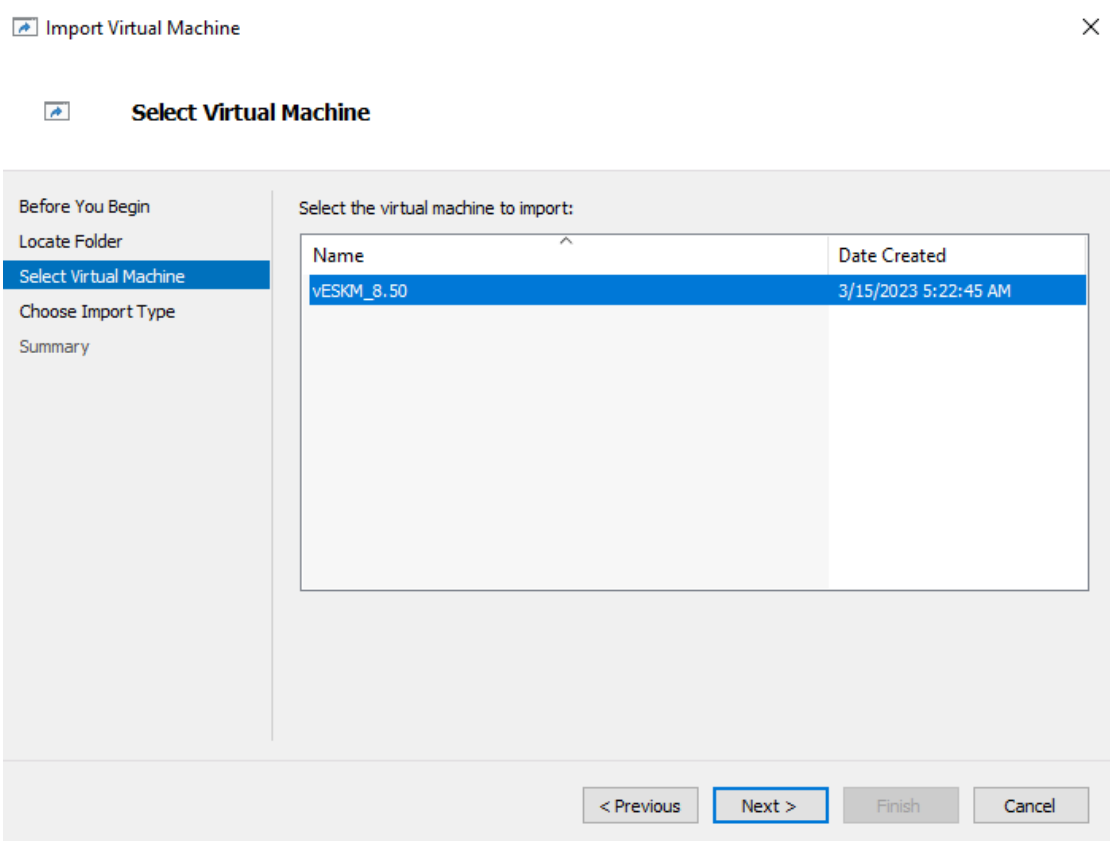


Figure 13 : Select Virtual Machine

5. Choose import type as "**Copy the virtual machine (create a new unique ID)**" option. Click **Next**.

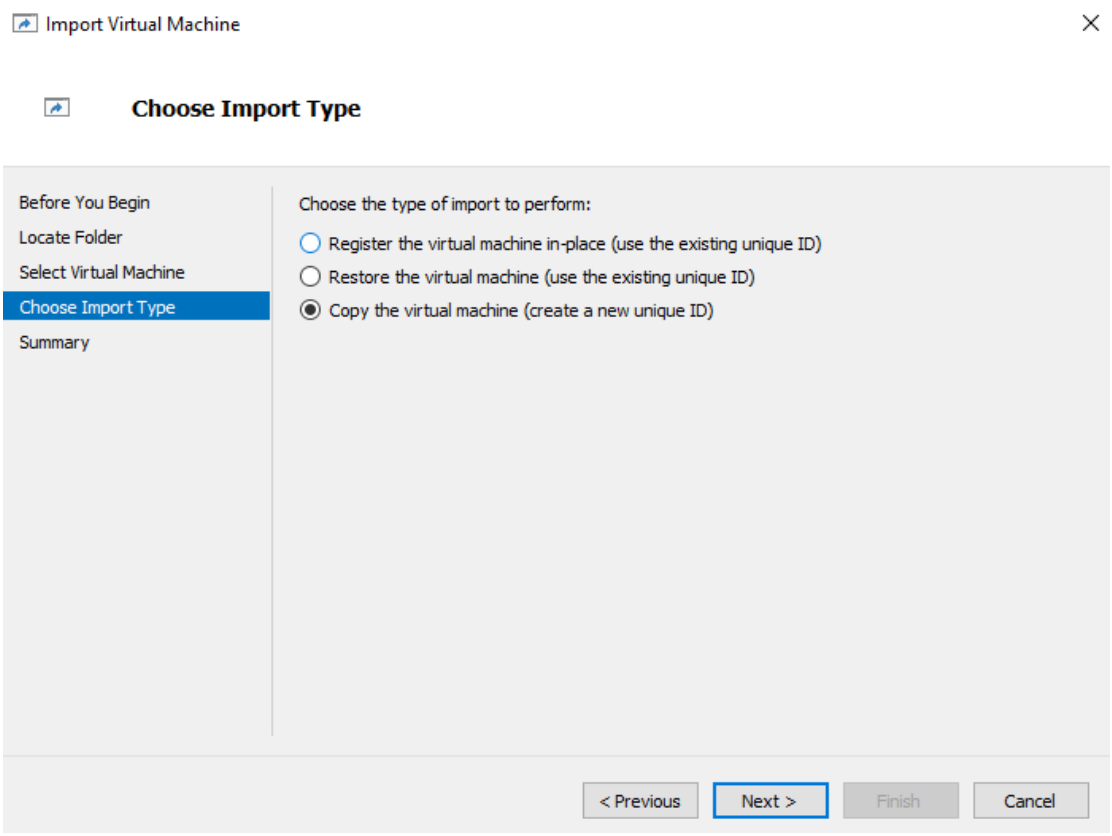


Figure 14 : Choose Import Type

6. In the **Choose Folders for Virtual Machine Files** wizard, select **Store the virtual machine in a different location** checkbox to store the individual components of the virtual machine in a difference locations. Click **Next**.

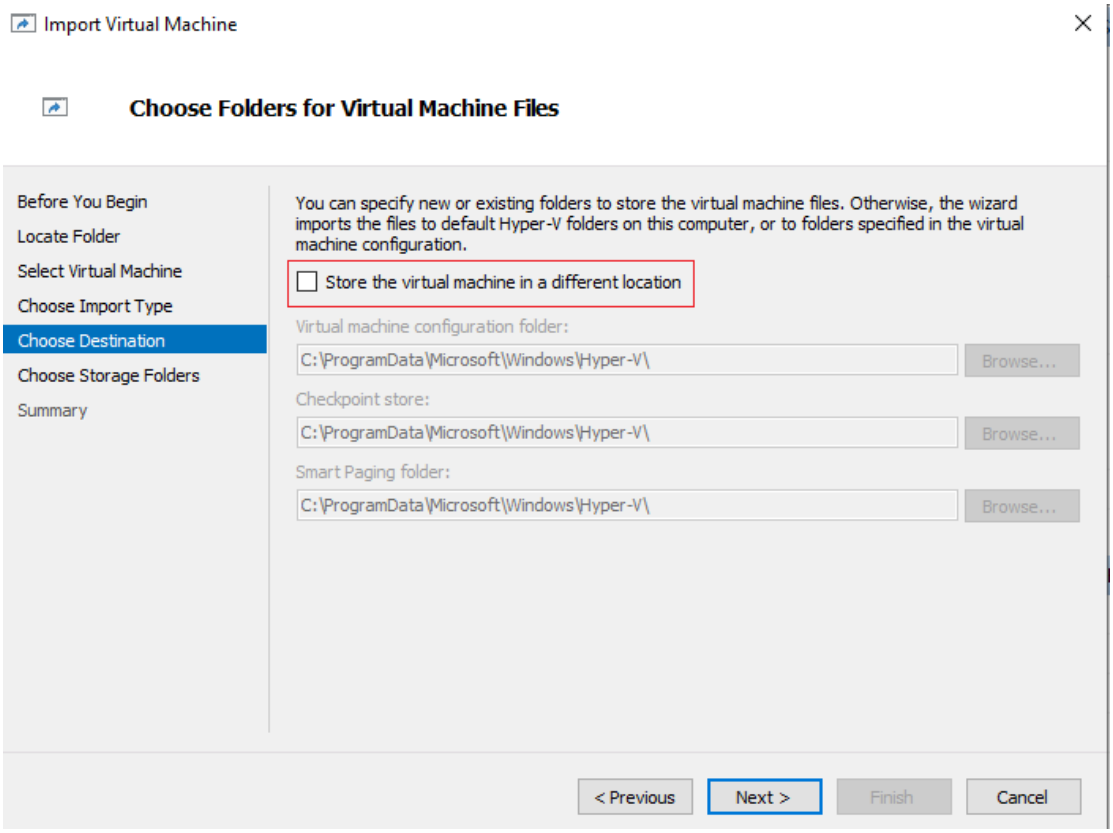


Figure 15 : Choose Destination

7. In the **Choose Folders to Store Virtual Hard Disks** wizard, select the location where you want to store virtual hard disks. Click **Next**.

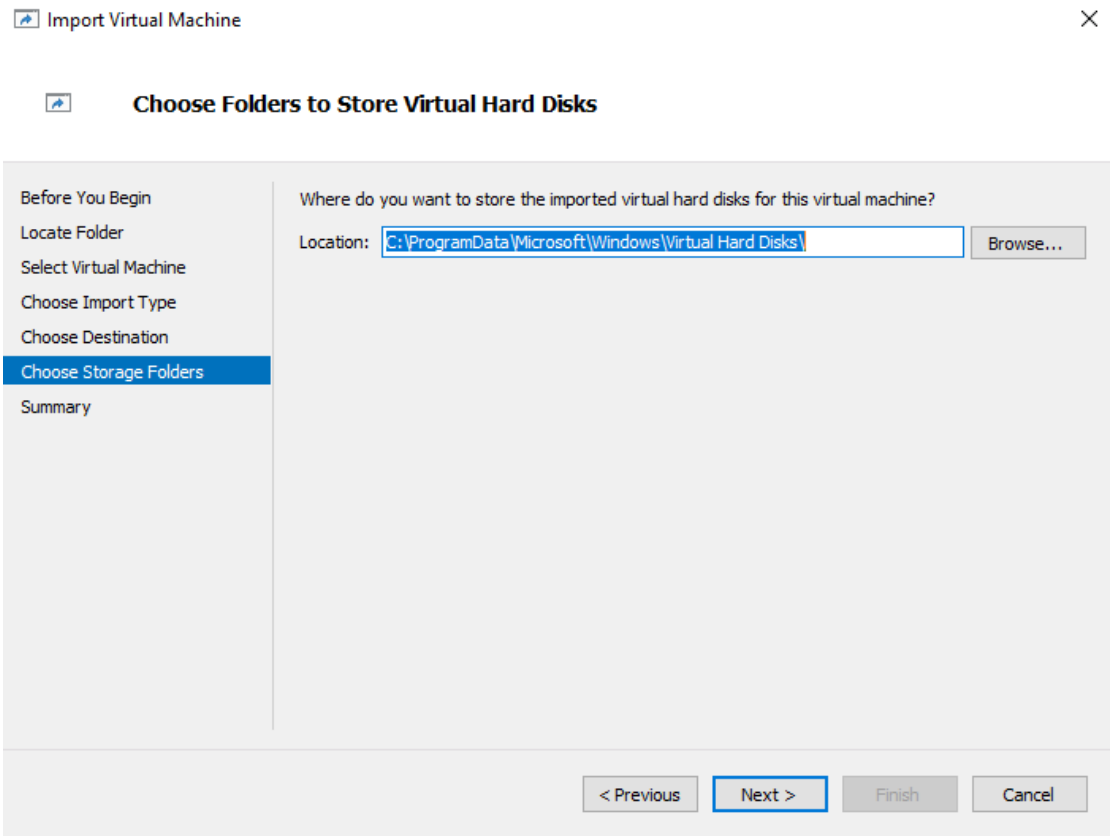


Figure 16 : Choose Folders to Store Virtual Hard Disks

8. The Import Virtual Machine window will summarize all options selected for the ESKM application deployment in Hyper V machine. Click Finish to begin the deployment of the virtual machine.

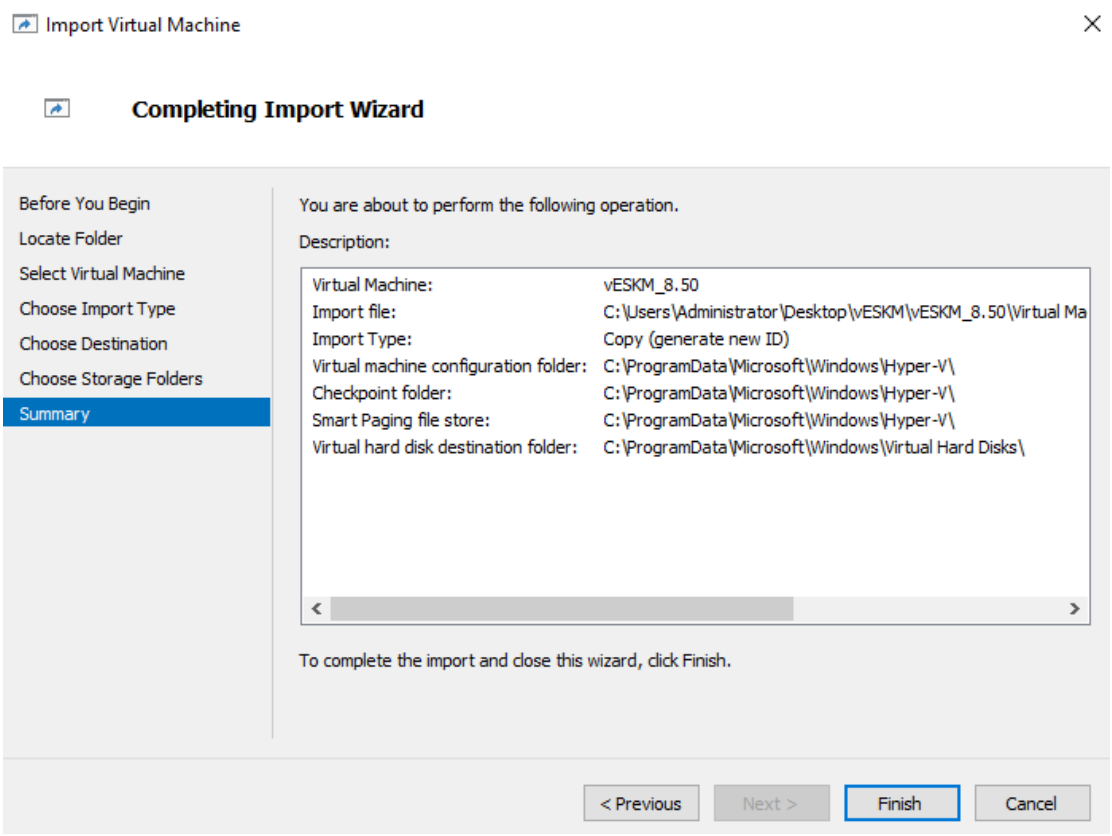


Figure 17 : Completing Import Wizard

After the deployment has completed, ESKM can be configured.

2.4 Deploy ESKM using KVM Machine

This section provides steps to deploy ESKM application via KVM Machine.

Before deploying the ESKM machine, ensure that KVM is enabled, Virtualization Manager components (qemu-kvm, libvirt-daemon, bridge-utils etc.) are installed, and bridge interface is created on the Linux system. Perform the following steps to deploy ESKM via KVM Machine:

ESKM is currently tested with CentOS 8 Stream and Ubuntu.

2.4.1 Extracting the vESKM disk image

1. Import the public key provided with veskm.qcow2.gpg signed image.
   `gpg --import pub.key`

   For example:
   ```
   [user@localhost ~]$ gpg --import veskm.pub
   gpg:key 06C482B0: public key "build" imported
   gpg:Total number processed: 1
   gpg:imported: 1  (RSA: 1)
   ```

2. Verify the sanity of the image, providing the key id obtained from step1.
   `gpg --verify --local-user <key-id> veskm.qcow2.gpg`

3. Get the decrypted disk image from the gpg file.
   `gpg --decrypt --local-user <key-id> veskm.qcow2.gpg > veskm850.qcow2`

*In the example given above, the key id is **06C482B0**, but it will vary and the correct one must be used in subsequent commands.*

2.4.2 Deploying vESKM using Virt Manager UI

1. Copy the **veskm.qcow2 image** to your libvirt's default storage path (**/var/lib/libvirt/images/)**

2. Navigate to the **Virtual Machine Manager,** select **File** > **New Virtual Machine**" to get the New VM window.

3. Select "**Import existing disk image**" and then click **Forward.**

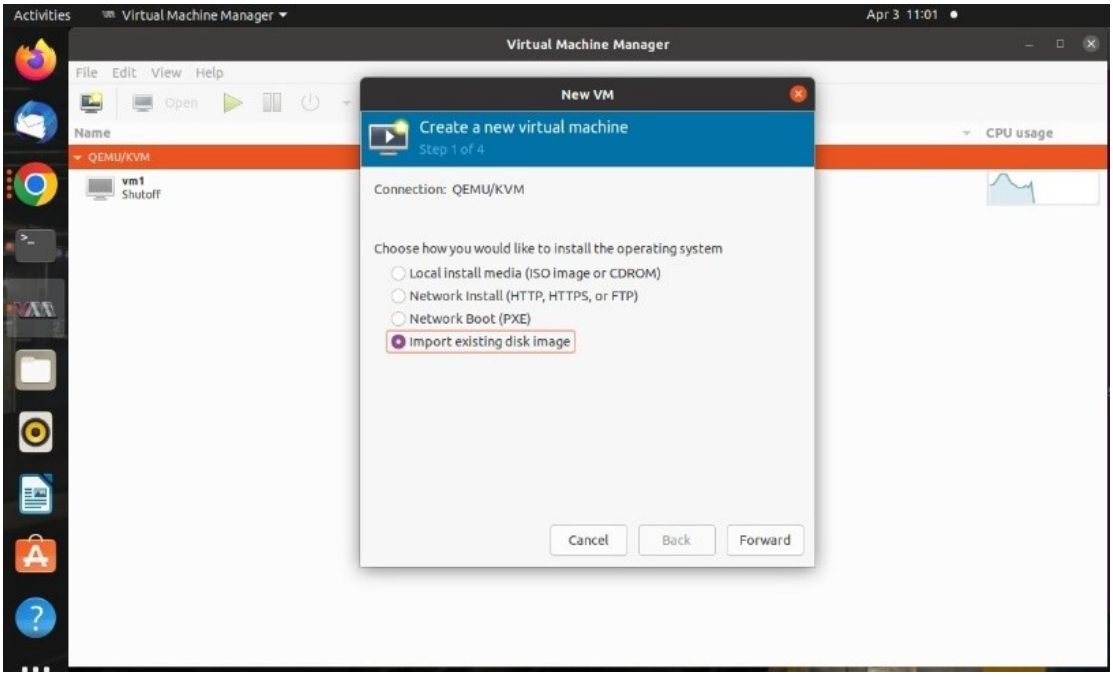


Figure 18 : Import existing disk image

4. Browse to select **vESKM disk image file** and select **Operating System** as "**CentOS 7**", and then click **Forward**.

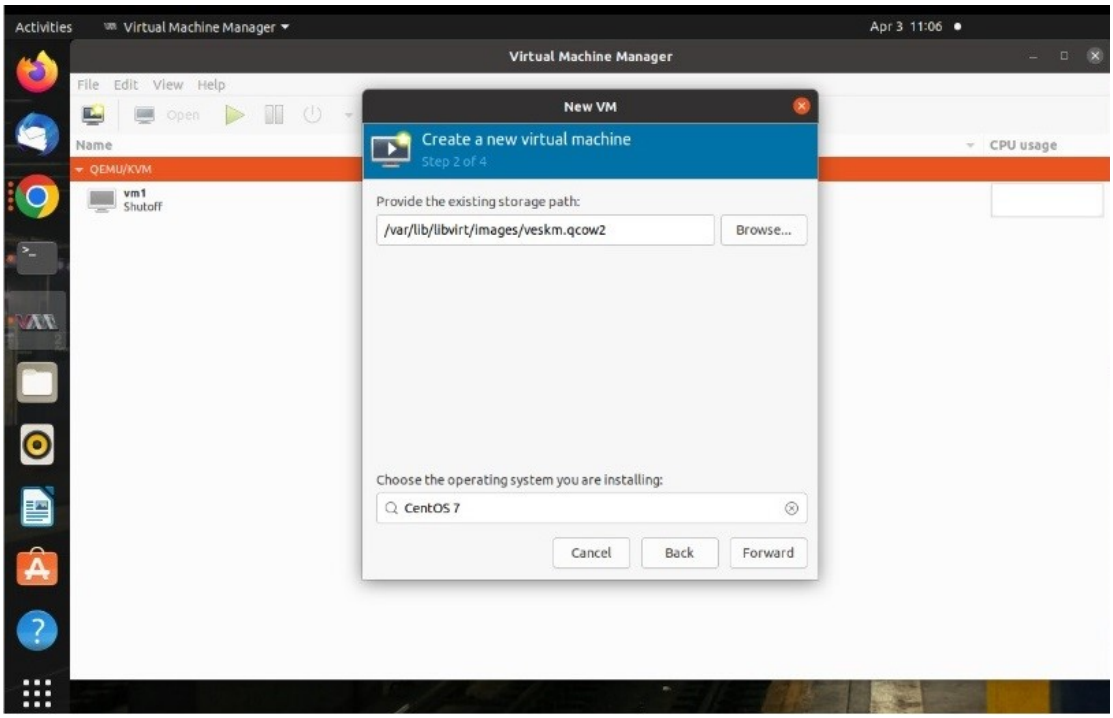


Figure 19 : Existing Storage Path

5. Specify Memory as **4096**, CPUs as **2**, and click **Forward**.

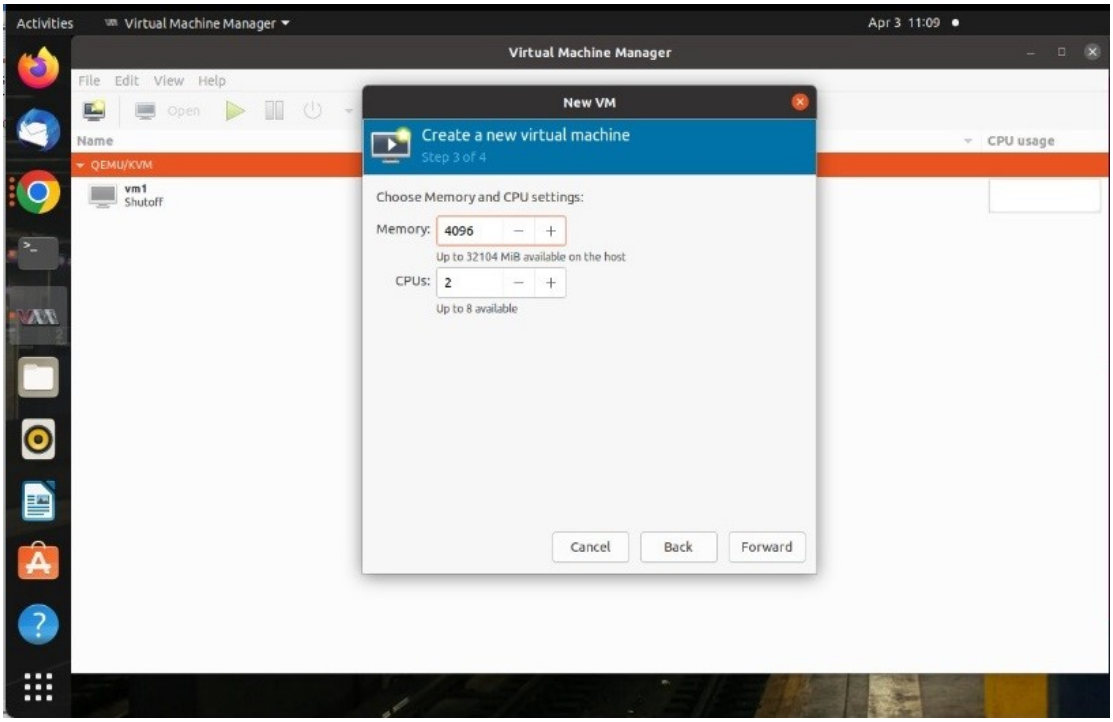


Figure 20 : CPU Settings

6. Change the "**Name**" if necessary, select "**Customize configuration before install**" checkbox, choose the required Network device, and click **Finish**.

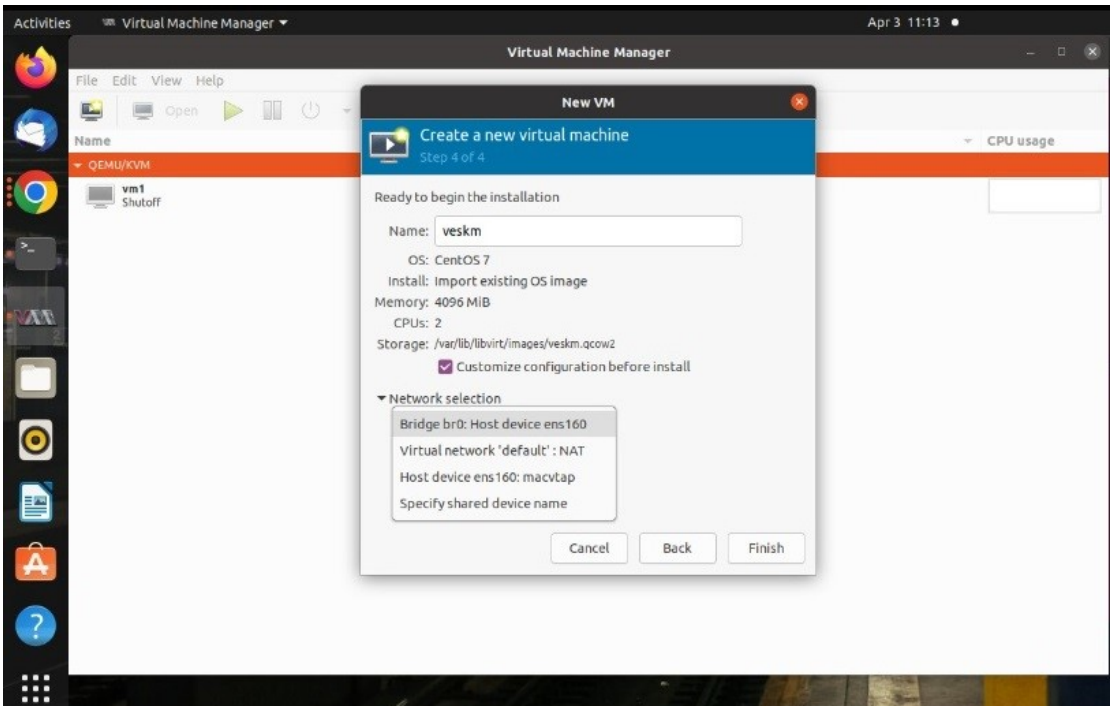


Figure 21 : Customize Configuration

7. The “**veskm on QEMU/KVM**” window appears.

8. In the left pane, click "**Add Hardware**". The “**Add New Virtual Hardware**” window appears.

9. Select "**Controller**" and choose **Type** as "**SCSI**" and **Model** as "**Virtio-SCSI**". Click **Finish**.

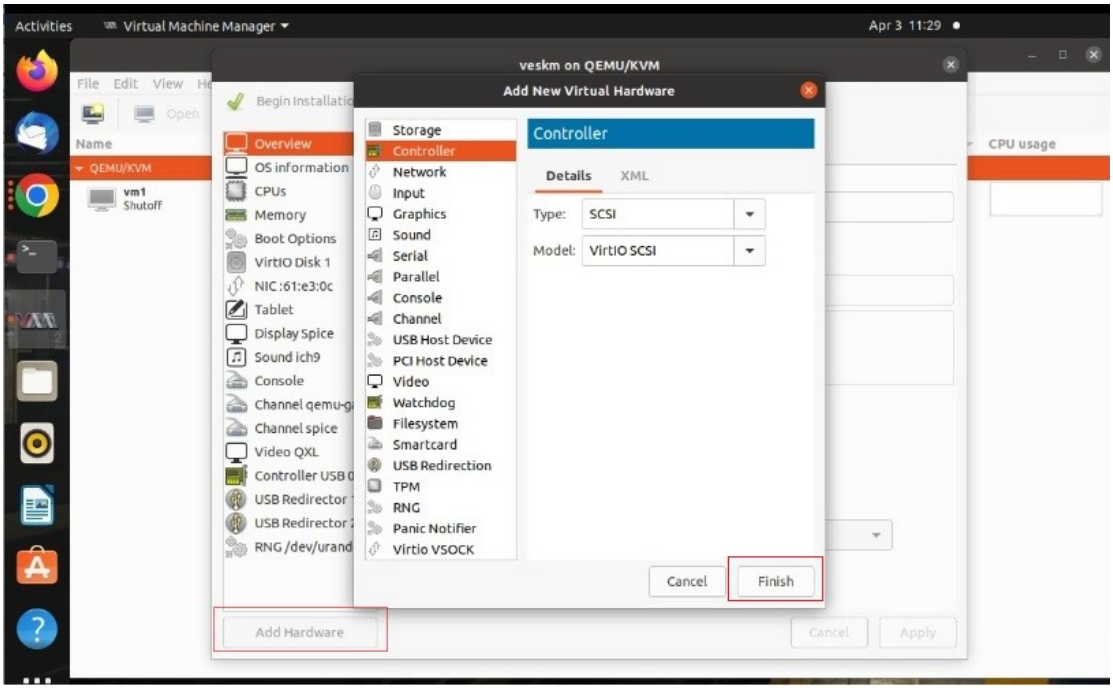
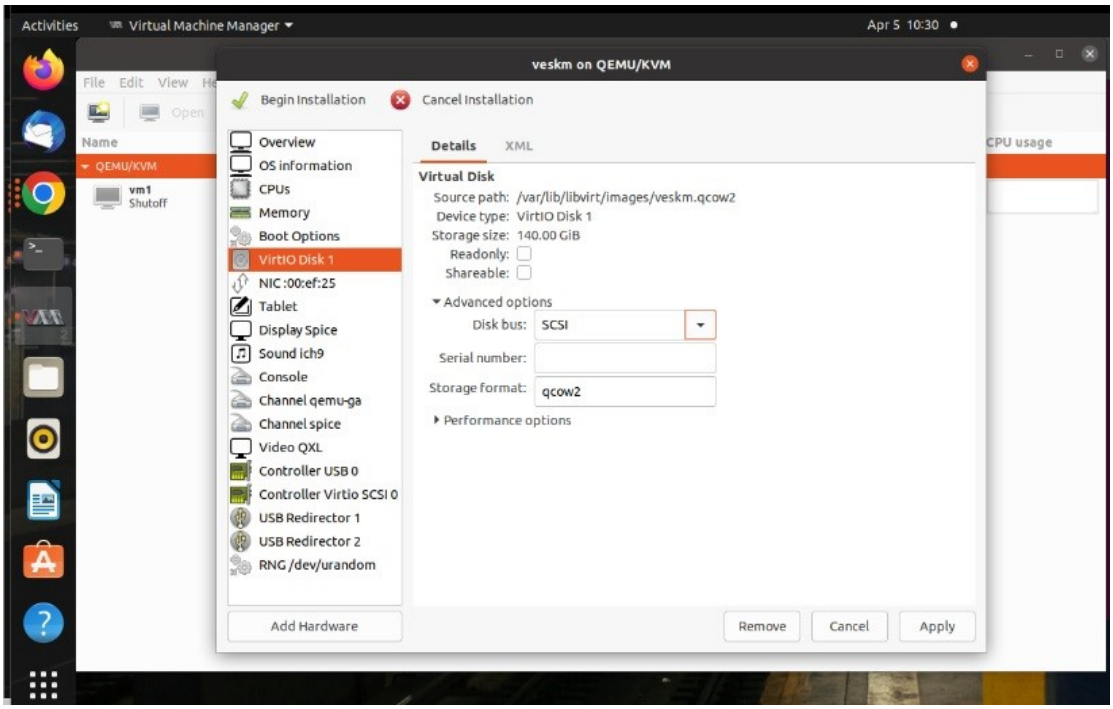


Figure 22 : Add Controller

10. In the left pane, select "**VirtIO Disk1**", click "**Advanced options**" and change "**Disk bus**" to "**SCSI**', and click "**Apply**".



11. Click "**Begin Installation**" at the top left corner of the window to start the ESKM deployment.

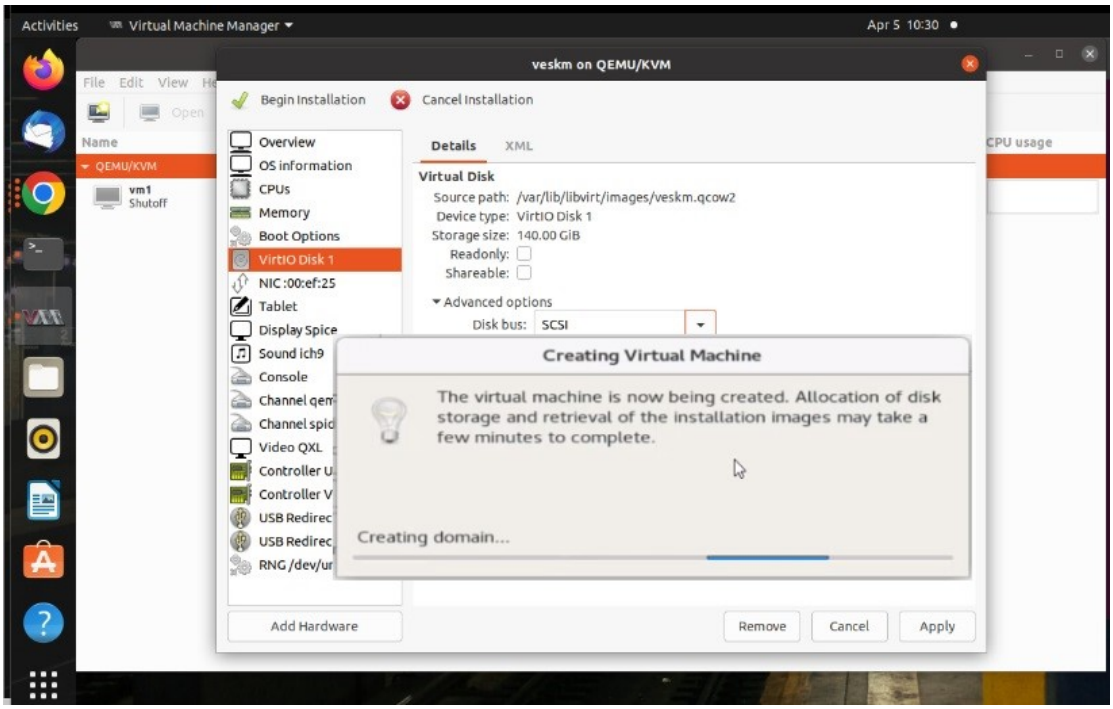


Figure 23 : Creating Domain

12. vESKM will complete disk encryption, reboot, and proceed to the 'Firstrun prompt' - "**Are you ready to begin setup?" (y/halt):** "

2.4.3 Using CLI to deploy the vESKM from disk image:

Extract the disk image by following the steps mentioned in Extracting the disk image (p. 23).

1. Copy the veskm.qcow2 image to your libvirt's default storage path - /var/lib/libvirt/images/

2. Invoke below command providing the disk image path, Network device and other parameters.

```
virt-install --name=veskm --import --disk=/var/lib/libvirt/images/veskm.qcow2,bus=scsi --vcpus=2 --ram=4096 --network bridge=br0 --os-type=Linux --os-variant="centos7.0" --wait 1
```

3 Configuring the vESKM server

On initial power-up of the VM, each vESKM server must be configured with specific values such as time zone, IP address, netmask, gateway, host name, and port number used for the vESKM Management Console interface.

3.1 Run the Setup utility

To configure the time zone, IP address, netmask, gateway, host name, and port number used for the vESKM Management Console interface, the following procedure must be performed once for each vESKM server. Ensure that the vESKM server is powered off before starting this procedure.

1. Power on the vESKM server by right clicking on a VM under the vCenter and navigate to **Power > Power On.**

2. Navigate to the **Summary** tab and click on the **Launch Remote Console** to take the remote control of the VM.

3. When the startup sequence completes, the vESKM will reboot once and the following prompt displays on the VM.
   `Are you ready to begin setup? (y/halt):`

   Enter `y`.

4. Follow the prompts to enter the necessary information:
   Press **Enter** to accept the default.

   - Admin account password. Be sure to record this value and store it in a safe place. The Security Officer will use the admin account to configure the vESKM servers.

Utimaco has no ability to assist or recover access if administrator credentials (username, password) are lost.

- Time zone.
- Date.
- Time. The time is based on a 24–hour clock; there is no a.m. or p.m. designation. For example, 1:20 p.m. is 13:20:00.
- The static IPv4 address of the vESKM server. The vESKM server cannot obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server.
- Subnet mask.
- Default gateway.
- Hostname, including the domain. For example, veskm.example.com. The screen displays the information you entered and the message "`Is this correct? (y/n)`:"

  If the information displayed is correct, enter `y`; if not, enter `n` and make the necessary corrections.
- Enable IPv6. If the vESKM server will be installed in an IPv6 network, enter **y** to the prompt and also the confirmation prompt. If the vESKM server will not be installed in an IPv6 network, or you wish to enable IPv6 later, enter **n**. If you entered **y**, you will be prompted to specify the IPv6 address. If you know the IPv6 address enter y, and then at the next prompt enter the IPv6 address with prefix in this format. `IPv6 address/prefix`. The default prefix is /64.

  If you do not know the IPv6 address, enter `n`. You can enter IPv6 addresses later using either the vESKM Management Console or Command Line Interface.

Only enable IPv6 if you are certain that the vESKM server is required to operate on an IPv6 network. Once enabled it cannot be disabled via the vESKM Management Console or the Command Line Interface.

Client systems can use IPv4 addresses to connect to the KMS and KMIP services running on the vESKM system. vESKM supports IPv6 addresses for clients that use either the KMIP or vESKM XML protocols, and are on the same subnet as the vESKM server. The following vESKM features, which utilize SCP to move files, support IPv6 addresses:

- backup, restore, scheduled backup, transfer logs, and software upgrade/ install

In addition, you can also use a server which has an IPv6 address to perform the following functions:

- remotely administer the vESKM server via the vESKM Management Console or the command line interface
- perform network diagnostics (ping and netstat)

If you decide later, after completing the setup process, that you need to enable IPv6 support, you can use the Command Line Interface command `ipv6 enable`, to enable IPv6. You can then use the `ipv6 address` command or the vESKM Management Console interface to specify the IPv6 address.

- Web interface port number.
- Press **Enter** to complete and save the configuration settings.

At this point, you have given the setup program everything it needs. The vESKM creates SSH keys and also a self-signed Web Admin server certificate. They are used to authenticate the vESKM to users making SSH and Web Admin connections to the vESKM.

```
Creating certificate for Web administration server...
Creating certificate for signing logs...
Creating SSH host keys...
SSH RSA key fingerprint:
2048 SHA256:aTp6A447vp8dOj43FTT5B/aux6V7zddPzNXxZB0C1SE
SSH ECDSA key fingerprint:
521 SHA256:BKO/EfVUKSFpIzVn/WiJ4fS+8CqLyGJSawoQAsvmUoM
```

```
SSH ed25519 key fingerprint:
256 SHA256:/hWJGM+7hzDRWPsyCP6/gKqWR99cgMh9/TV5WLTFIrs
Webadmin certificate fingerprint (SHA-1):
2048 64:50:e2:01:fb:2a:28:54:1a:3b:30:94:3b:25:b7:ff:97:73:13:70
Initializing key store. This could take several minutes.
Performing KMIP setup
Starting services...
The Web-based Management Console will now be available at this URL:
<https://xxx.xxx.xxx.xxx:9443>
This device has now been configured.Press Enter to continue.
```

A log-in prompt displays.

To prevent a "man-in-the-middle" attack when connecting to the vESKM, Utimaco recommends that you write down these fingerprints and compare them with what is presented when you connect to the vESKM via SSH or HTTPS.

3.2 Configuring the first vESKM server in a cluster

If you have more than one vESKM server, Utimaco recommends that they be clustered for high availability.

All vESKM servers in a cluster must be running the same version of software.

In this section, one vESKM server will be configured first. In Establishing a cluster (p. 50), that configuration will be transferred to the remaining vESKM servers in the cluster.

If you are replacing a vESKM server or adding a member to an existing cluster, skip to Adding vESKM servers to the cluster (p. 51).

The configurations in this step are performed from the vESKM Management Console, which can be accessed from any web browser with access to the vESKM server using either an IPv4 or IPv6 IP address.

The IPv4 URL for the vESKM server is:

```
<https://[<server> IP address>]:<service port number>
```

The IPv6 URL for the vESKM server is:

`<https://[<server> IPv6 address>]:<service port number>`

`<service port number>` is 9443 by default.

3.2.1 Setting up the local Certificate Authority (CA)

The local CA is used to sign and verify the server certificate and may also be used to sign client certificate requests.

To create and install a local CA:

1. Log in to the vESKM Management Console using the admin username and the password.
2. Select the **Security** tab.
3. In **Certificates & CAs**, click **Local CAs**.
4. Enter the information required in the Create Local Certificate Authority section of the window to create your local CA.

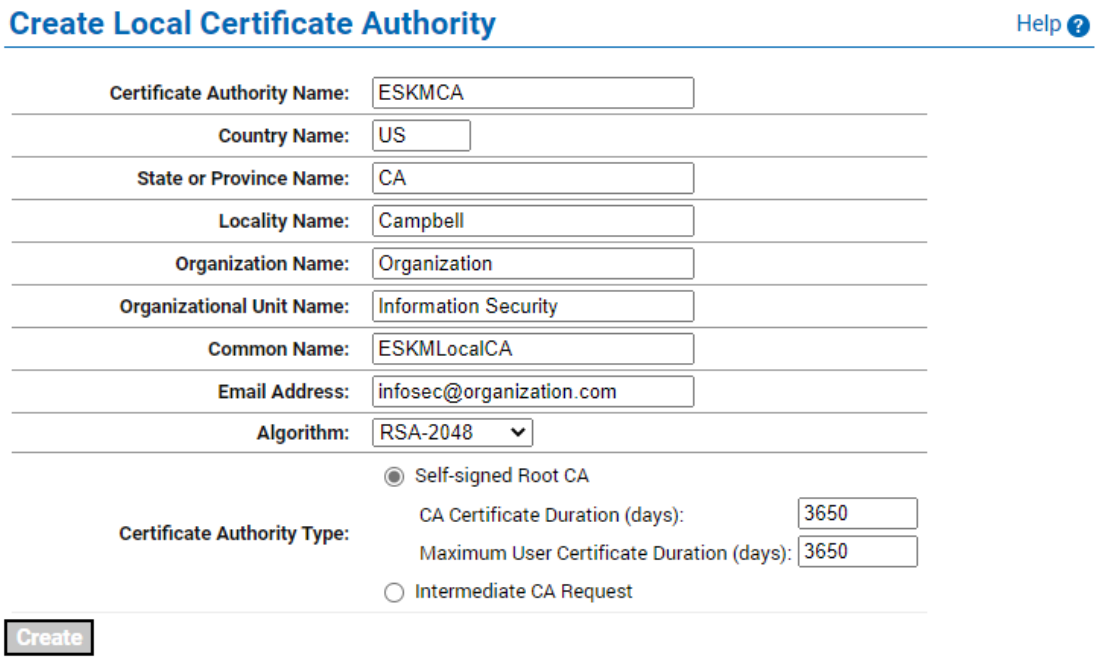


Figure 24 : Create Local Certificate Authority

a. Enter a **Certificate Authority Name** and **Common Name**. These may have the same value, for example, **vESKM Local CA**.

b. Enter your organizational information.

c. Enter the **Algorithm**. Utimaco recommends using an algorithm with security strength of at least 128 bits (e.g., ECDSA-P256).

d. Click **Self-signed Root CA** and enter the **CA Certification Duration** and **Maximum User Certificate Duration**. These values determine when the certificate must be renewed and should be set in accordance with your company's security policies. The default value for both is 3650 days or 10 years.

5. Click **Create**.

6. If the local CA will be used to sign vESKM client certificate requests, add the CA to the Trusted CA list.

   a. In **Certificates & CAs**, click **Trusted CA Lists** to display the **Trusted Certificate Authority List Profiles**.

   b. Click on the **Default** Profile Name (not the radio button).

c. In the **Trusted Certificate Authority List**, click **Edit**.

d. From the list of Available CAs in the right panel, select the CA you created in step 4. For example, `vESKM Local CA`.

e. Click **Add**.

f. Click **Save**.

Repeat the steps above to create another local CA. For example, you may want to create a KMIP Local CA to support the KMIP Certify/Re-certify operations.

Add a third-party CA certificate

If your client certificates were signed by a third-party CA, you must install the third-party CA certificate, and then add it to the Trusted CA list.

To install a third-party CA certificate:

1. In **Certificates & CAs**, click **Known CAs** to display the **Install CA Certificate section**.
2. Enter a value for the Certificate Name and paste the CA certificate text in the **Certificate** field.
3. Click **Install**. The CA certificate will be added to the Known CAs list.

To add the third-party CA certificate to the Trusted CAs list:

1. In **Certificates & CAs**, click **Trusted CA Lists** to display the **Trusted Certificate Authority List Profiles**.
2. Click on the **Default** Profile Name.
3. In the **Trusted Certificate Authority List**, click **Edit**.
4. From the list of Available CAs in the right panel, select the third-party CA you require.

5. Click **Add**.

6. Click **Save**.

3.2.2 Creating the vESKM server certificates

vESKM server certificates are used by the client to authenticate the vESKM server during the TLS/SSL handshake. vESKM supports two types of clients.

- Clients that use the KMS protocol are referred to as KMS clients.
- Clients that use the KMIP protocol are referred to as KMIP-enabled clients.

The KMS clients communicate with the KMS server and KMIP-enabled clients communicate with the KMIP server.

Clients can also communicate with the vESKM using REST APIs.

During the execution of the Setup utility a default KMIP Server Certificate is automatically created. This certificate should only be used for testing purposes, as it is a self-signed certificate. If your vESKM system will be communicating with KMIP-enabled clients, Utimaco highly recommends that you create a new KMIP server certificate. The name you assign to these server certificates should clearly indicate their purpose. For example: **vESKM KMS Server and vESKM KMIP Server**.

KMIP requires mutual authentication. After configuring the KMIP server, **enable** KMIP client certificate authentication. The KMIP client certificate authentication status is **disabled** by default.

By default, REST Server uses the system-generated server certificate. Utimaco highly recommends replacing the default certificate.

If you will be using a third-party CA, and wish to use an existing server certificate, see Import a third-party server certificate (p. 43).

To create a vESKM server certificate:

1. Click the **Security** tab.

2. In **Certificates and CAs**, select **Certificates**.

3. Enter the information required in the **Create Certificate** section of the window to create the vESKM server certificate.

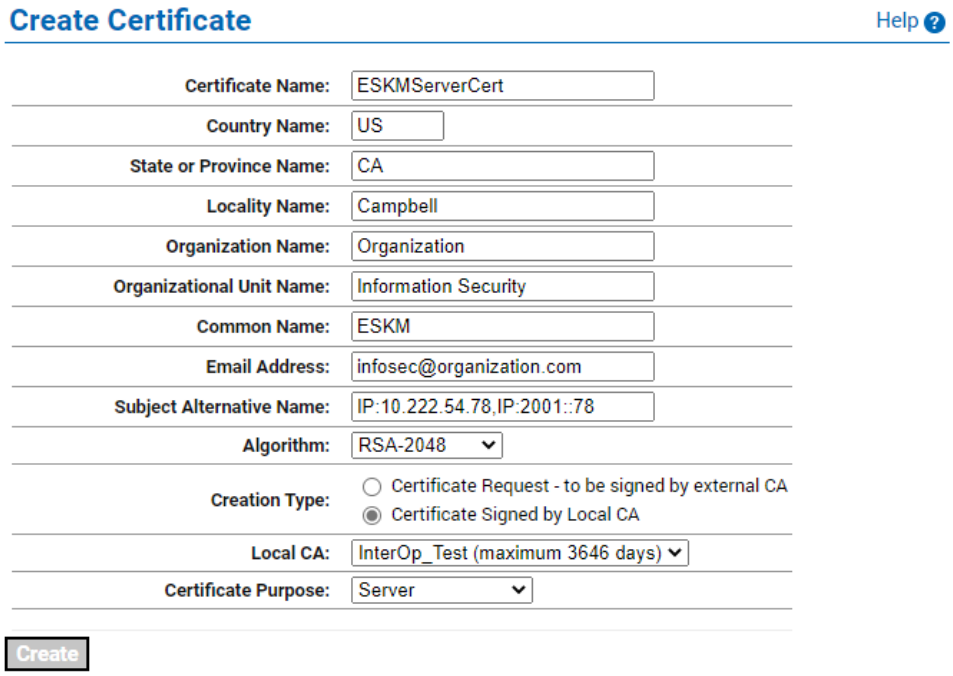


Figure 25 : Create Certificate

   a. Enter a Certificate Name and Common Name.

   b. Enter your Organizational information.

   c. Enter/Select the **Subject Alternative Name**, **Algorithm, Creation Type**, **Local CA**, and **Certificate Purpose**. Utimaco recommends using an algorithm with security strength of at least 128 bits (e.g., ECDSA-P256).

4. Click **Create**.

5. The Certificate List will include the newly created certificate, its status will be **Request Pending**. Click on the certificate name.

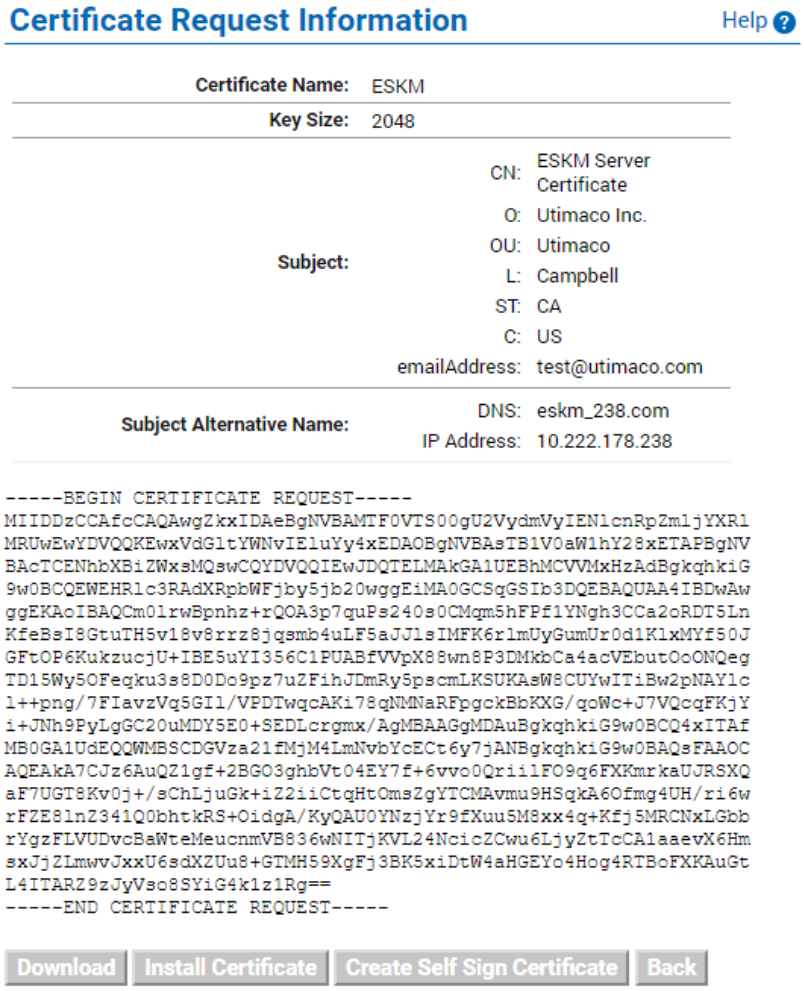


Figure 26 : Certificate Request Information

- Key Size refers to the size of the key or elliptic curve associated with this certificate.

6. In the **Certificates & CAs** menu, click **Local CAs**.

7. Click on the CA name you created in Setting up the local Certificate Authority (CA) (p. 36).

8. Click **Sign Request**.

9. Enter the data required in the **Sign Certificate Request** section of the window.

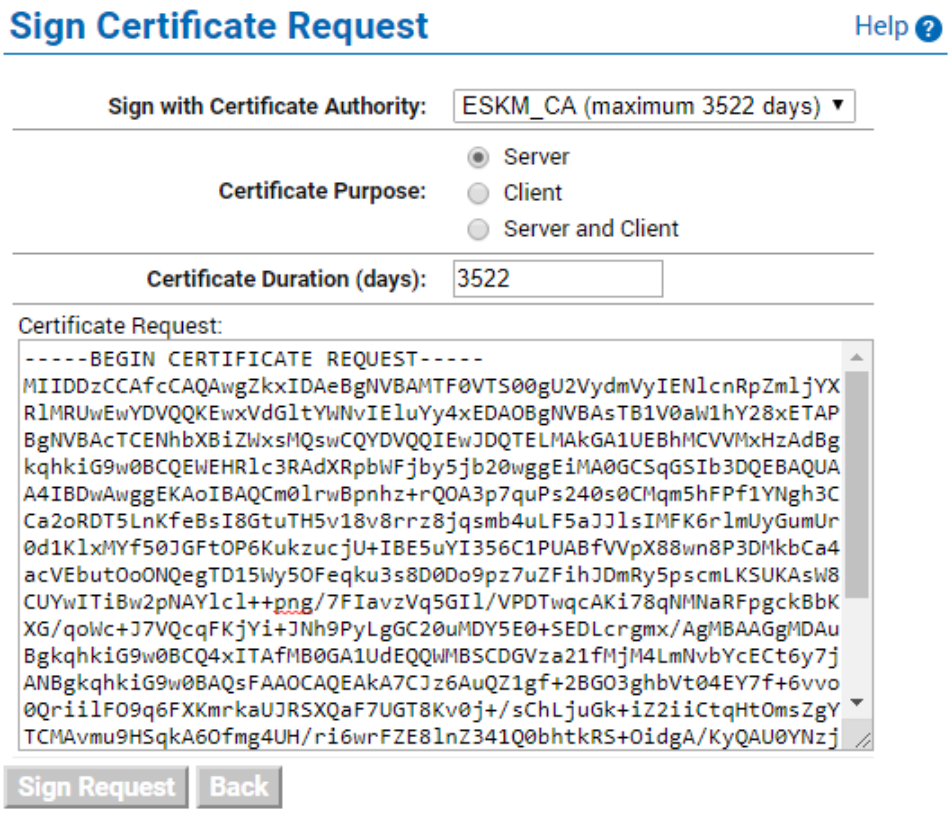


Figure 27 : Sign Certificate Request

   a. Select the CA name from the **Sign with Certificate Authority** drop down box.
   b. Select **Server** as the Certificate Purpose.
   c. Enter the number of days before the certificate must be renewed based on your site's security policies. The default value is 3649 days (10 years).

10. Click **Sign Request**.

11. In the **Certificates & CAs** menu, click on **Certificates**.

12. Click on the certificate name created in step 3 of this section.

13. Click **Install Certificate**.

14. Click **Save**. Note that the Certificate status is now Active

Repeat all of the steps above for the KMIP server certificate. You must perform these steps on each vESKM server after joining the cluster.

3.2.2.1 Import a third-party server certificate

An externally generated public/private key pair can be imported into the vESKM system for use as a server certificate. The encrypted private key data and the public key certificate must be present in the third-party server certificate file. For example:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBAB..........vvbKI=
-----END ENCRYPTED PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDhjCCA..........MKH9Fk
-----END CERTIFICATE-----
```

In addition, the password for the private key file must be known.

To import a third-party server certificate:

1. In **Certificates & CAs**, click **Certificates** to display the **Import Certificate section**.
2. Provide the source location of the certificate file.
3. Enter the Certificate Name and private key password.
4. Click **Import Certificate**.

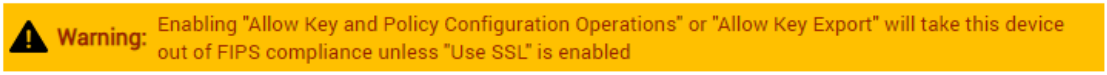
3.2.3 Enabling SSL on the Key Management Server

This section covers KMS server configuration only. For KMIP server configuration see Configuring the KMIP server. Utimaco recommends enabling FIPS compliance before enabling SSL, see "Enabling and Disabling FIPS Compliance" in the *Enterprise Secure Key Manager 8.50 User Guide*. After SSL is enabled on the first vESKM server it will be automatically enabled on the other cluster members when they are added to the cluster.
To configure and enable SSL on the KMS server:

1. Select the **Device** tab.

2. In the **Device Configuration** menu, click **KMS Server** to display the **Key Management Services Configuration** window.

3. In the **KMS Server Settings** section of the window, click **Edit**. The following warning may be displayed.



4. Configure the **KMS Server Settings**.The IP address can be an IPv4 address or IPv6 address, if support for IPv6 has been enabled, see Run the Setup utility (p. 32). If necessary, change the Port and Connection Timeout values. Utimaco recommends the default values of 9000 for the Port and 3600 for the Connection Timeout. For **Server Certificate**, select the name of the certificate you created in Creating the vESKM server certificates (p. 39).

5. Be sure to check A**llow Key and Policy Configuration Operations** and/or **Allow Key Export**.

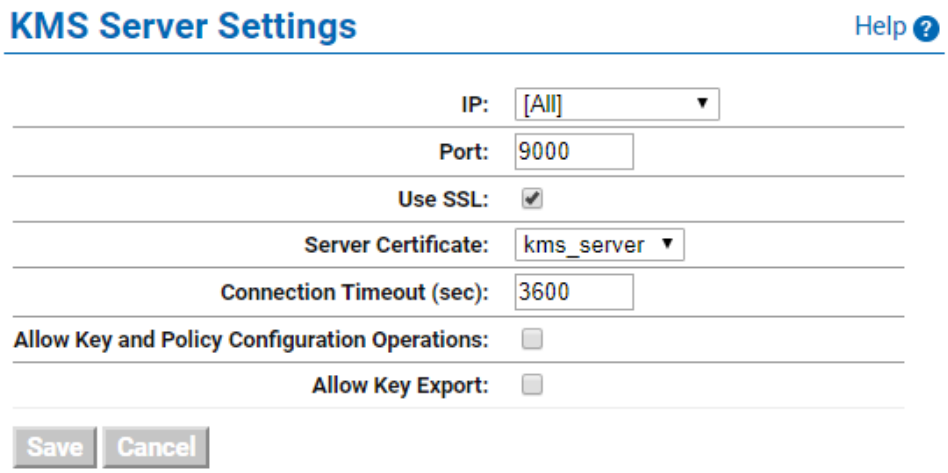


Figure 28 : KMS Server Settings

6. Click **Save**.

TLS 1.0 is disabled by default and not allowed when operating in FIPS mode.

There is no option to enable SSL/TLS for the KMIP server; It is always enabled.

3.2.4 Configuring the KMIP server

Skip this section if your vESKM system will not be communicating with KMIP-enabled clients.

The KMIP server provides the interface to clients that use the KMIP protocol. Transport Layer Security (TLS) is required, therefore you must specify the name of the server certificate.

To configure the KMIP server:

1. Select the **Device** tab.

2. In the **Device Configuration** menu, click **KMIP Server** to display the **KMIP Server Configuration** window.

3. In the **KMIP Server Settings** section of the window, click **Edit**.

4. Configure the **KMIP Server Settings**. The IP address can be an IPv4 address or IPv6 address, if support for IPv6 has been enabled, see Run the Setup utility (p. 32). If necessary, change the Port and Connection Timeout values. Utimaco recommends the default values of 5696 for the Port and 3600 for the Connection Timeout. For **Server Certificate**, select the name of the certificate you created in Creating the (p. 39) vESKM server certificates (p. 39).
    - If your vESKM server is operating in FIPS compliant mode, you must specify a KMIP server certificate that complies with the FIPS requirements.
    - If your vESKM servers are in a cluster and you are selecting a new KMIP server certificate from the "Server Certificate:" field, you must make sure that all of the

vESKM servers in the cluster already have a KMIP server certificate installed with this same name.

- If your vESKM server will support the KMIP Certify or Re-certify operations you must specify the name of a Local CA that will be used to create the certificate. In addition, you must set the KMIP user group permissions for these operations to enabled. For more information on setting KMIP user group permissions, see the KMIP Permission model description, which is located in section 3 of the *Enterprise Secure Key Manager 8.50.0 User Guide*.

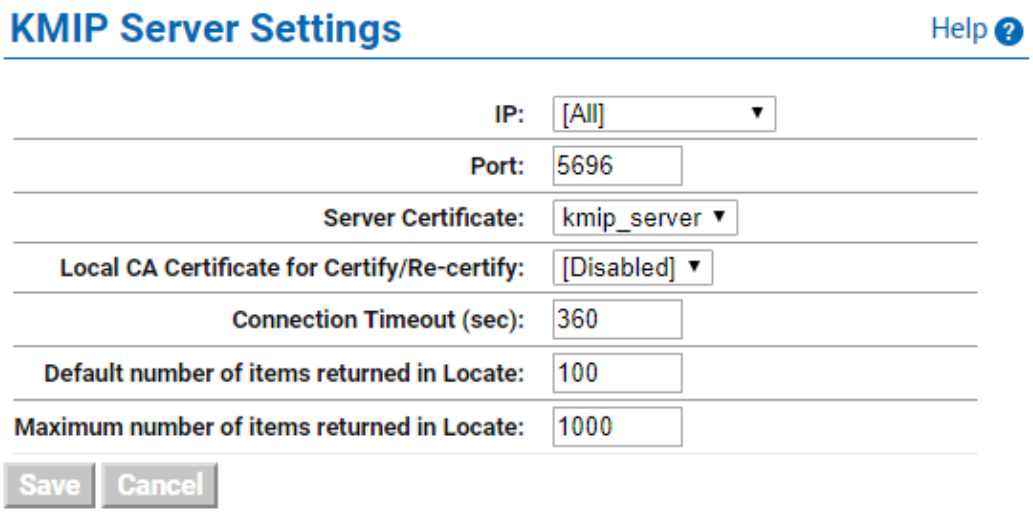


Figure 29 : KMIP Server Settings

5. Click **Save**.
   - Changing the KMIP server setting causes the KMIP server to restart.

6. Confirm that the KMIP server is started.
   a. Navigate to the Services List section of the Services Configuration page(**Device** > **Maintenance** > **Services** > **KMIP Server**).
   b. The status of the KMIP server should be Started. If the status is Stopped, select the KMIP Server, and then click **Start**.

During the execution of the Setup utility a default KMIP Server Certificate is automatically created. This certificate should only be used for testing purposes, as it is a self-signed certificate. If your vESKM system will be communicating with KMIP-enabled clients, Utimaco highly recommends that you create a new

KMIP server certificate. The name you assign to these server certificates should clearly indicate their purpose. For example: **vESKM KMS Server and vESKM KMIP Server**.

KMIP requires mutual authentication. After configuring the KMIP server, **enable** KMIP client certificate authentication. The KMIP client certificate authentication status is **disabled** by default.

To enable KMIP client certificate:

1. In the **KMIP Server Authentication Settings** section of the window, click **Edit**.

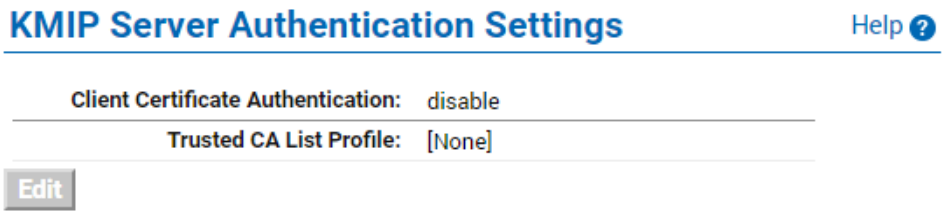


Figure 30 : KMIP Server Authentication Settings

2. Click **enable**, select the appropriate Trusted CA list.

3. Click **Save**.

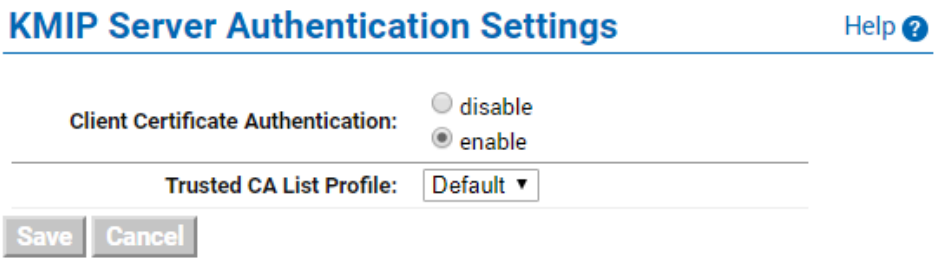


Figure 31 : Enable Client Certificate

3.2.5 KMIP interoperability settings

Skip this section if your vESKM system will not be communicating with KMIP-enabled clients.

Some KMIP-enabled clients require a specific configuration on the vESKM. Refer to your client's documentation for vESKM configuration information. Additional information on the KMIP Interoperability Settings is provided in Section 6 of the *Enterprise Secure Key Manager 8.50 User Guide*.

To configure the KMIP Interoperability Settings:

1. Select the **Device** tab.
2. In the **Device Configuration** menu, click **KMIP Server** to display the **KMIP Server Configuration** window.
3. Click **Interoperability**.
4. In the **KMIP Interoperability Settings** section of the window, click **Edit**.
5. Check the appropriate interoperability settings.

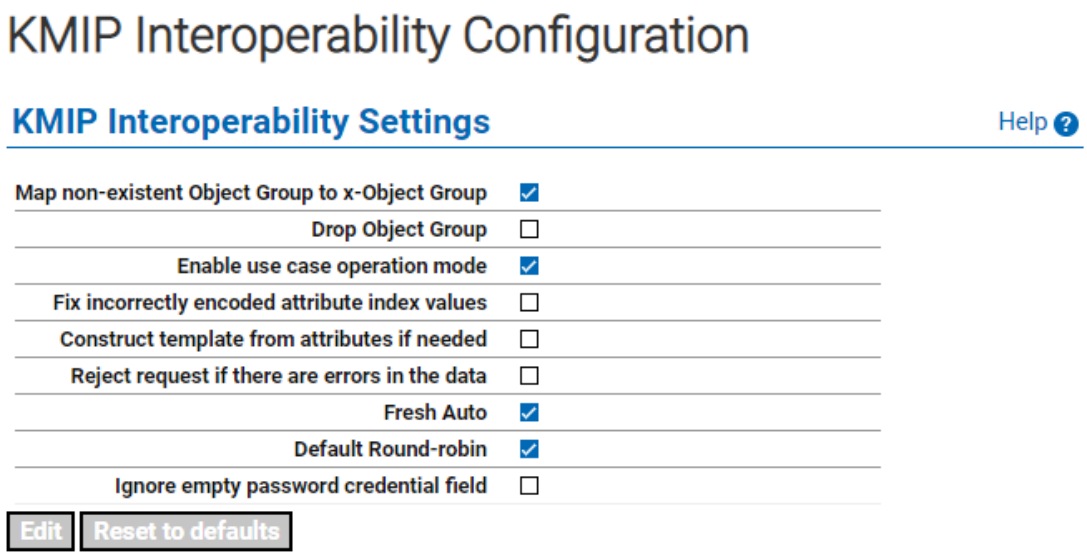


Figure 32 : KMIP Interoperability Settings

6. Click **Save**.

3.2.6 Configuring the REST server

The REST server provides the interface to clients that use REST APIs. Transport Layer Security (TLS) is required, so you must specify the server certificate.

To configure the REST server:

1. Select the **Device** tab.
2. In the **Device Configuration** menu, click **REST Server** to display the **REST Server Configuration** window.
3. In the **REST Server Settings** section of the window, click **Edit**.
4. Configure the **REST Server Settings**.
    a. Change the **Port** number, if necessary.
        i. Utimaco recommends the default value of 8443 for the Port.
    b. For **Server Certificate**, select the certificate created in Creating the (p. 39) vESKM server certificates (p. 39).
        i. Utimaco strongly recommends replacing the default system-generated server certificate.
        ii. If the vESKM server is operating in FIPS compliant mode, you must specify a REST server certificate that complies with the FIPS requirements.
        iii. If the vESKM servers are in a cluster, you must make sure that all vESKM servers in the cluster have the same REST server certificate.
5. Select **Enable Key and Crypto Operations**.
    a. Client applications will be able to do cryptographic key management in the vESKM using REST APIs, only if Key Operations are enabled.
6. Click **Save**.

Changing the REST Server Settings causes the REST server to restart.

3.3 Establishing a cluster

If you only have one vESKM server, skip this section.

The procedures in this section will establish a cluster configuration on one vESKM server and then transfer that configuration to the remaining vESKM servers.

- In Creating the cluster (p. 50), the cluster is created on one vESKM server.
- In Adding vESKM servers to the cluster (p. 51), each of the additional vESKM servers are added to the cluster.

3.3.1 Creating the cluster

To create the cluster, perform the following steps on one of the vESKM servers to be clustered:

1. From the vESKM Management Console, click the **Device** tab.

2. In the **Device Configuration** menu, click **Cluster**.

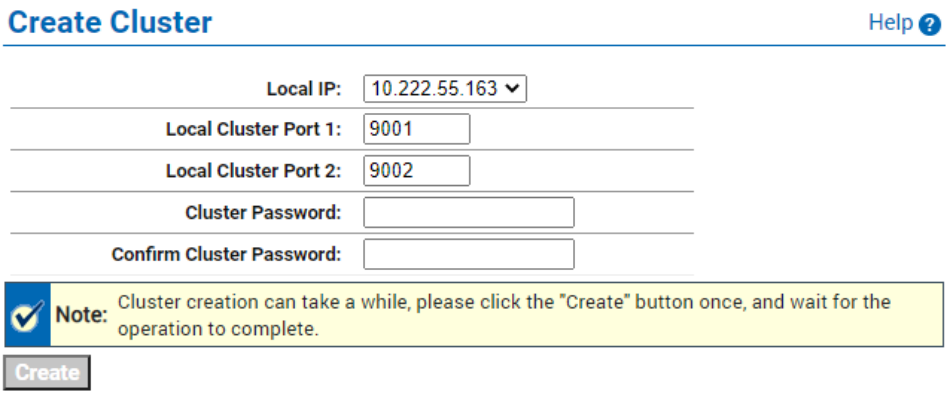


Figure 33 : Create Cluster

3. If required, change the **Local IP** value. If you have enabled Ethernet#2 you can use its IP address for clustering.
    a. All vESKM servers in a cluster must use an IPv4 address for the cluster.
    b. All vESKM servers in a cluster must be time-synchronized before creating the cluster.

4. If required, change the **Local Cluster Port 1** value. Utimaco recommends using the default value of 9001.

5. If required, change the **Local Cluster Port 2** value. Utimaco recommends using the default value of 9002.

6. Choose a cluster password and enter it into the **Cluster Password** field. Enter the password a second time into the **Confirm Cluster Password** field.

7. Click the **Create** button.

8. In the **Cluster Settings** section of the window, click **Download Cluster Key** and save the key to a convenient location, such as your computer's desktop.

The cluster key is a text file and is only required temporarily. It may be deleted from your computer's desktop after all vESKM servers have been added to the cluster.

3.3.2 Adding vESKM servers to the cluster

To add vESKM servers to the cluster, perform the following steps on each additional vESKM server.

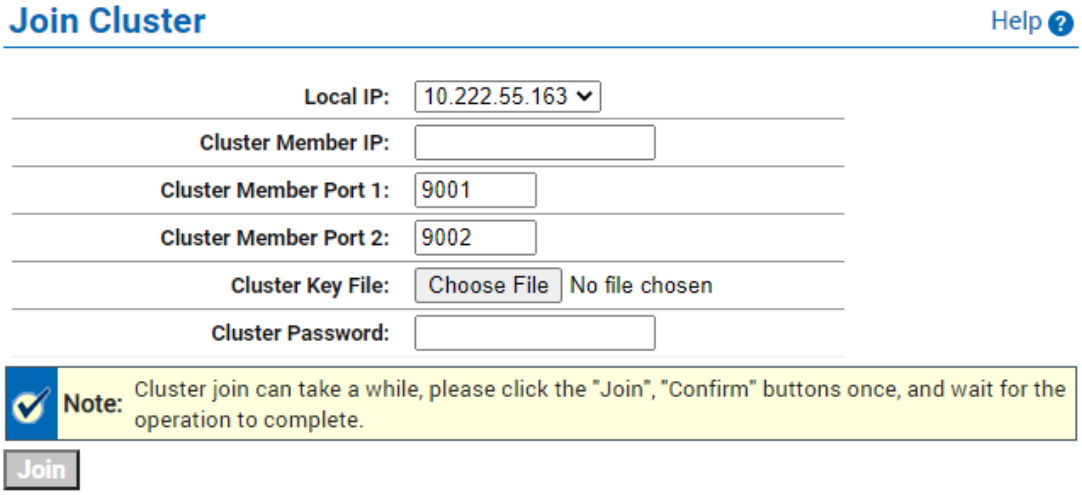


Figure 34 : Join Cluster

Adding multiple vESKM servers to the cluster is a serial process. Add the first vESKM server and then monitor the system log for the status of the synchronization process. Wait until the "**Cluster synchronization succeeded.**" message appears in the system log before attempting to add the next vESKM server to the cluster. The amount of time required to complete the synchronization process is a function of the number of keys in the cluster.

If the new vESKM server is a replacement and is configured with the same IP address as the failed vESKM server, make sure the client does not send any key generation requests until the new vESKM server has successfully completed the cluster synchronization process. Alternately, you can stop the KMS and KMIP servers and then start them once the cluster synchronization process is complete. Use the system log to monitor the progress of the cluster synchronization process.

Join the vESKM server to the cluster

1. Select the **Device** tab.
    a. In the **Device Configuration** menu, click on **Cluster**.
    b. In the **Join Cluster section** of the window, select the appropriate **Local IP** value.
        i. All vESKM servers in a cluster must use an IPv4 address for the cluster.
        ii. All vESKM servers in a cluster must be time-synchronized before creating the cluster.

c. Type the original cluster member's IP into **Cluster Member IP**.

d. Type the original cluster member's port into **Cluster Member Port 1**. The default value of this port is 9001. If this value was changed in Creating the cluster (p. 51), step 4, use that value.

e. Type the original cluster member's port into **Cluster Member Port 2**. The default value of this port is 9002. If this value was changed in Creating the cluster (p. 51), step 5, use that value.

f. Click **Browse** and select the **Cluster Key File** you saved in Creating the cluster (p. 51), step 8.

g. Type the cluster password into **Cluster Password**. This is the password entered in Creating the cluster (p. 51), step 6.

h. Click **Join**.

i. Click **Confirm** to synchronize with the cluster.

If the vESKM server joining the cluster is SSL enabled, this step will cause the WebAdmin service and the KMS and KMIP servers to restart, resulting in a temporary connection loss. To restore the connection, refresh the browser.

- After adding all members to the cluster, you can delete the cluster key file from the desktop.
- After clustering the vESKM servers, follow the steps in Creating the vESKM server certificates (p. 51) to create and install the server certificates on each vESKM server that has joined the cluster. Depending on the KMS, KMIP, and REST configuration, separate server certificates may need to be created for each vESKM server in the cluster.

Make sure to use the same server certificate name as specified under KMS/KMIP/REST Server Settings.

- Once the KMIP server certificate is created, restart the KMIP server manually. Navigate to the Services List section of the Services Configuration page (**Device** > **Maintenance** > **Services** > **KMIP Server**).

- Once the REST server certificate is created, save the same certificate in the REST Server configuration. Navigate to REST Server section of the Device Configuration page (**Device** > **REST Server**).

3.4 Removing a vESKM server from the cluster

In some situations it may be necessary to remove one or more vESKM servers from a cluster. Perform the following steps on the vESKM server to remove it from the cluster:

1. Verify the cluster integrity.
    a. All vESKM nodes must show active on cluster setting page.
    b. Confirm that there are no replication failure events in any of the logs.
    c. Pick a key at random and confirm that it exists on each vESKM node. Or export all key names and then confirm that they all exist on each vESKM node.
    If any of the steps above fail, you must back up each vESKM node, and restore the backup onto every vESKM node in the cluster.

2. Stop the KMS and KMIP servers on the vESKM server that is being removed from the cluster.
    a. From the vESKM Management Console, click on **Devices**, and then **Services**.
    b. Select **KMS Server**.
    c. Click **Stop**.
    d. At the secondary approval screen, click **Confirm** to stop the KMS Server.
    e. Click **Refresh** to confirm that the KMS server has stopped.
    f. To stop the KMIP Server, repeat steps b-e above, specifying **KMIP Server**.

3. Remove the vESKM server from the cluster.
    a. From the vESKM Management Console, click on **Devices**, and then **Cluster**.
    b. Click **Remove from Cluster**.
    c. At the secondary approval screen, click **Confirm** to remove the vESKM server from the cluster.

Perform the following steps if the vESKM server will be added back to the cluster. Confirm that the key counts on all vESKM nodes are identical.

4. Add the vESKM server to the cluster. Perform steps 1 through 8 in Adding vESKM servers to the cluster (p. 51). Do not perform step 9, instead click **Cancel**.

5. Back up each vESKM server that was not removed from the cluster and restore the backup onto each vESKM server that was added to the cluster. If no configuration changes were made, while the vESKM server was removed from the cluster, backup and restore just the keys. If configuration changes were made, backup and restore the keys and the configuration—do not back up the network configuration.

3.5 Cluster behavior

The following table shows the behavior of the cluster at different licensing stages.

Table 2: Cluster Behavior

Joining Node	***Clustered Nodes***	***Trial period of the trial versioned cluster nodes***
Trial Version	Trial Version	Minimum of the clustered and joining node's trial period
Trial Version	Licensed	No Change
Trial Version	Trial Version + Licensed	Minimum of the clustered (trial version) and joining node's trial period
Licensed	Trial Version	No Change
Licensed	Licensed	No Change
Licensed	Trial Version + Licensed	No Change

3.6 Enrolling client devices with the vESKM server

The vESKM server is compatible with many client devices. To establish correct communication between the vESKM server and the client, you must create a client account, then configure the client to obtain keys from the vESKM server. KMIP-enabled clients require KMIP objects to be created or registered. Groups may need to be created and permissions need to be defined to control access to KMIP objects and operations. Please refer to the client device's documentation for information on how to correctly configure the client and the vESKM server.

A KMIP-enabled client will by default belong to the default user group and its objects will by default belong to the default object group. This means that any user who has permission to access the default object group will be able to access the user's KMIP objects. Set the applicable group permissions when registering the user to ensure that only authorized KMIP-enabled users are able to access the KMIP objects.

3.7 Client licenses

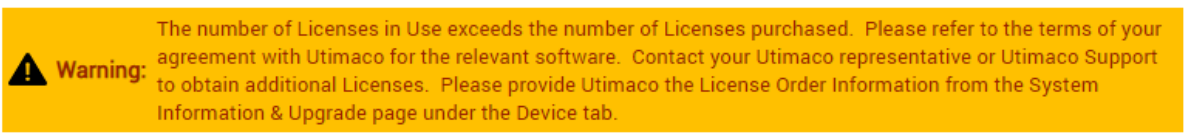
A client license is required for each client device or application user enrolled in the vESKM cluster either as a KMS user or as a KMIP-enabled user. When vESKM servers are clustered, the number of vESKM servers in the cluster establishes and aggregates the initial default number of clients that can be enrolled.

This section describes the following processes:

- Obtaining license order information (p. 56)
- Installing a client license pack (p. 58)

3.7.1 Obtaining license order information

If the number of clients to be enrolled exceeds the number of vESKM servers you have purchased, a warning message will display similar to following.



You must purchase and install a client license pack to allow these additional clients to be enrolled in the cluster. To order a license pack, contact Utimaco Sales or your reseller for ordering information and provide them with the License Order Information from the vESKM.

Before requesting the client license, user has to get the vESKM licensed first.

License Order Information will not be available for vESKMs running on trial mode.

Follow these steps to obtain the License Order Information from the vESKM server.

1. Log in to the vESKM Management Console using the admin password.
2. Select the **Device** tab.
3. In Maintenance, click **System Information & Upgrade**.
4. Enter the information required in the **License Order Information** section of the window.

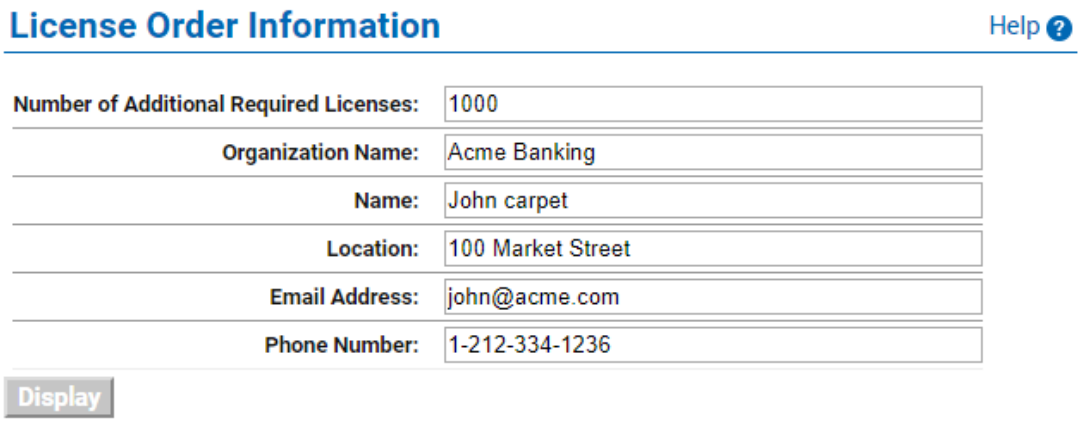


Figure 35 : License Order Information

5. Click **Display**.
6. Copy the information (as highlighted below) or click the **Download** button to store the License Order Information on your computer.

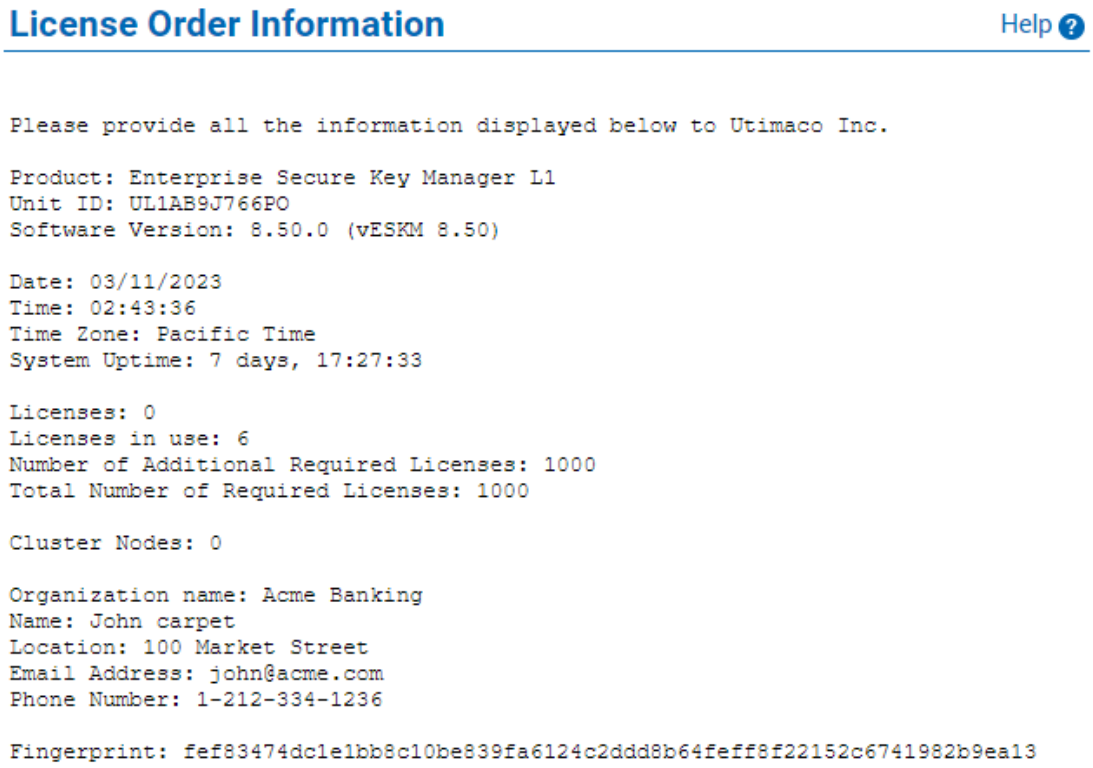


Figure 36 : License Order Information

If the vESKM servers are clustered, confirm that the value in the **Cluster Node**s field is correct. If the value is incorrect, one or more vESKM servers in the cluster is not running the correct software version. To determine which vESKM server should be upgraded, click the **Device Configuration** menu, click on **Cluster** and use the **Software Version** column to obtain software version of each vESKM server in the cluster. Once you have determined which vESKM server needs to be upgraded, follow the steps in the Appendix A vESKM software upgrade procedure (p. 66).

7. Provide Utimaco with the License Order Information.

3.7.2 Installing a client license pack

The license pack file will be sent to you in an email, copy this file to a PC, and then perform the following steps:

1. Log in to the vESKM Management Console using the admin password you supplied in Run the Setup utility, step 4.

2. Select the **Device** tab.

3. In **Maintenance**, click **System Information & Upgrade**.

4. In the **Software Upgrade/Install** section of the window, select **Upload** from browser, click **Browse** and locate the license pack file, and then click **Open**.

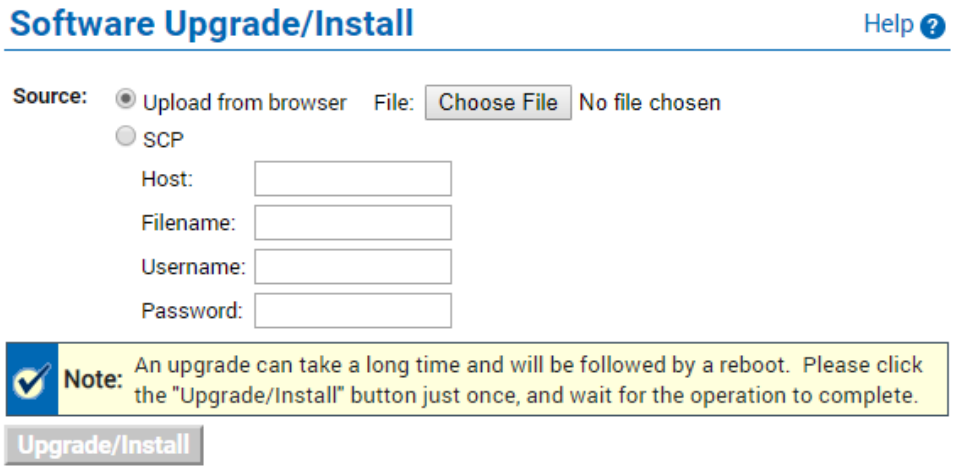


Figure 37 : Software Upgrade/Install

5. Click **Upgrade/Install**. The license pack will be applied immediately. The vESKM server will not reboot.

A license pack can be installed at any time, not just during the vESKM server installation process. When a new license pack is installed, it will override any previous license pack. License packs are automatically replicated to all vESKM servers in a cluster.

3.8 Changing the KMIP server certificate in a vESKM cluster

In certain situations it may be necessary to change the server certificate on the KMIP server. To accomplish this task, perform the following steps:

- On each vESKM server in the cluster execute the instruction sequence listed in Creating the vESKM server certificates (p. 39). In step 3a specify a new name for the KMIP server certificate, for example "**vESKM KMIP server certificate #2**". Be sure you assign the same name to this KMIP server certificate on all of the vESKM servers in the cluster.
- On one vESKM server in the cluster execute the instruction sequence listed under “To configure the KMIP server” in Configuring the KMIP server (p. 45). In step 4, Configure the KMIP server settings, be sure to specify the name of the new KMIP server certificate you created in step 1 above.

4 Licensing

The virtual Enterprise Secure Key Manager (vESKM) server is delivered as a fully functional trial, valid for 60 days. During this trial period, you will be able to perform all the activities that can be performed on any licensed vESKM server.

The indication message “This is a trial version!” is displayed on login page, home page and license information page.

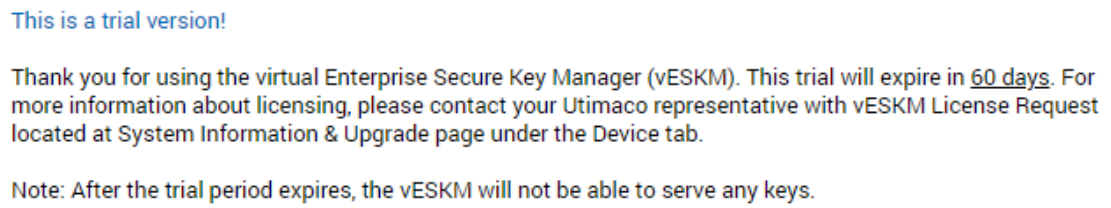


Figure 38 : Trial Version message

Once the trial period expires, a warning message “Warning: Your free trial has expired!” is displayed on all the respective pages, indicating that new license packs have to be purchased to restore all the functionalities.

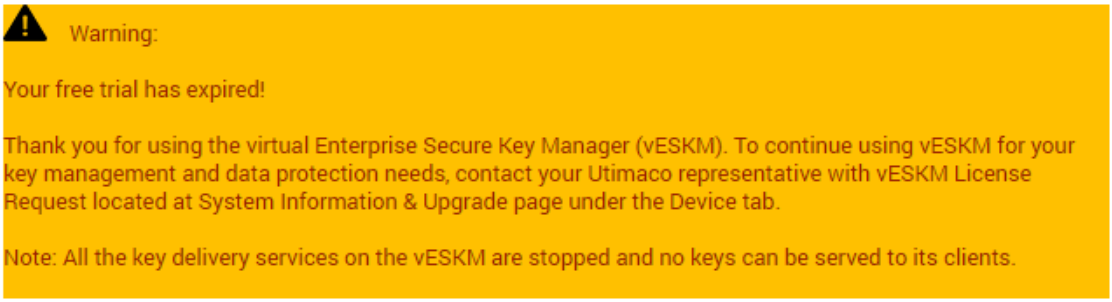


Figure 39 : Trial period expired warning

4.1 Feature availability post trial period expiry

Post expiry of trial period:

- Users can view their configuration data and take backups
- Users will not be able to do any configuration changes either through Web Admin or CLI
- All key delivery services (KMS and KMIP) get disabled
- SNMP service gets disabled

- Replication service gets disabled

4.2 vESKM licenses

To run the vESKM as licensed version, user has to install the license by creating a vESKM license request. In order to get vESKM licensed, user has to purchase the vESKM license. For more information about licensing, contact your Utimaco representative with **vESKM License Request** located at **System Information & Upgrade** page under the **Device** tab.

This section describes the following processes:

- Creating a vESKM license request (p. 62)
- Installing a vESKM license (p. 63)

4.2.1 Creating a vESKM license request

vESKM license request section gathers all the required information from the user to create a new vESKM license.

1. Log in to the vESKM Management Console using the admin password.
2. Select the **Device** tab.
3. In Maintenance, click **System Information & Upgrade**.
4. Enter the information required in the **vESKM License Request** section of the window.
5. Click the **Download** button to store the license request on your computer.
6. Contact Utimaco representative and provide the **vESKM License Request**.

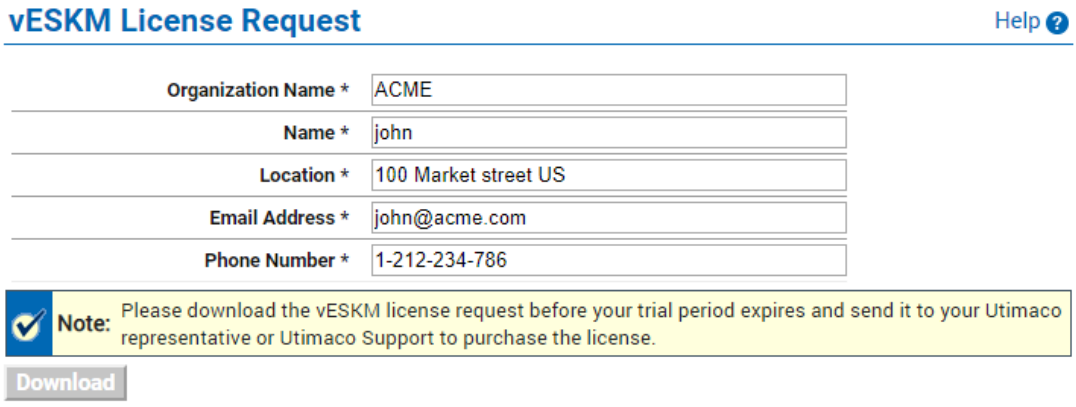


Figure 40 : License Request

The following table describes the components of the vESKM license request section.

Table 3: Components-vESKM license request section

Components	***Description***
Organization Name	Name of the organization requesting vESKM licenses.
Name	Name of the person requesting vESKM licenses.
Location	City, state, and country where the organization is based.
Email Address	Email address of the person requesting vESKM licenses.
Phone Number	Phone number of the person requesting vESKM licenses.

4.2.2 Installing a vESKM license

To install the license:

1. Log in to the vESKM Management Console using the admin password.
2. Select the **Device** tab.

3. In **Maintenance**, click **System Information & Upgrade**.

4. In the **Software Upgrade/Install** section of the window, select **Upload** from browser, click **Browse** and locate the license pack file, and then click **Open**.

5. Click **Upgrade/Install**. The license will be applied immediately. The vESKM server will not reboot.

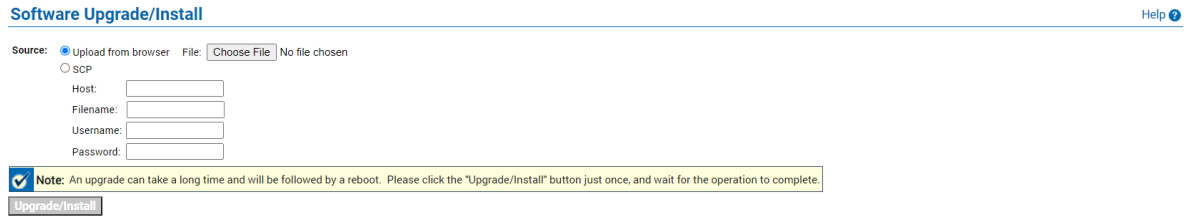


Figure 41 : Software Upgrade/Install

The following table describes the components of the Software Upgrade/Install section.

Table 4: Software Upgrade/Install-components

Component	***Description***
Source	Specify the method for copying the software file to the vESKM. If you are uploading the file through the browser, select Upload from browser, then click Browse and locate the file on the local drive or network. If you are using SCP to copy the file to the vESKM, select the appropriate option and enter the following information: ▪ Host: the source host. IPv4 addresses are supported. IPv6 addresses are also supported, if IPv6 is enabled. ▪ Filename: the name of the file on the source host. ▪ Username: the username of the account on the source host. ▪ Password: the password for the user account on the source host.

The software upgrade and installation mechanism can be used to install new features, upgrade core software, and apply security patches. You can upgrade or install software from both the Management Console and the Command Line Interface. If you are interested in monitoring the status of the upgrade, you should perform the upgrade from the Command Line Interface.

Software upgrades must be applied to all vESKMs individually in a cluster. Software upgrades are not replicated across members of a cluster.

To safeguard vESKMs, only software signed by Utimaco can be installed on the Virtual Enterprise Secure Key Manager. Changes to multiple components of the system are bundled together in an encrypted software file provided by the Technical Support organization at Utimaco.

5 Appendix A vESKM software upgrade procedure

5.1 Prerequisites

Only versions 8.1 and higher are supported for upgrade.

- Perform a complete backup before the software upgrade. For backup instructions, please refer to the Backup procedures mentioned in section 4 of the *Enterprise Secure Key Manager User Guide*.
- Record the total number of keys and KMIP objects present in the vESKM. You can obtain these values by logging on to the vESKM Management Console and clicking on the **Security** tab. The totals are listed in **General** section of the **Key and Policy Configuration** window.
- Temporarily store the Utimaco provided software upgrade file on your personal computer.
- Record the vESKM date and time prior to performing the upgrade. You can obtain this by logging on to the vESKM Management Console and reviewing the **System Summary** section under the **Home** tab.

5.2 Installation instructions

Perform these steps on each vESKM. Do not upgrade more than one vESKM at a time. For example, complete the software upgrade procedure on the first vESKM before upgrading the second one.

1. Log on to the vESKM Management Console as an administrator who has software upgrade privileges.

2. Navigate to the Services List section (**Devices >Services**) and stop the KMS and KMIP servers.

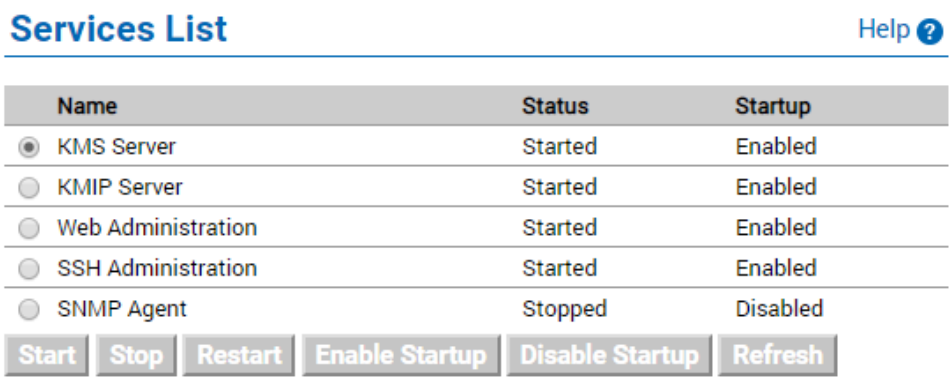


Figure 42 : Services List

3. Navigate to the Software Upgrade/Install section (**Devices >System Information & Upgrade**).

4. Make sure the **Upload from browser** radio button is enabled, and then click the **Browse...** button.

5. Navigate to the vESKM upgrade file location on your personal computer, for example vESKM_upgrade, and then click Open. At the vESKM Management Console, the **Software Upgrade/Install** section will look like this.

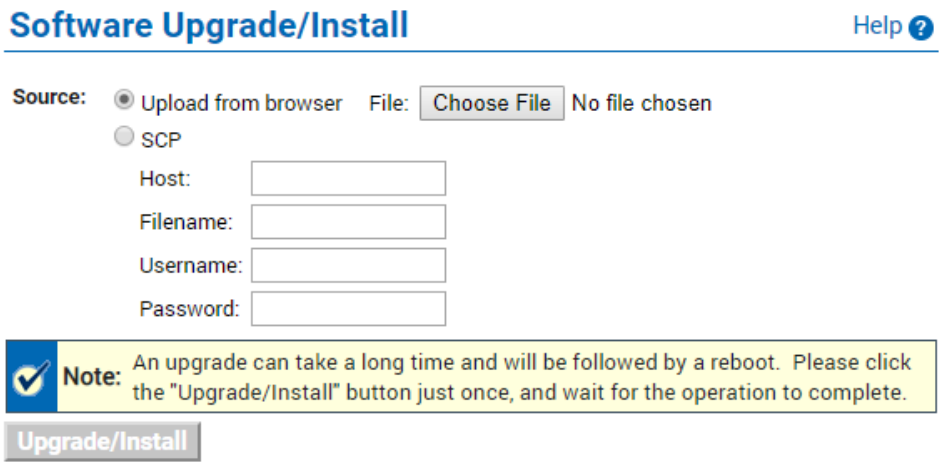


Figure 43 : Software Upgrade/Install

6. Click the **Upgrade/Install** button to install the upgrade. After installing the upgrade, the vESKM will automatically reboot.

7. Wait 5 to 7 minutes, and then log on to the vESKM.

8. View the **System Summary** section, located in the **Home** tab, to confirm that the software version corresponds to the upgraded vESKM version.

9. Navigate to the Services List section (**Devices >Services**) and confirm that the status of all the services is Started.

10. Click on the **Security** tab, and then view the totals listed in the **General** section of the **Key and Policy Configuration** window, as shown below, to confirm that the number of keys and KMIP objects in the vESKM has not changed.

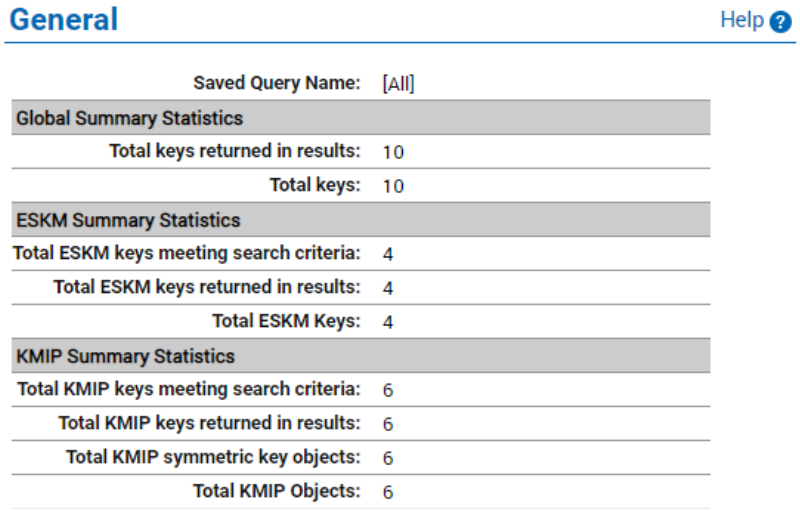


Figure 44 : General section

11. The software upgrade process is now complete. If necessary, you can rollback the software upgrade by executing this CLI command: `software rollback`

The CLI must be in configuration mode (`config#`) when executing the `software rollback` command.

When the rollback command is executed, keys and configuration data also get reverted. Any key that is created after the last software update gets deleted. Perform a backup of keys and configuration data, prior to executing the rollback command.

Do not refresh the Management Console page when the upgrade is in progress.

After confirming that the prerequisites have been performed, make a note of the time before upgrade. Repeat steps 1-9 on each additional vESKM to be upgraded. After all the vESKMs have been upgraded, delete the upgrade file from the personal computer.

If the upgraded vESKMs are members of a cluster, perform these additional steps after all cluster members have been upgraded.

1. Log on to each of the clustered vESKM's Management Console as an administrator.

2. Navigate to the Cluster Configuration section (**Device > Cluster**).

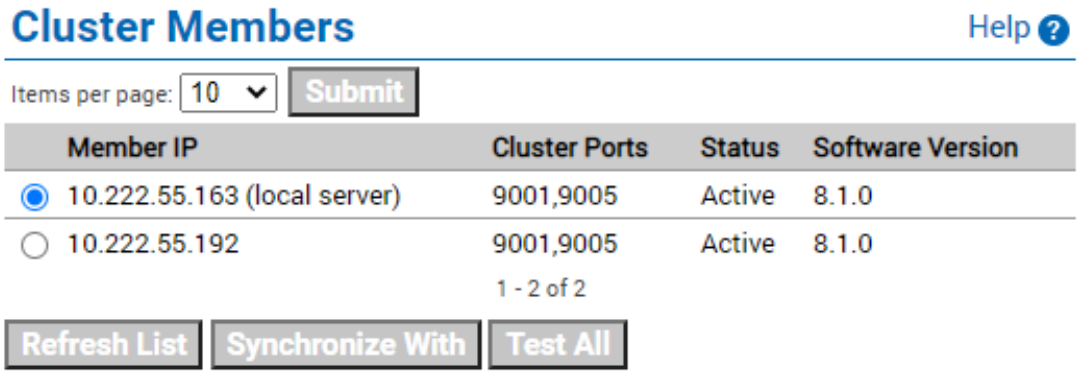


Figure 45 : Cluster Members

3. Click on the radio button of one of the cluster members.

4. Click **Refresh List**.

Make sure that all the vESKMs in the cluster are running the same software version. If necessary, follow the steps in this appendix to upgrade any vESKM that is not at the correct software version level.

5.3 Verify vESKM cluster integrity

This step ensures that there are no latent issues on the cluster that would affect the key integrity. Verify the following to ensure that the vESKM cluster is synchronized:

1. Confirm that the key counts on all vESKM nodes are identical.

2. All vESKM nodes must be joined to the same cluster.

3. All vESKM nodes must show active on cluster setting page.

4. Confirm that there are no replication failure events after upgrading all vESKM nodes.

If the vESKM nodes are not synchronized, repair the cluster by backing up keys from each vESKM node and restore each backup to each vESKM node. It may be sufficient to only restore keys that were created during the upgrade process. Do not use the Synchronize function.