



VMWARE VSPHERE

Integration Guide

Applicable Devices:

KMES Series 3

Applicable Versions:

6.1.4.x



THIS DOCUMENT CONTAINS CONFIDENTIAL INFORMATION PROPRIETARY TO FUTUREX, LP. ANY UNAUTHORIZED USE, DISCLOSURE, OR DUPLICATION OF THIS DOCUMENT OR ANY OF ITS CONTENTS IS EXPRESSLY PROHIBITED.

TABLE OF CONTENTS

| | |
|--|----|
| [1] OVERVIEW OF THE VMWARE VSPHERE / KMES SERIES 3 INTEGRATION | 3 |
| [1.1] PURPOSE OF THE DOCUMENT | 3 |
| [1.2] WHAT IS KMIP? | 3 |
| [1.3] WHAT IS VMWARE VSPHERE | 3 |
| [1.4] ABOUT VMWARE ENCRYPTION | 3 |
| [2] PREREQUISITES | 5 |
| [3] CONFIGURE TLS CERTIFICATES FOR THE KMIP PORT ON THE KMES SERIES 3 | 6 |
| [3.1] CREATE A CERTIFICATE AUTHORITY (CA) ON THE KMES SERIES 3 | 6 |
| [3.2] CONFIGURE TLS CERTIFICATES FOR THE KMIP CONNECTION PAIR | 8 |
| [4] REGISTER THE KMES SERIES 3 AS A STANDARD KEY PROVIDER IN VCENTER SERVER USING THE VSPHERE CLIENT | 12 |
| [5] CONFIGURE TLS CERTIFICATES FOR VCENTER SERVER | 15 |
| [5.1] GENERATE A CERTIFICATE SIGNING REQUEST (CSR) WITH THE VSPHERE CLIENT | 15 |
| [5.2] SIGN THE VCENTER CSR USING A CERTIFICATE AUTHORITY (CA) ON THE KMES | 16 |
| [5.3] EXPORT THE SIGNED VCENTER CERTIFICATE | 16 |
| [5.4] IMPORT THE SIGNED VCENTER CERTIFICATE INTO VCENTER SERVER WITH THE VSPHERE CLIENT | 17 |
| [6] CREATE A USER ON THE KMES SERIES 3 FOR VCENTER SERVER | 18 |
| [7] VM AND VSAN ENCRYPTION IN VSPHERE | 20 |
| [7.1] ENCRYPTING AN EXISTING VIRTUAL MACHINE WITH THE VSPHERE CLIENT | 20 |
| [7.2] VIEWING THE KEYS THAT VSPHERE CREATED ON THE KMES | 21 |
| APPENDIX A: XCEPTIONAL SUPPORT | 22 |

[1] OVERVIEW OF THE VMWARE VSPHERE / KMES SERIES 3 INTEGRATION

[1.1] PURPOSE OF THE DOCUMENT

The purpose of this document is to provide information regarding the configuration of the Futurex KMES Series 3 with VMware vSphere using KMIP. For additional questions related to your KMES Series 3 device, see the relevant administrator's guide.

[1.2] WHAT IS KMIP?

The Key Management Interoperability Protocol (KMIP) is an extensible communication protocol that defines message formats for the manipulation of cryptographic keys on a key management server. This facilitates data encryption by simplifying encryption key management. Keys may be created on a server and then retrieved, possibly wrapped by other keys. Both symmetric and asymmetric keys are supported, including the ability to sign certificates. KMIP also allows for clients to ask a server to encrypt or decrypt data, without needing direct access to the key.

[1.3] WHAT IS VMWARE VSPHERE

From VMware's documentation website: "VMware vSphere is VMware's virtualization platform, which transforms data centers into aggregated computing infrastructures that include CPU, storage, and networking resources. vSphere manages these infrastructures as a unified operating environment, and provides you with the tools to administer the data centers that participate in that environment.

The two core components of vSphere are ESXi and vCenter Server. ESXi is the virtualization platform where you create and run virtual machines and virtual appliances. vCenter Server is the service through which you manage multiple hosts connected in a network and pool host resources."

For more general information about vSphere, please refer to [VMware's documentation site](#).

[1.4] ABOUT VMWARE ENCRYPTION

[VMware vSphere encryption](#) debuted in vSphere 6.5 and vSAN 6.6, enabling both virtual machine (VM) encryption and disk storage encryption. The required components are vCenter vSphere Server, a third-party Key Management Server (KMS), and ESXi hosts.

[1.4.1] Encryption Process Flow

The encryption process flow is essentially identical for VMs and vSAN clusters. All of the involved steps are outlined below:

1. Register the KMES Series 3 as a Standard Key Provider in the vSphere Client.
2. Set up a domain of trust (i.e., mutual authentication) between vCenter Server and the KMS.

- This is done by exchanging TLS certificates between your KMS and vCenter Server to establish trust.
3. When the user performs an encryption task, for example, creating an encrypted virtual machine, vCenter Server requests a new key from the default key server. This key is used as the KEK.
 4. vCenter Server stores the key ID and passes the key to the ESXi host. If the ESXi host is part of a cluster, vCenter Server sends the KEK to each host in the cluster.

The key itself is not stored on the vCenter Server system. Only the key ID is known.

5. The ESXi host generates internal keys (DEKs) for the virtual machine and its disks. It keeps the internal keys in memory only, and uses the KEKs to encrypt internal keys.

Unencrypted internal keys are never stored on disk. Only encrypted data is stored. Because the KEKs come from the key server, the host continues to use the same KEKs.

6. The ESXi host encrypts the virtual machine with the encrypted internal key.

Any hosts that have the KEK and that can access the encrypted key file can perform operations on the encrypted virtual machine or disk.

[2] PREREQUISITES

Supported Hardware:

- KMES Series 3, version 6.1.3.11 and above, with the *KMIP* license enabled

Other:

- vCenter Server
- ESXi host(s) with at least one virtual machine installed on it

[3] CONFIGURE TLS CERTIFICATES FOR THE KMIP PORT ON THE KMES SERIES 3

Before KMIP connections can occur between vCenter Server and KMES Series 3, both parties must establish a mutual trust relationship by validating their respective digitally signed certificates.

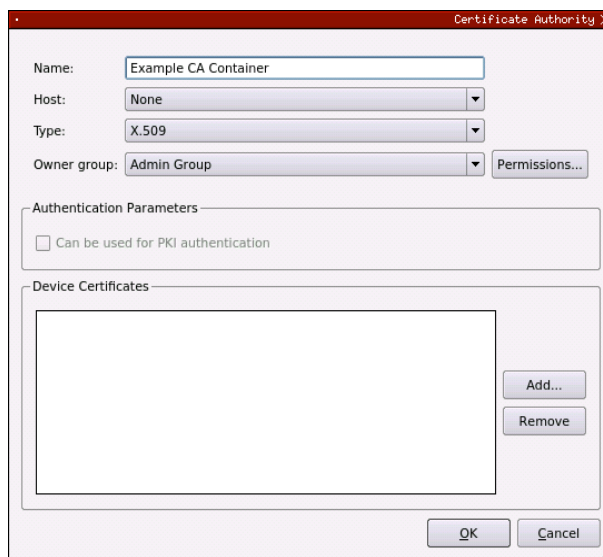
In this section, a certificate will be generated and signed for the KMIP connection pair on the KMES Series 3.

In the next section, while registering the KMES as a Standard Key Provider in the vSphere Client, the KMES will present the TLS certificate that is configured for the KMIP connection pair. After accepting the presented certificate, vCenter will trust the KMES moving forward.

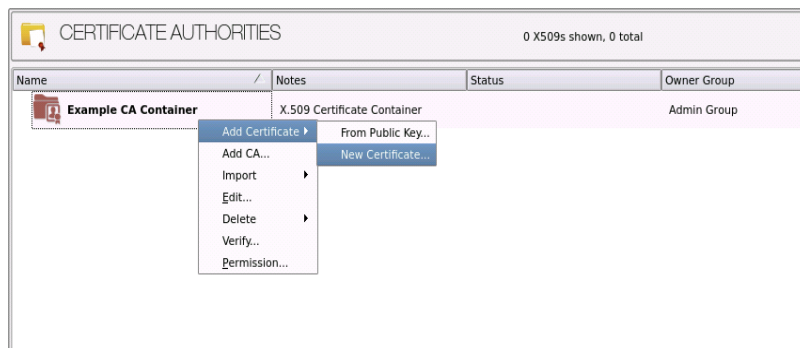
TLS certificates for the vCenter Server will be generated, signed, and registered in a later section.

[3.1] CREATE A CERTIFICATE AUTHORITY (CA) ON THE KMES SERIES 3

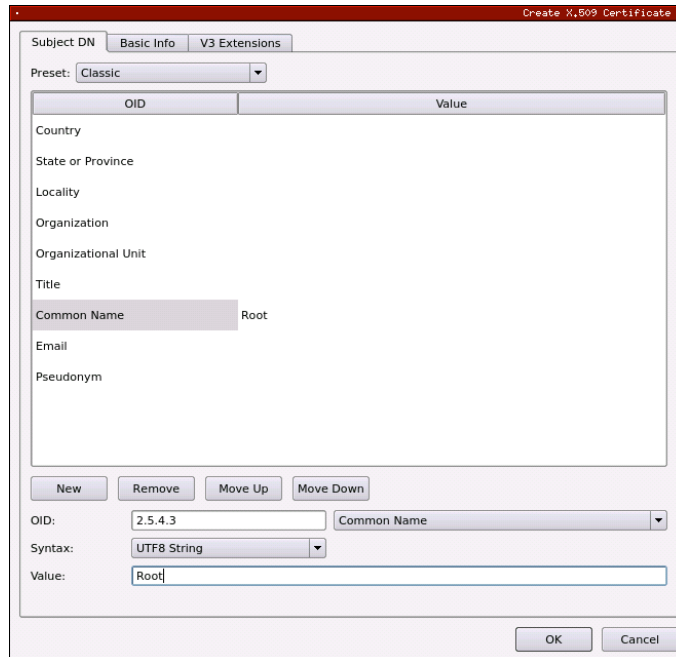
1. Log in to the KMES Series 3 application interface with the default Admin users.
2. Navigate to the *Certificate Authorities* menu, then click the **Add CA...** button.
3. Specify a name for the CA, then click **OK**.



4. Right-click on the newly created CA, then select **Add Certificate -> New Certificate....**



5. Change the **Preset** dropdown to "Classic", then set the **Common Name** value to "Root".

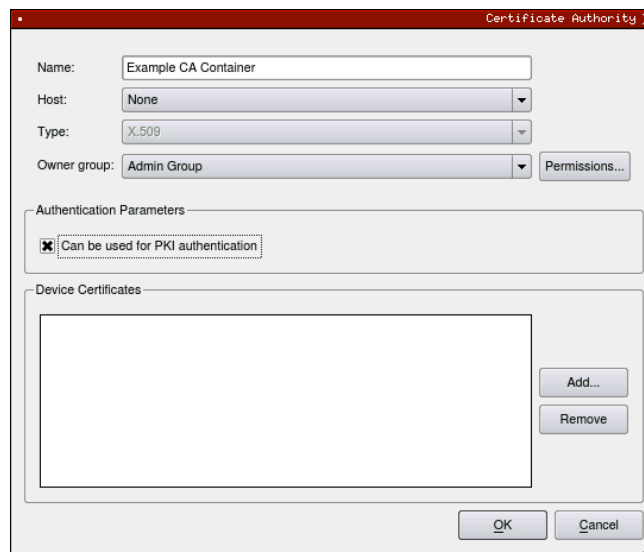


6. In the *Basic Info* tab, change the **Major key** to the "PMK". All other settings can be left as the default values.

7. In the *V3 Extensions* tab, set the **Profile** to "Example Certificate Authority", then click **OK** to save.

8. Right-click on the Certificate Container, then select **Edit...**

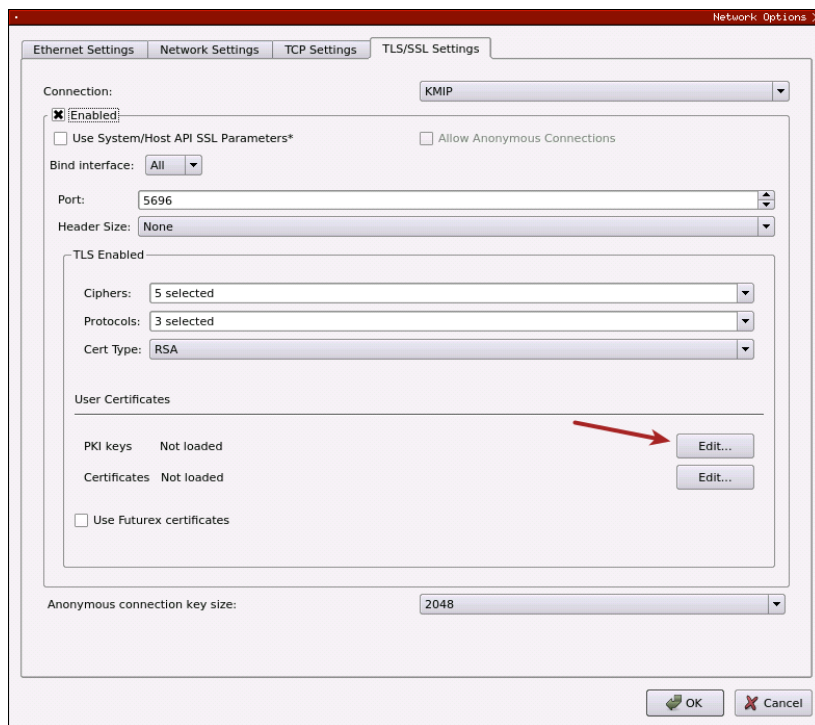
9. Give the CA permission to be used for PKI authentication by checking the box, as shown below, then click **OK**.



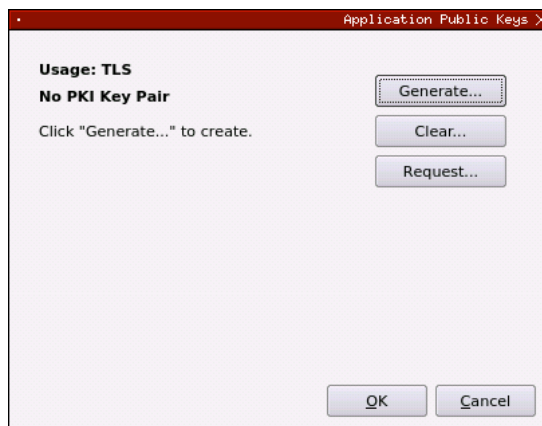
[3.2] CONFIGURE TLS CERTIFICATES FOR THE KMIP CONNECTION PAIR

[3.2.1] Generate a new PKI key pair and CSR for the KMIP connection pair

1. Navigate to the *Configuration* menu, then double-click on *Network Options*. Under the *TLS/SSL Settings* tab, click the **Connection** dropdown and select the **KMIP** connection pair.
2. Enable the KMIP connection pair if it is not already enabled.
3. Uncheck **Use System/Host API SSL Parameters** if it is selected.
4. In the User Certificates section, click the **Edit...** button next to PKI keys.

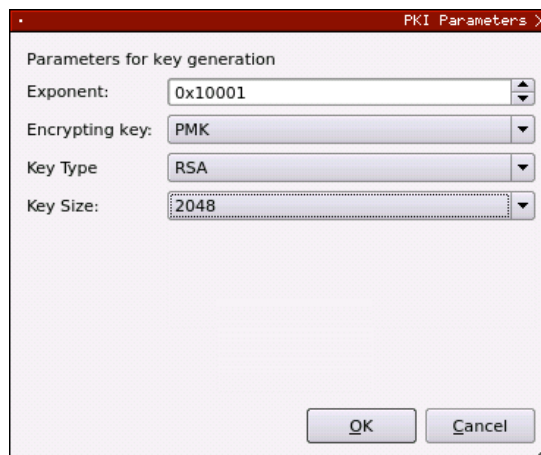


5. Click the **Generate...** button to create a new PKI Key Pair.



6. Click **Yes** and bypass the warning about SSL not being functional until new certificates are imported.

7. This will open the *PKI Parameters* dialog. Set the **PMK** as the Encrypting key, then change the Key Size to **2048**. Click **OK**.



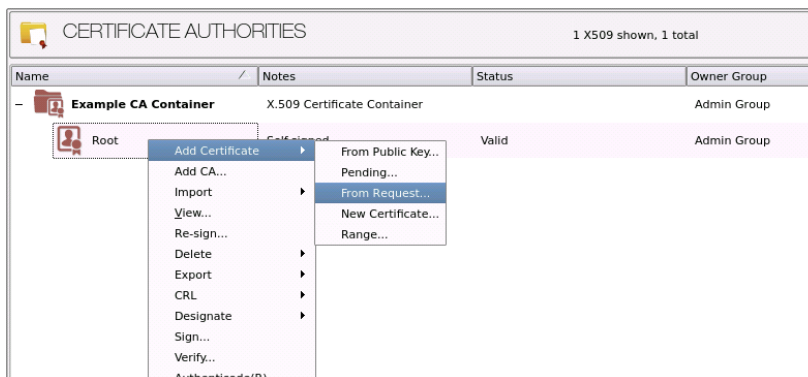
8. The *Application Public Keys* dialog should now show that the PKI Key Pair is **Loaded**. If this is the case, click **Request...**



9. The values in the *Subject DN* tab can be left as default. In the *V3 Extensions* tab, set the profile to **Example TLS Server Certificate**. In the *PKCS #10 Info* tab, specify a save location and name for the CSR file, then click **OK**.
10. A message box should appear saying that the certificate signing request was successfully written to the specified location. Click **OK** in this box.
11. Click **OK** in the *Application Public Keys* dialog, then click **OK** once more in the main *Network Options* dialog.

[3.2.2] Sign the KMIP connection pair CSR

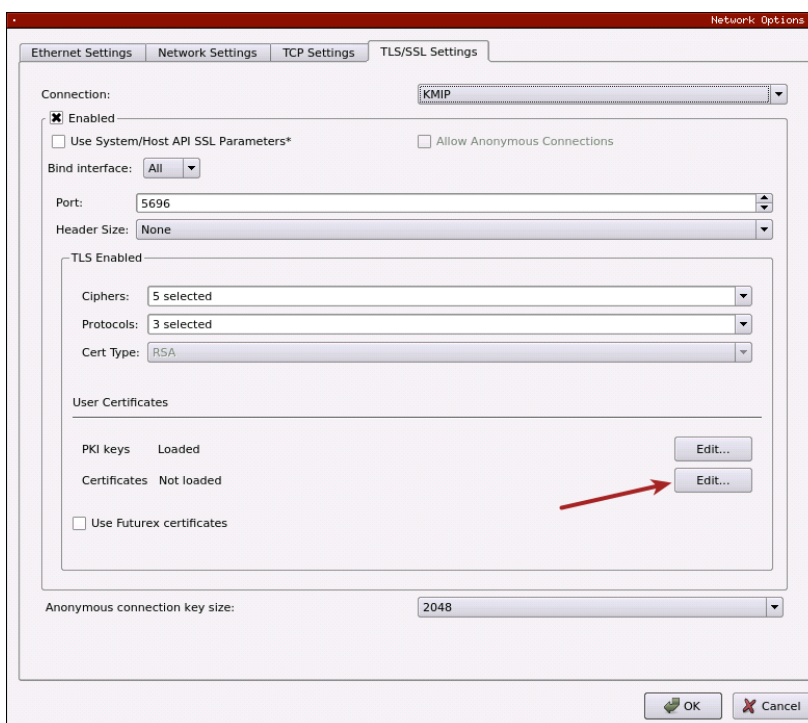
1. Navigate to the *Certificate Authorities* menu. Right-click on the Root CA certificate, then select **Add Certificate -> From Request...**



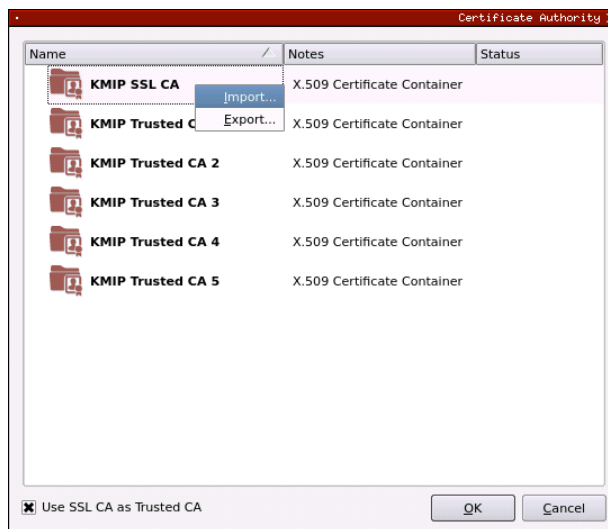
2. In the file browser, find and select the KMIP connection pair CSR. Certificate information should populate in the *Create X.509 From CSR* window.
3. Leave all settings exactly as they are and click **OK** to save.
4. The signed KMIP server certificate should be under the Root CA certificate in the CA tree now.

[3.2.3] Import the signed KMIP connection pair certificate

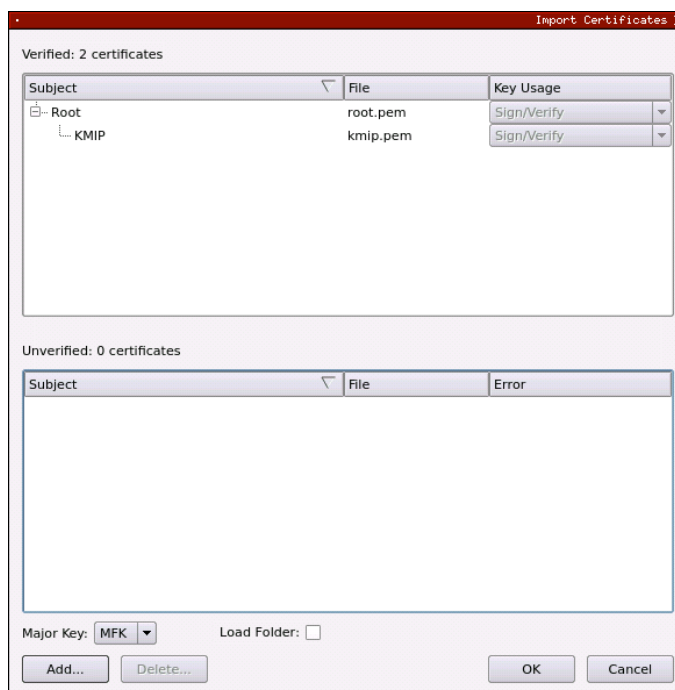
1. Navigate to the *Configuration* menu, then double-click on *Network Options*. Under the *TLS/SSL Settings* tab, click the **Connection** dropdown and select the **KMIP** connection pair.
2. In the User Certificates section, click the **Edit...** button next to Certificates.



- In the *Certificate Authority* dialog, right-click on the **KMIP SSL CA** X.509 Certificate Container, then select **Import....**



- In the *Import Certificates* dialog, click the **Add...** button at the bottom of the window. In the file browser, select both the root CA certificate and the signed KMIP server certificate and click **Open**. The certificates should now be listed in the "Verified" section of the *Import Certificates* dialog. Click **OK** to save.



- It should now say **Signed loaded** next to "Certificates" in the User Certificates section of the *Network Options* dialog. Click **OK** to save.

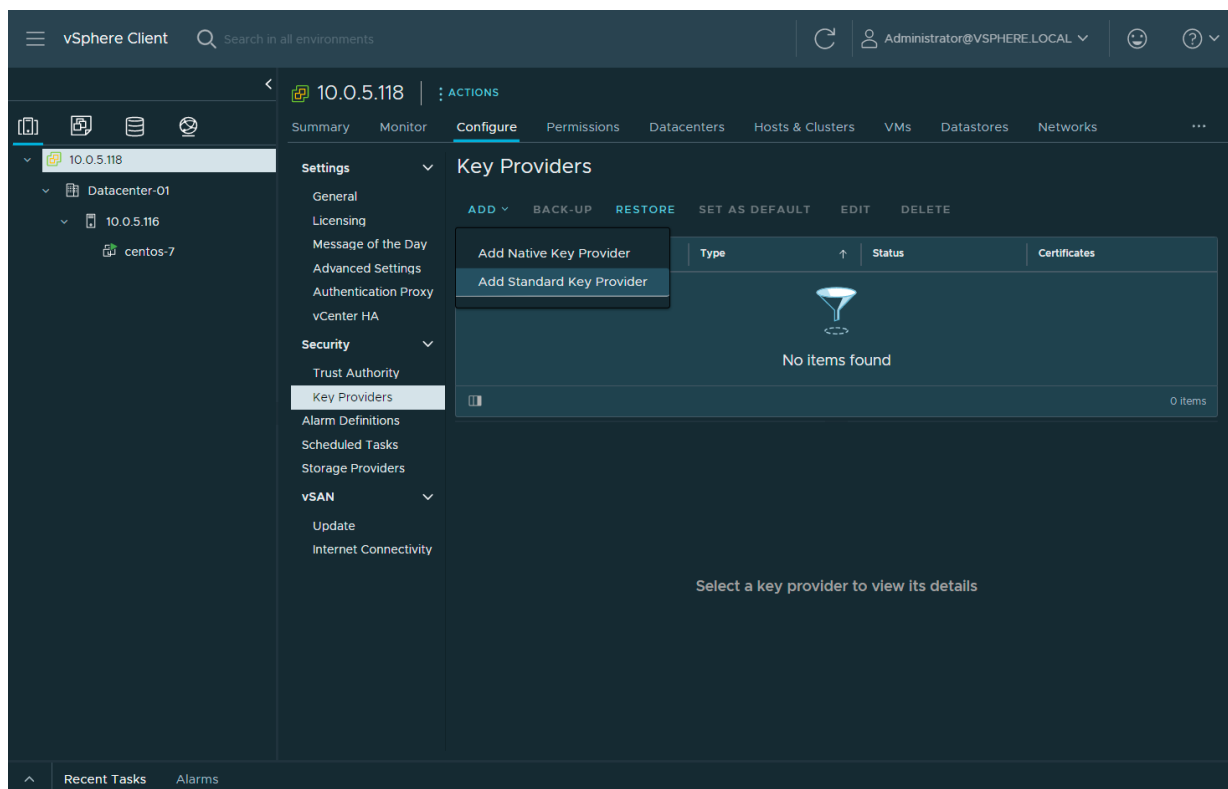
[4] REGISTER THE KMES SERIES 3 AS A STANDARD KEY PROVIDER IN VCENTER SERVER USING THE VSPHERE CLIENT

Before you can start with virtual machine encryption tasks, you must set up the standard key provider.

Setting up a standard key provider includes adding the key provider and establishing trust with the key server. When you add a key provider, you are prompted to make it the default. You can explicitly change the default key provider. vCenter Server provisions keys from the default key provider.

NOTE: What was previously called a Key Management Server cluster in vSphere 6.5 and 6.7 is now called a key provider.

1. Log in to the vCenter Server system with the vSphere Client.
2. Browse the inventory list and select the vCenter Server instance.
3. Click **Configure** and select **Key Providers** under **Security**.
4. Select **Add** -> **Add Standard Key Provider**.



5. Enter the key provider information then click **Add Key Provider**.

Add Standard Key Provider

Name: Futorex KMES Series 3

| KMS | Address | Port |
|-------------|------------------|-------------|
| <u>kmes</u> | <u>10.0.8.20</u> | <u>5696</u> |

> Proxy configuration (optional)

> Password protection (optional)

NOTE: The values specified in the **Name** and **KMS** fields can be anything. The IP of your KMES needs to be set in the **Address** field, and in the **Port** field, the port number for the KMIP connection pair on the KMES needs to be specified (it is 5696 by default). Disregard the **Proxy configuration** and **Password protection** fields.

- The TLS certificate that was configured for KMIP connection pair on the KMES should be presented. Click **Trust**.

Make vCenter Trust Key Provider

Futorex KMES Series 3

| | |
|---------------|---|
| Serial number | 0xFE53D200000068 |
| > Subject | KMIP |
| > Issuer | Root |
| Valid from | 01/05/2022, 6:00:00 PM |
| Valid to | 01/04/2023, 6:00:00 PM |
| Fingerprint | 86:79:9C:A6:53:92:1E:E0:51:85:88:C7:93:45:13:A8:60:39:AF:49 |
| > Certificate | Expand to view details |

The Futurex KMES Series 3 will now be listed as a key provider in the vSphere Client.

The screenshot shows the 'Key Providers' management interface in the vSphere Client. At the top, there are several action buttons: 'ADD', 'BACK-UP', 'RESTORE', 'SET AS DEFAULT', 'EDIT', and 'DELETE'. Below these buttons is a table with the following columns: 'Key Provider', 'Type', 'Status', and 'Certificates'. A single row is present in the table, representing the 'Futurex KMES Series 3 (default)' provider. The 'Type' is 'Standard', the 'Status' is '1 KMS not connected' (indicated by a yellow warning triangle), and the 'Certificates' column shows '1 certificate issue(s)' (also indicated by a yellow warning triangle). At the bottom right of the table area, it says '1 item'.

| Key Provider | Type | Status | Certificates |
|---------------------------------|----------|---------------------|------------------------|
| Futurex KMES Series 3 (default) | Standard | 1 KMS not connected | 1 certificate issue(s) |

[5] CONFIGURE TLS CERTIFICATES FOR VCENTER SERVER

As mentioned at the beginning of section 3, vCenter Server and the KMES Series 3 must establish a mutual trust relationship by validating their respective digitally signed certificates before KMIP connections can occur.

The steps completed in the previous two sections established vCenter's trust of the KMES. The steps in this section will establish the KMES's trust of vCenter.

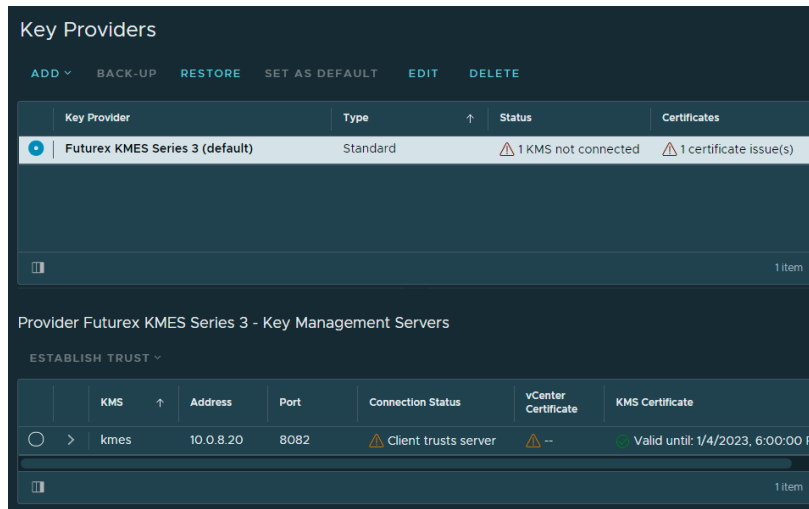
This will be accomplished by generating a Certificate Signing Request (CSR) in the vCenter Server system with the vSphere Client, signing the CSR using the Certificate Authority (CA) that was created on the KMES, then importing the signed certificate back into the vCenter Server system with the vSphere Client.

Once all of these steps are completed, vCenter Server and the KMES Series 3 will be able to establish a TCP/IP session secured by TLS, making it possible for KMIP connections, and therefore encryption operations, to occur.

[5.1] GENERATE A CERTIFICATE SIGNING REQUEST (CSR) WITH THE VSPHERE CLIENT

1. Log in to the vCenter Server system with the vSphere Client.
2. Browse the inventory list and select the vCenter Server instance.
3. Click **Configure** and select **Key Providers** under **Security**.
4. Select the Futurex KMES Series 3 key provider.

The KMS for the key provider is displayed.

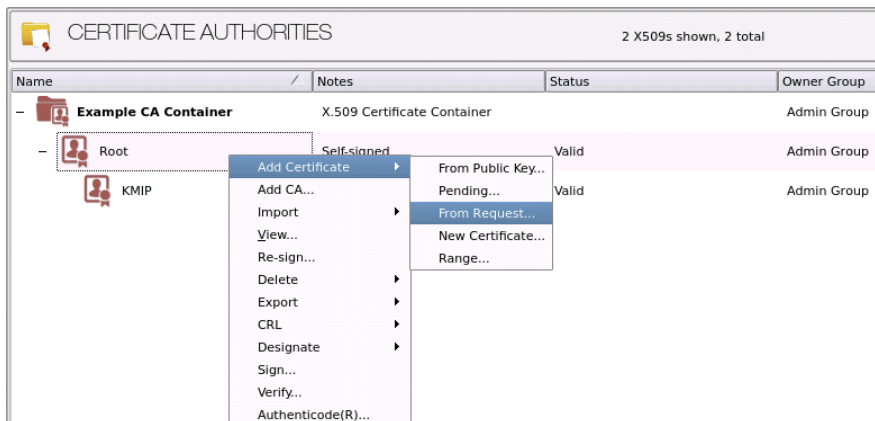


5. Select the "kmes" KMS, click the **Establish Trust** drop-down menu, and select **Make KMS trust vCenter**.
6. Select the **New Certificate Signing Request (CSR)** method and click **Next**.
7. In the dialog box, click **Download** to download the CSR as a file.

NOTE: The CSR file needs to be copied to the storage medium that is configured for the KMES.
8. Click **Done**.

[5.2] SIGN THE VCENTER CSR USING A CERTIFICATE AUTHORITY (CA) ON THE KMES

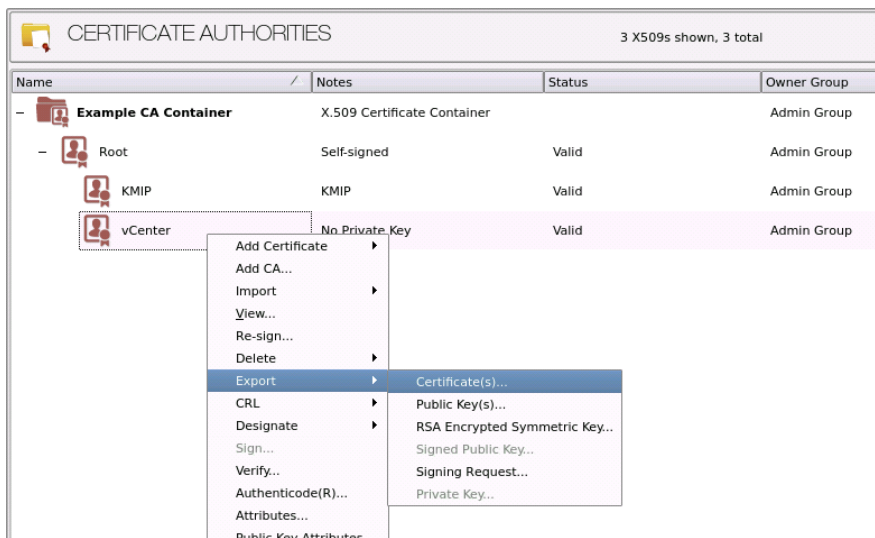
1. Log in to the KMES Series 3 application interface with the default Admin users.
2. Navigate to the *Certificate Authorities* menu, then right-click on the Root CA certificate created in section 3.1 and select **Add Certificate -> From Request...**



3. In the file browser, find and select the vCenter CSR.
4. In the *Subject DN* tab, change the Common Name value to a shorter string, such as "vCenter".
NOTE: The Common Name of the certificate needs to match the name of the user created in the next section so that vCenter will be able to authenticate to the KMES through TLS certificate authentication.
5. In the *V3 Extensions* tab, select the **Example TLS Client Certificate** profile.
6. Click **OK** to finish generating the signed vCenter certificate.

[5.3] EXPORT THE SIGNED VCENTER CERTIFICATE

1. Navigate to the *Certificate Authorities* menu, then right-click on the vCenter certificate and select **Export -> Certificate(s)...**



2. In the Export Certificate dialog, change the encoding to **PEM**, then click **Browse...**

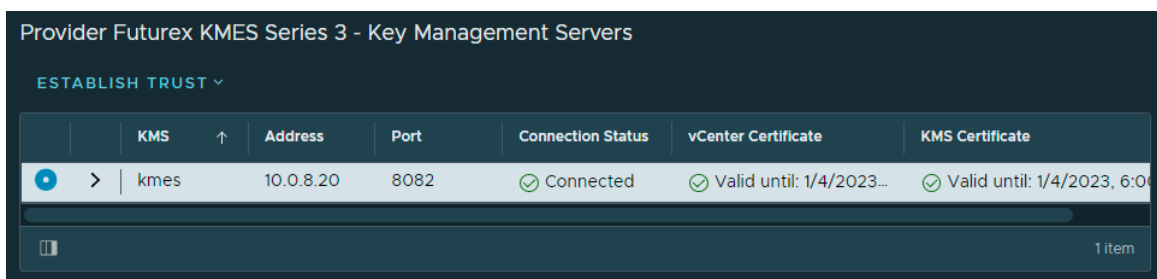
3. In the file browser, navigate to the location where you want to save the certificate. Specify a name for the file, then click **Open**.
4. Click **OK**. A message box will pop up stating that the PEM file was successfully written to the location that you specified.

NOTE: The signed vCenter certificate file needs to be copied from the KMES storage medium to the computer that is accessing vCenter Server via the vSphere Client.

[5.4] IMPORT THE SIGNED VCENTER CERTIFICATE INTO VCENTER SERVER WITH THE VSPHERE CLIENT

1. Log in to the vCenter Server system with the vSphere Client.
2. Browse the inventory list and select the vCenter Server instance.
3. Click **Configure** and select **Key Providers** under **Security**.
4. Select the Futurex KMES Series 3 key provider.
The KMS for the key provider is displayed.
5. Select the "kmes" KMS, click the **Establish Trust** drop-down menu, and select **Upload Signed CSR Certificate**.
6. Click **Upload A File**, then find and select the signed vCenter certificate in the file browser. The content of the certificate should populate in the window.
7. Click **Upload**.

The **Connection Status** column should now have a green checkmark and say "Connected". The **vCenter Certificate** and **KMS Certificate** columns should also show green checkmarks, with certificate validity dates sometime in the future.



| Provider Futurex KMES Series 3 - Key Management Servers | | | | | | |
|---|------|-----------|------|-------------------|----------------------------|-------------------------------|
| ESTABLISH TRUST ▾ | | | | | | |
| | KMS | Address | Port | Connection Status | vCenter Certificate | KMS Certificate |
| • > | kmes | 10.0.8.20 | 8082 | ✓ Connected | ✓ Valid until: 1/4/2023... | ✓ Valid until: 1/4/2023, 6:00 |

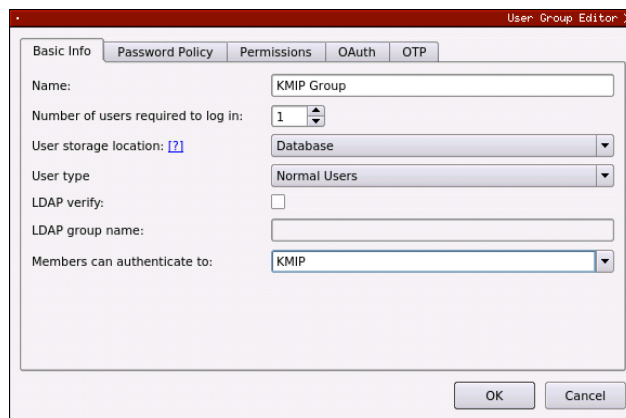
1 item

[6] CREATE A USER ON THE KMES SERIES 3 FOR VCENTER SERVER

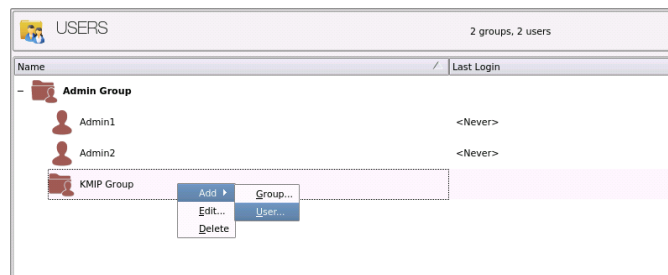
In this section, a user will be created on the KMES with the permissions that vCenter requires to generate keys that can be used for various encryption tasks within vSphere.

As mentioned briefly in the previous section, the name of the user that is created needs to match exactly the Common Name of the vCenter TLS certificate. This will allow vCenter to authenticate with the KMES via the certificate.

1. Log in to the KMES Series 3 application interface with the default Admin users.
2. Navigate to the *Users* menu, then click the **Add Group...** button.
3. In the *Basic Info* tab, set the fields to how they are shown below (**NOTE:** The name of the group can be anything.)



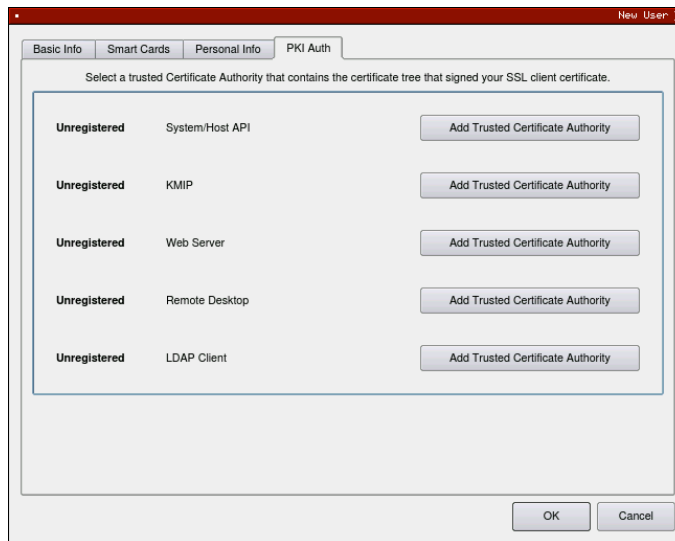
4. Go directly to the *Permissions* tab and enable all **Manage keys** permissions for the group.
5. Click **OK** to save.
6. Right-click on the newly created User Group, then select **Add -> User...**



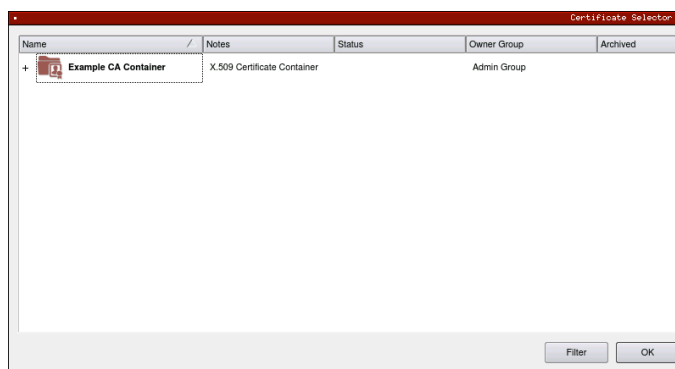
7. In the **User name** field, type in "vCenter" to match the Common Name of the vCenter TLS certificate. Also uncheck the **Allow password login** option.

NOTE: If a name other than "vCenter" was set as the Common Name of the vCenter TLS certificate, set whichever name was set as the name for the user.

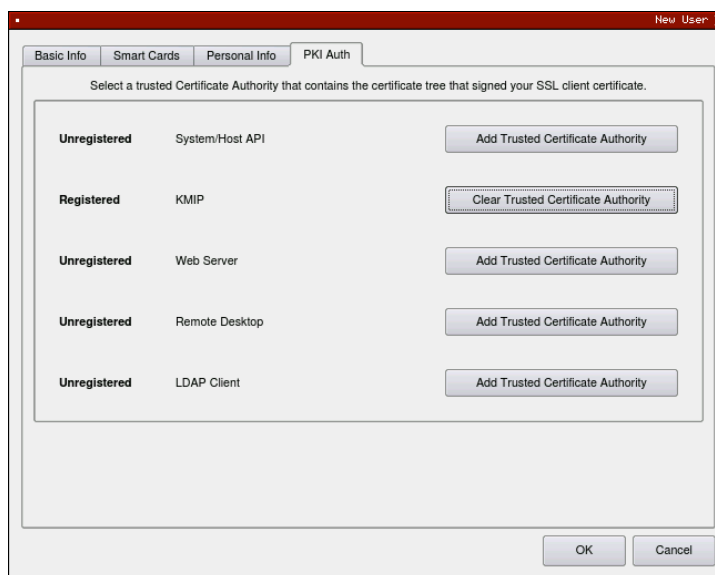
8. Navigate to the *PKI Auth* tab, then click the **Add Trusted Certificate Authority** button next to KMIP.



9. Select the CA container that the signed vCenter certificate is in, then click **OK**.



10. It should show "Registered" next to KMIP now. Click **OK** to save.



[7] VM AND VSAN ENCRYPTION IN VSPHERE

Now that the KMES Series 3 is set up as a key provider in vCenter Server, vSphere users with the required privileges can [create encrypted virtual machines and disks](#). Those users can also [encrypt existing virtual machines](#) and [decrypt encrypted virtual machines](#), and [add Virtual Trusted Platform Modules \(vTPMs\) to virtual machines](#).

In addition to virtual machine encryption, users can [encrypt data-in transit for vSAN clusters](#), and [encrypt data-at-rest in vSAN datastores](#).

In this section, encrypting an existing virtual machine will be demonstrated. Please refer to the VMware documentation linked above for instructions on performing the other various encryption tasks that the vSphere / KMES Series 3 KMIP integration makes possible.

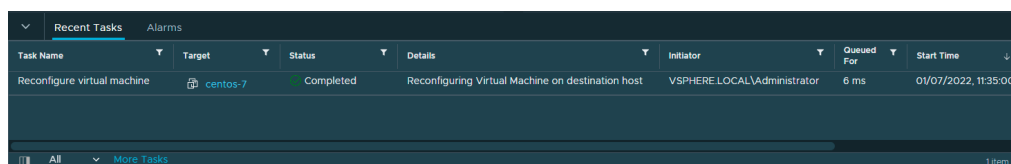
[7.1] ENCRYPTING AN EXISTING VIRTUAL MACHINE WITH THE VSPHERE CLIENT

Existing virtual machines or virtual disks can be encrypted by changing their storage policy. Virtual disks can only be encrypted for encrypted virtual machines.

NOTE: Ensure that the virtual machine is powered off.

1. Log in to the vCenter Server system with the vSphere Client.
2. Right-click the virtual machine that you want to change and select **VM Policies** -> **Edit VM Storage Policies**.
You can set the storage policy for the virtual machine files, represented by VM home, and the storage policy for virtual disks.
3. Select the **VM Encryption Policy** in the dropdown.
 - To encrypt the VM and its hard disks, select an encryption storage policy and click **OK**.
 - To encrypt the VM but not the virtual disks, toggle on **Configure per disk**, select the encryption storage policy for VM Home and other storage policies for the virtual disks, and click **OK**.
4. If you prefer, you can encrypt the virtual machine, or both virtual machine and disks, from the **Edit Settings** menu in the vSphere Client.
 - a. Right-click the virtual machine and select **Edit Settings**.
 - b. Select the **VM Options** tab, and open **Encryption**. Choose an encryption policy. If you deselect all disks, only the VM home is encrypted.
 - c. Click **OK**.

If the VM encryption operation is successful the status of the task will show as **Completed**.

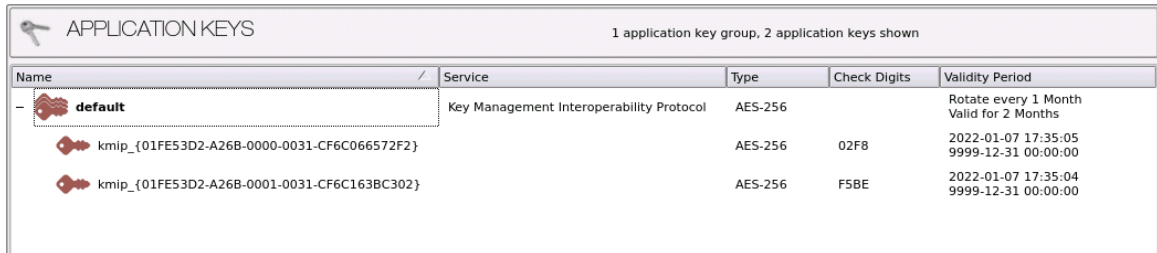


| Task Name | Target | Status | Details | Initiator | Queued For | Start Time |
|-----------------------------|----------|-----------|---|-----------------------------|------------|----------------------|
| Reconfigure virtual machine | centos-7 | Completed | Reconfiguring Virtual Machine on destination host | VSPHERE.LOCAL\Administrator | 6 ms | 01/07/2022, 11:35:00 |

[7.2] VIEWING THE KEYS THAT VSPHERE CREATED ON THE KMES

1. Log in to the KMES Series 3 application interface with the default Admin users.
2. Navigate to the *Application Keys* menu, then expand the **default** application key group by clicking the plus (+) sign next to it.

We can see that vSphere created two AES-256 symmetric keys, which it used to encrypt the virtual machine in the previous step.



| Name | Service | Type | Check Digits | Validity Period |
|--|--|---------|--------------|--|
| default | Key Management Interoperability Protocol | AES-256 | | Rotate every 1 Month Valid for 2 Months |
| kmp_{01FE53D2-A26B-0000-0031-CF6C066572F2} | | AES-256 | 02F8 | 2022-01-07 17:35:05 9999-12-31 00:00:00 |
| kmp_{01FE53D2-A26B-0001-0031-CF6C163BC302} | | AES-256 | F5BE | 2022-01-07 17:35:04 9999-12-31 00:00:00 |

APPENDIX A: XCEPTIONAL SUPPORT



In today's high-paced environment, we know you are looking for timely and effective resolutions for your mission-critical needs. That is why our Xceptional Support Team does whatever it takes to ensure you have the best experience and support possible. Every time. Guaranteed.

- 24x7x365 mission critical support
- Level 1 to level 3 support
- Extremely knowledgeable subject matter experts

At Futurex, we strive to supply you with the latest data encryption innovations as well as our best-in-class support services. Our Xceptional Support Team goes above and beyond to meet your needs and provide you with exclusive services that you cannot find anywhere else in the industry.

- Technical Services
- Onsite Training
- Virtual Training
- Customized Consulting
- Customized Software Solutions
- Secure Key Generation, Printing, and Mailing
- Remote Key Injection
- Certificate Authority Services

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com



ENGINEERING CAMPUS

864 Old Boerne Road
Bulverde, Texas, USA 78163
Phone: +1 830-980-9782
+1 830-438-8782
E-mail: info@futurex.com

EXCEPTIONAL SUPPORT

24x7x365
Toll-Free: 1-800-251-5112
E-mail: support@futurex.com

SOLUTIONS ARCHITECT

E-mail: solutions@futurex.com