VMware Cloud Director Encryption Management 1.2.0

Table of Contents

VMware Cloud Director Encryption Management Documentation

VMware Cloud Director Encryption Management is a solution add-on which grants tenant administrators the ability to use encryption keys from their own key providers for encryption of virtual machines (with or without vTPM devices), vApp templates, and named disks in their VMware Cloud Director virtual data centers (VDCs).

What's new in VMware Cloud Director Encryption Management 1.2

- As a service provider, you can perform the following tasks.
  - Register a key provider cluster, that consists of multiple servers, which are configured in high availability and improve service reliability.
  - Publish a key provider with a custom name.
- As a tenant administrator, you can perform the following tasks.
  - Use a unique encryption key for each object in your organization VDC.
  - Create a rotation schedule for your encryption keys.
  - Encrypt objects with a specific encryption policy, depending on the storage policy you use in your VDC.
  - Avoid re-encryption of the objects in your VDC, when removing an encryption policy.

How to set up VMware Cloud Director Encryption Management

As a cloud provider, follow these steps to set up VMware Cloud Director Encryption Management for tenant organizations.

1. Install VMware Cloud Director Encryption Management in a configured solution landing zone in your VMware Cloud Director environment.
2. Register key providers through VMware Cloud Director Encryption Management and associate them with vCenter Servers.
3. Publish key providers to tenant organizations.

Once a key provider is published for a tenant, they gain access to VMware Cloud Director Encryption Management.

As a tenant administrator, follow these steps to complete the key provider configuration:

1. Authenticate to your key provider through VMware Cloud Director Encryption Management.
2. Set up keys for encryption of VMs, vApp templates, and non-shared named disks in your VDCs.

How to upgrade VMware Cloud Director Encryption Management

You upgrade VMware Cloud Director Encryption Management as all standard add-on solutions for VMware Cloud Director. See Upgrade a Solution Add-On Instance in VMware Cloud Director.

> **NOTE**
> Before upgrading your VMware Cloud Director to version 10.6, first upgrade VMware Cloud Director Encryption Management to version 1.2.

Table 1: VMware Cloud Director Encryption Management compatibility with VMware Cloud Director

	VMware Cloud Director 10.5	VMware Cloud Director 10.6
VMware Cloud Director Encryption Management 1.1	#	#
VMware Cloud Director Encryption Management 1.2	#	#

Installing and Configuring VMware Cloud Director Encryption Management as a Cloud Provider

As a cloud provider, refer to the content in this chapter to learn how to set up VMware Cloud Director Encryption Management for your tenants.

Before you begin

Before you install and configure the VMware Cloud Director Encryption Management solution, you must first prepare your environment.

The VMware Cloud Director Encryption Management appliance requires your VMware Cloud Director environment to be configured in a specific way. To prepare all components in your environment, ensure you satisfy the requirements in the following table.

Product	Requirements
vSphere	• A default key provider must be defined. **NOTE** For vSphere 8.0 and later, you can configure a native or standard key provider as the default key provider. For all other versions, you must configure a standard key provider as the default one. For more details about vSphere encryption support, refer to *Virtual Machine Encryption Interoperability* in the *vSphere Documentation*.
VMware Cloud Director	• Running version 10.5.1 • Configure an organization VDC capable of running VMs as the solution landing zone for the VMware Cloud Director Encryption Management solution add-on. Refer to *Configure Solution Landing Zone* in the *VMware Cloud Director Documentation*. • The smallest appliance size for VMware Cloud Director Encryption Management solution is 2 vCPU and 4 GB memory. Larger sizes are available but not needed unless you are supporting encryption of many objects. You must secure enough resources in your solution landing zone to run the appliance. • One or more storage policies with encryption enabled (VM Encryption Policy) added to your provider VDC and organization VDCs.
Key Provider	• Obtain the key provider's IP address, port, and proxy settings. • vCentre Server must have network connectivity to the key provider. The default key provider port is 5696. • Verify that the key provider is included in *VMware Compatibility Guide for Key Management Servers (KMS)*. • The key provider cannot be vSphere Native Key Provider.
VMware Cloud Director Encryption Management	• Log in to the Broadcom Support Portal and download the VMware Cloud Director Encryption Management ISO file.

Installing VMware Cloud Director Encryption Management

You install VMware Cloud Director Encryption Management on a configured VMware Cloud Director solution landing zone.

Make sure your environment is prepared.

1. Open the VMware Cloud Director provider portal.
2. From the side navigation bar, expand **More** and select **Solution Add-On Management**.
3. Click **UPLOAD**.
4. Click **Browse Files** and select the VMware Cloud Director Encryption Management ISO on your local drive.
5. Make sure **Create add-on instance after upload is completed** is checked.
6. Click **UPLOAD**.
7. Once the upload is completed, click **Finish**.
8. Accept the VMware license agreement.
9. Enter the solution input parameters.
   a) Enter a name for the VMware Cloud Director Encryption Management add-on instance.
   b) Select the deployment configuration.
   c) Optional: Enter the name of an existing global role which will be granted full access to VMware Cloud Director Encryption Management.

      The default global role is the built-in Organization Administrator. If the specified global role does not exist in the system, the solution will still operate but no access is granted to tenants. For information how to grant access after the installation is complete, see View and Edit a Global Tenant Role Using Your VMware Cloud Director in the *VMware Cloud Director* documentation.
   d) Click **Next**.
10. On the final step of the wizard, review the details and click **Finish**.

The solution is being installed with a **PENDING** installation status. Wait until the installation status is **READY** and reload the browser page, before proceeding with configuring VMware Cloud Director Encryption Management.

Register key provider with VMware Cloud Director Encryption Management

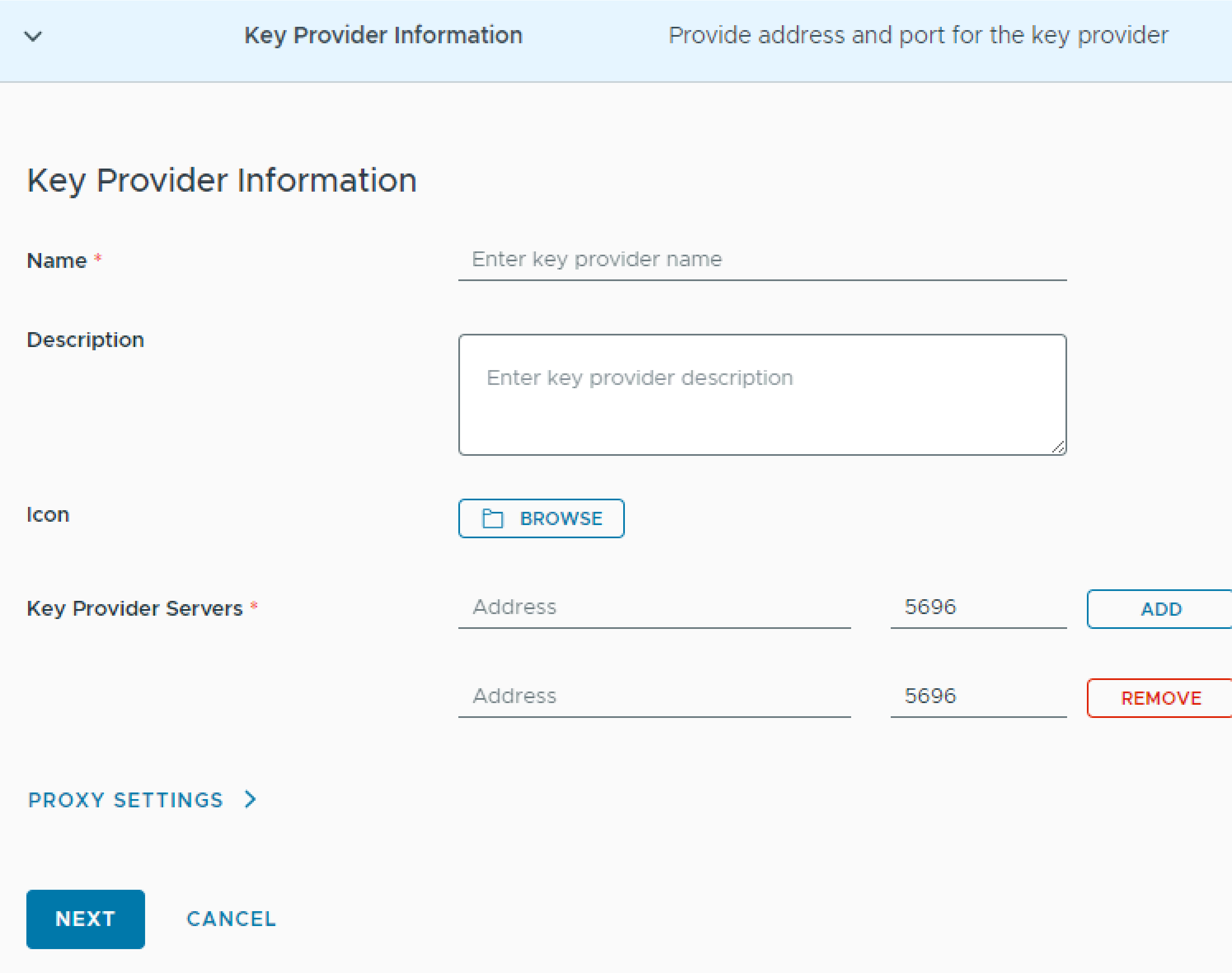
You register a key provider with VMware Cloud Director Encryption Management and associate it with a vCenter Server.

- Verify that VMware Cloud Director Encryption Management is installed in your environment.
- Obtain the IP addresses and ports of the key provider servers you are registering. The default port is 5696.

1. From the side navigation bar, expand **More** and select **Encryption Management**.

   If this is the first key provider you are registering, an introductory page is displayed.

2. To register a key provider, click **Get Started** or **Register**.
3. Fill in the key provider details.



Key Provider Information — Provide address and port for the key provider

Key Provider Information

Name * Enter key provider name

Description Enter key provider description

Icon BROWSE

Key Provider Servers * Address 5696 ADD

Address 5696 REMOVE

a) Enter a key provider name.
b) Optional: Enter a description.
   This description will be visible to tenant administrators.
c) Optional: To upload an icon from your local drive, click **Browse**.
d) Enter a key provider server IP address and port.
e) Optional: To add more key provider servers, select **ADD** and enter the server's IP address and port.

> **NOTE**
> Additional key provider servers ensure high availability of the service. The servers must share the same encryption keys.

   f) Optional: To set up a proxy, expand **PROXY SETTINGS** and enter the proxy address and port.
   g) Click **Next**.

4. Select the vCenter Server to be associated with the key provider.

   If you are registering a key provider with a selected vCenter Server for the first time, you are prompted to enter the vCenter Server username and password.

5. Click **Register**.

   You are prompted to validate and trust the certificates of the key provider servers.

Publish key provider to tenant organization

To grant tenant access to a key provider, you publish a key provider registered in VMware Cloud Director Encryption Management to a tenant organization.

1. From the side navigation bar, expand **More** and select **Encryption Management**.
2. Next to a key provider, click the **vertical-ellipsis icon (⋮)** > **Publish**.
3. From the list of organizations, select the ones you want to publish the key providers to.
4. Optional: Under **Cluster Name**, enter a custom key provider name for each tenant organization.

   > **NOTE**
   > After you publish a key provider to your tenants, you cannot change the cluster name of the key provider.

5. Click **PUBLISH**.

Unpublish key provider from a tenant

If you want to revoke a tenant organization's access to a key provider, you can unpublish the key provider from their organization.

To unpublish a key provider, vSphere must be configured with a default key provider or there must be no tenant objects encrypted with the key provider you want to unpublish.

1. From the side navigation bar, expand **More** and select **Encryption Management**.
2. Click the name of the key provider you want to unpublish.
3. Under **Organizations**, next to the organization you want to unpublish the key provider from, click the **vertical-ellipsis** icon (⋮) and click **Unpublish**.
4. Move the slider to the right, review the information and if you agree, select the check box, and click **UNPUBLISH**.

The unpublish process runs in the background. The organization is revoked access to the key provider and all affected objects are re-encrypted with vSphere's default key provider.

Edit key provider

You can edit a registered key provider's details and network configuration.

> **IMPORTANT**
>
> If you edit the network configuration of a key provider, all tenants with access to the key provider must re-authenticate to it before they can use it again. Failiure to authenticate after changing the network configuration

may prevent tenants from performing operations on existing encrypted objects as well as create new encrypted ones. You are responsible of notifying your tenants about this change.

1. From the side navigation bar, expand **More** and select **Encryption Management**.
2. Click the name of the key provider you want to edit.
3. Click **Edit**.
4. Edit the key provider details.
   a) Enter a key provider name.
   b) Optional: Enter a description.
   c) Optional: To upload an icon from your local drive, click **Browse**.
   d) Enter a key provider server IP address and port.
   e) Optional: To add more key provider servers, select **ADD** and enter the server's IP address and port.

      NOTE
      Additional key provider servers ensure high availability of the service. The servers must share the same encryption keys.

   f) Optional: To set up a proxy, expand **PROXY SETTINGS** and enter the proxy address and port.
   g) Click **SUBMIT**.

Using VMware Cloud Director Encryption Management as a Tenant

As a tenant, refer to the content in this chapter to learn how to configure and manage encryption with VMware Cloud Director Encryption Management.

Encrypting objects in VDCs

With VMware Cloud Director Encryption Management, you can encrypt VMs, vApp templates and non-shared named disks in your VDCs with keys from your key provider. Encryption of VMs with Virtual Trusted Platform Module (vTPM) is also supported. Encrypting objects with VMware Cloud Director Encryption Management works the same way as encryption normally does in VMware Cloud Director. For more details about encryption in VMware Cloud Director, refer to Virtual Machine Encryption in the *VMware Cloud Director Documentation*.

Set up key provider

You set up your key provider for encryption by authenticating to it with your credentials and setting up your encryption policies.

- You have a third-party key provider account and access to the key provider credentials.
- Your cloud provider has already registered and published the key provider to your organization.
- You must have a tenant role which grants you the right to configure key providers.

1. From the side navigation bar, expand **More** and select **Encryption Management**.
2. In the card of an available key provider, click **Configure**.
3. Fill in your vCenter Server user credentials or the client certificate and private key of your key provider and click **REGISTER**.

   Some key providers support only one authentication method while others may give you choice. For more information, refer to the documentation of your key provider.

4. Generate a new key in your key provider.
   a) Select a key type.

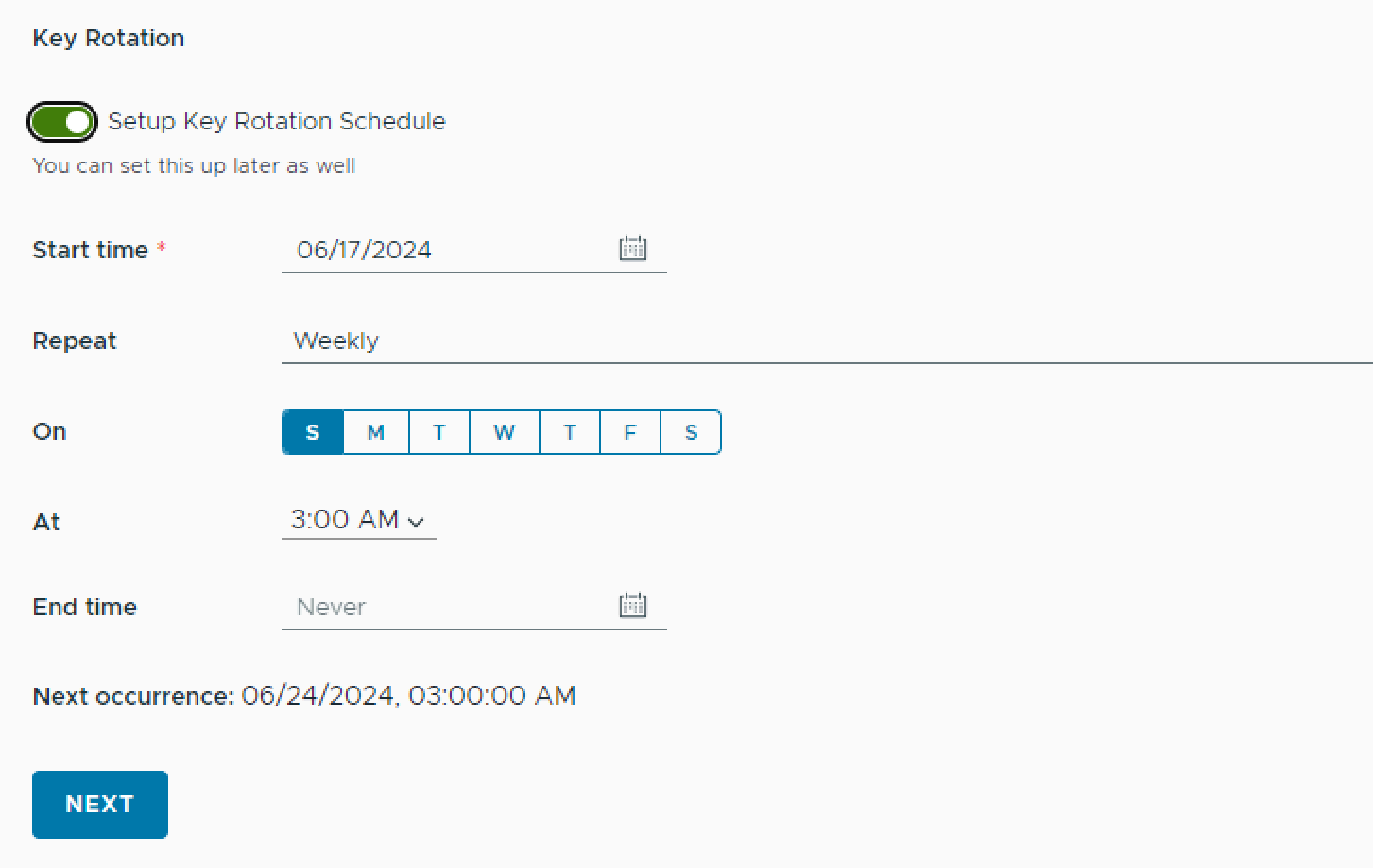
      - To use the same encryption key for all objects, select **Use the same key every time** and click **GENERATE KEY**. Alternatively you can paste the ID of a pre-generated key.

NOTE
You must use AES-256 key type. For more information on how to find a key ID in your key provider, refer to the documentation of your key provider.

- To use a unique encryption key for all objects, select **Generate a new key every time**.

b) Optional: Specify a rotation schedule for your encryption keys.

You can rotate your encryption keys on daily, weekly, or monthly basis.



Key Rotation

Setup Key Rotation Schedule

You can set this up later as well

Start time * 06/17/2024

Repeat Weekly

On S M T W T F S

At 3:00 AM

End time Never

Next occurrence: 06/24/2024, 03:00:00 AM

5. Select which organization VDCs will use this key for encryption.
6. Select a storage policy.
   - To use the encryption key for all existing storage policies in your VDC, select **All storage policies**.
   - To use the encryption key for specific storage policies only, select **Specific storage policies** and click the check boxes next to the listed storage policie names.
7. Review your encryption details and click **SUBMIT**.

The encryption process runs in the background, re-encrypting all affected objects with the specified key.

Configure virtual data center encryption policy

You can encrypt virtual data centers (VDCs) without an associated key provider or override the encryption of already encrypted VDCs.

1. From the side navigation bar, expand **More** and select **Encryption Management**.
2. Click the name of the key provider you want to use.
3. Click **ENCRYPT ORG VDCS**.
4. Generate a new key in your key provider.
   a) Select a key type.
      - To use the same encryption key for all objects, select **Use the same key every time** and click **GENERATE KEY**. Alternatively you can paste the ID of a pre-generated key.

        NOTE
        You must use AES-256 key type. For more information on how to find a key ID in your key provider, refer to the documentation of your key provider.
      - To use a unique encryption key for all objects, select **Generate a new key every time**.

   b) Optional: Specify a rotation schedule for your encryption keys.

      You can rotate your encryption keys on daily, weekly, or monthly basis.
5. Select which organization VDCs will use this key for encryption.
6. Select a storage policy.
   - To use the encryption key for all existing storage policies in your VDC, select **All storage policies**.
   - To use the encryption key for specific storage policies only, select **Specific storage policies** and click the check boxes next to the listed storage policie names.
7. Review your encryption details and click **SUBMIT**.

The encryption process runs in the background, re-encrypting all affected objects with the specified key.

Change virtual data center encryption policy

You can change the encryption policy details of your virtual data center (VDC).

1. From the side navigation bar, expand **More** and select **Encryption Management**.
2. Click the name of the key provider you want to use.
3. Under **Encryption Policies**, next to your VDC, click the **vertical-ellipsis** icon (⋮) and click **Edit Encryption Policy**.
4. Change the encryption key type and rotation schedule.
   a) Select a key type.
      - To use the same key for all objects in your VDC, select **Use the same key every time** and click **GENERATE KEY**. Alternatively you can paste the ID of a pre-generated key.

        NOTE
        You must use AES-256 key type. For more information on how to find a key ID in your key provider, refer to the documentation of your key provider.
      - To use a dedicated encryption key for all objects in your VDC, select **Generate a new key every time**.

   b) Optional: Specify a rotation schedule for your encryption keys.

      You can rotate your encryption keys on daily, weekly, or monthly basis.

5. Optional: Change your storage policy.
    - To use the encyption key for all existing storage policies in your VDC, select **All storage policies**.
    - To use the encryption key for specific storage policies only, select **Specific storage policies** and click the check boxes next to the listed storage policie names.

      NOTE
      If you change your storage policy encryption from **All storage policies** to **Specific storage policies**, newly created storage policies on the selected organisation VDC are not assigned automatically to your encryption policy. You must manually select and assign these from the list.
6. Review your changes and click **SUBMIT**.

The encryption process runs in the background, re-encrypting all affected objects with the specified key.

Remove virtual data center encryption policy

You can deactivate the encryption of a virtual data center (VDC) by removing the policy used for encryption.

To remove your current encyption policy, your vCenter instance must be configured with a default key provider. Alternativelty, if no default key provider is configured and there are encrypted objects in that VDC, when you deactivate the encryption policy, the objects in the VDC become unreachable after being powered off. For more information, refer to the vCenter documentation.

1. From the side navigation bar, expand **More** and select **Encryption Management**.
2. Click the name of the key provider used to encrypt the VDC you want to manage.
3. Under **Encryption Policies**, next to your VDC, click the **vertical-ellipsis** icon (⋮) and click **Remove Encryption Policy**.
4. Remove the encyption policy.
    - To remove your encryption policy and use the default key provider that you configured in your vCenter instance, select **Re-encrypt using the Default Key Provider** and click **REMOVE**.
    - To remove your encryption policy without specifying a new policy, select **Do not re-encrypt**.
        a. To remove the encyption keys that are cached in vSphere, select **Purge keys cache**.
        b. To power off your encrypted objects, select **Power Off encrypted VMs**.
        c. Enter the name of your VDC and click **REMOVE**.

The process runs in the background for all affected objects.

Troubleshooting VMware Cloud Director Encryption Management as a Cloud Provider

If you lose connectivity or encounter an error when trying to access VMware Cloud Director Encryption Management, you can troubleshoot and remediate your appliance.

Command-line interface and common parameters

You can fetch logs and check the status of a VMware Cloud Director Encryption Management appliance by mounting the ISO file and interfacing with it through command-line. To authenticate your actions, you need to always enter the following authentication parameters as part of your commands:

Parameter	Description
`--host`	VMware Cloud Director host name, where VMware Cloud Director Encryption Management is installed.
`--username`	The user name used to authenticate to the host VMware Cloud Director.
`--password`	The password used to authenticate to the host VMware Cloud Director.
`--insecure` or `--certificate-file`	To ignore certificate validation, use `--insecure` . Alternatively use `--certificate-file` and enter the path to the file with the trusted certificates for validation.

The authentication parameters in the table are hereafter referred to as `common_parameters` .

1. Fetching and analyzing the log files

The first step in troubleshooting errors with your VMware Cloud Director Encryption Management appliance is to fetch and analyze the log files. There are three types of logs you can fetch:

Log name	Type of events containted in log file
`byok.log`	Contains information and warning events.
`byok-error.log`	Contains error events.
`byok-debug.log`	Contains all events, including information, warning, error, debug, and trace events.

1. Mount the VMware Cloud Director Encryption Management ISO file using command-line interface and navigate to the `cli>your_operating_system` folder.
2. Run the fetch log command, replacing `<log_name>` with the type of log you want to fetch.

   ```
   vcdemctl appliance logs [common_parameters] --log-name <log_name> --all
   ```
3. If you are able to fetch the logs, open them and analyze them for errors. In the `byok-debug.log` log, scroll down until you see the "`Server started`" event. If there are no errors afterwards, your appliance is running and operational.
4. If there are errors after the "`Server started`" event, go to step 3 to remediate your appliance.
5. If you get an error when trying to fetch the logs, it may be because the appliance lost connectivity to VMware Cloud Director. Go to step 2.

2. Check appliance status

If you cannot access the logs of your VMware Cloud Director Encryption Management appliance, you need to check the status and network connectivity of the appliance.

1. Mount the VMware Cloud Director Encryption Management ISO file using command-line interface and navigate to the `cli>your_operating_system` folder.

2. Run the command to check the status of your appliance.

   ```
   vcdemctl appliance status [common_parameters]
   ```

   The payload returns data about the status of your appliance.

   > **IMPORTANT**
   >
   > The returned status is not real-time but is updated every 30 minutes.

   If your appliance is running bot not operational, continue with the procedure.
3. Ensure that virtual machine of the appliance has newtork connectivity with the VMware Cloud Director public endpoint.
4. In the VMware Cloud Director administrator portal, go to **Administration** > **Provider Access Control** > **Service Accounts** and ensure the `encryption-managemenet-system-user` service account is active.

When you are done ensuring that all components are properly set up, go back to step 1 and try to fetch the logs again. If you are able to fetch the logs, VMware Cloud Director Encryption Management is most likely operational. If you still experience errors, contact VMware support and provide them with the logs.

In case you still cannot fetch the logs or there are errors in the logs, go to step 3.

3. Remediate VMware Cloud Director Encryption Management

You can remediate the VMware Cloud Director Encryption Management appliance.

1. On the VMware Cloud Director toolbar, click **More** > **Solution Add-On Management**.
2. Click **Encryption Management**.
3. Next to the instance you want to remediate, click the **vertical-ellipsis icon (⋮)** > **Remediate**.
4. Click **Confirm**.
5. Once the remediation process is complete, refresh your browser and try to access VMware Cloud Director Encryption Management again.

If your issue persists, open a support ticket.

Documentation Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Broadcom at any time. This Documentation is proprietary information of Broadcom and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Broadcom.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Broadcom copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Broadcom that all copies and partial copies of the Documentation have been returned to Broadcom or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL BROADCOM BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF BROADCOM IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice

The manufacturer of this Documentation is Broadcom Inc.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.