



VMware Sovereign Cloud Bring Your Own Encryption

Table of Contents

Version History	3
Business requirement	3
Introduction	3
Architecture	4
Provider Admin	4
Tenant Admin	4
Tenant User	4
Bill of Materials	4
Prerequisites	4
Installation	5
Configure Solution Landing Zone	5
Installation with UI	6
Installation with CLI	10
Provider Operations.....	11
Configure KMS servers	11
Publish KMS servers	14
Unpublish KMS servers	15
Tenant Operations	16
Configure KMS servers	16
Configure VDC encryption	20
Rotate VDC encryption keys	21
Disabling VDC encryption	22
Encrypting a vApp or VM	23
Known Behavior	23
Unable to remove KMS without a default key provider	24
Unable to encrypt a powered-on VM that isn't already encrypted	24
Unable to specify an encryption key for a specific vApp or VM	24
New vApps or VMs are not encrypted by default	24
Slow processing with many VMs	25
Failure cloning unencrypted VM to encrypted	25
Troubleshooting	25

Removing the BYOEaaS solution	25
Retrieving BYOEaaS logs	27
Glossary	27

Version History

Date	Description
8/15/2023	Initial version

Business requirement

In today's world, more and more customers insist on managing and bringing their own encryption keys and having operational independence from the cloud service providers. This is especially important and critical when it comes to data sovereignty where regulated and government tenants are looking for providers to build zero trust environments to maintain full ownership and control of their sensitive and confidential data at all times.

VMware Sovereign Cloud global program continues to bring differentiated innovations in the areas of security, compliance, data management and data protection without compromising data sovereignty, residency and operational jurisdiction. In today's world more and more regulated industries and public sector organizations are looking for encryption and security services where they have complete sovereign ownership and autonomy of their data. VMware and VCPP BU, in collaboration with the CSPs and 3rd party best in class ISV ecosystem partners, are happy to announce the tech preview of Bring Your Own Encryption as a Service offering as part of the Cloud Director platform.

This security offering is fully Sovereign compliant and allow Sovereign tenants to bring their own encryption keys (BYOK) and/or their own key management system (BYOKMS) when creating and encrypting virtual machines. Provider can host this Sovereign service within their Sovereign Cloud infrastructure however provider will have no access to keys. Only Customers will have access to their keys. Providers have zero visibility however providers will ensure that encryption keys never leave Sovereign boundaries.

Based on the feedback from several large providers worldwide, team has put in significant effort and is very excited to offer a beta launch of the solution for providers to deploy and test the solution as well as leverage all its core capabilities in their POC environments. This will help the product and engineering teams to gather important feedback early in the process and help VMware prepare the support and enablement teams for a full GA launch later this year. Thank you for your continued collaboration and partnership as we bring new and differentiated Sovereign innovations to the CSP market.

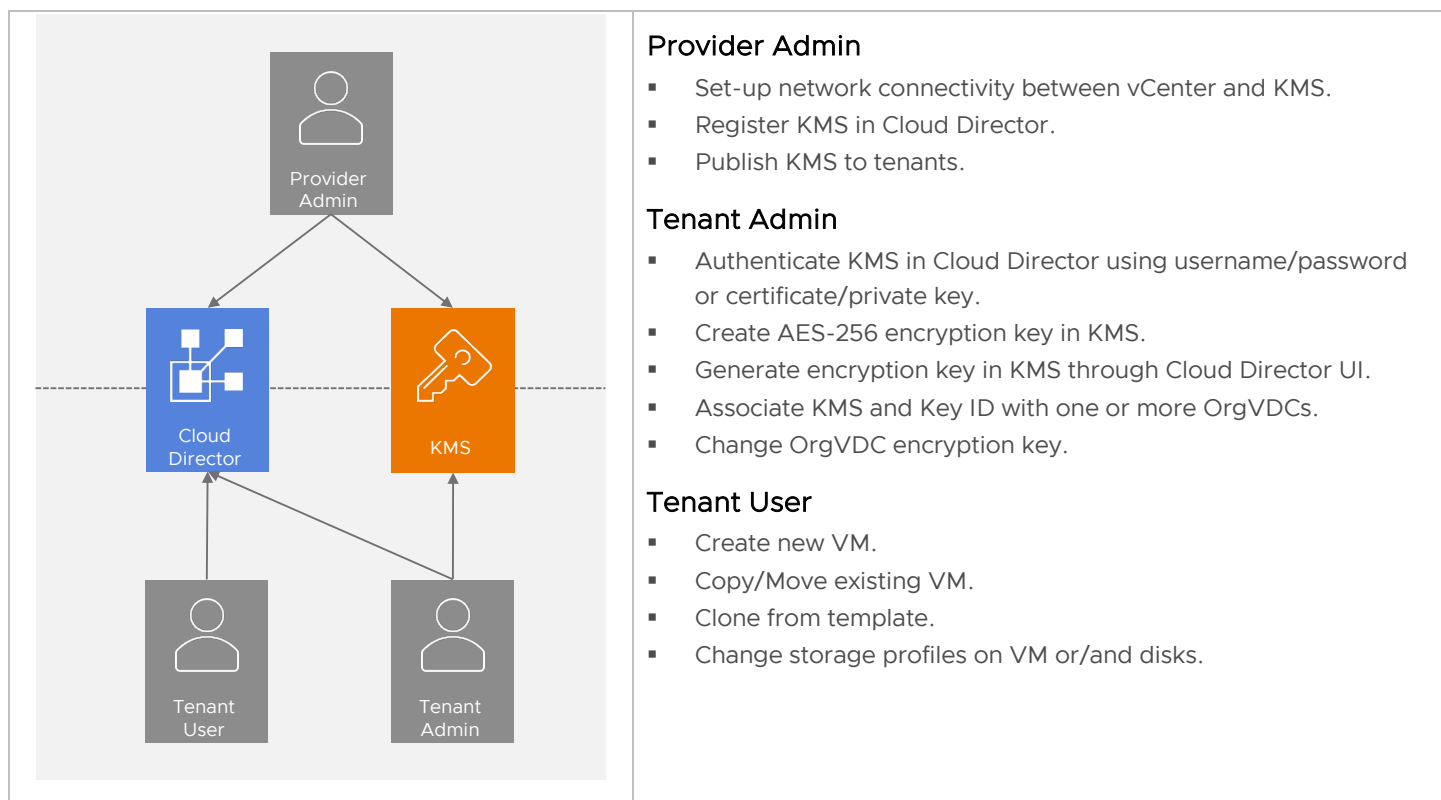
Bring Your Own Encryption as a Service (BYOEaaS) is essential because it enhances data security, ensures compliance with regulations, and builds customer trust. Organizations can customize encryption methods to match their security needs, reducing the risk of data breaches. BYOEaaS helps meet regulatory requirements like GDPR, HIPAA, and PCI DSS. It also supports Data Sovereignty, protecting data even if it moves to different locations. In cloud services, BYOEaaS adds an extra layer of protection, encrypting data in the cloud and limiting access by the cloud provider. Implementing BYOEaaS aligns security practices with specific needs, regulations, and customer expectations, creating a more secure and compliant environment that builds stakeholder trust.

Introduction

The VMware Cloud Director Bring Your Own Encryption as a Service (BYOEaaS) solution empowers tenant administrators with the authority to manage encryption keys for Virtual Machines (VMs) within their respective Virtual Data Centers (VDCs).

Previously, this privilege was exclusive to the provider administrator, who could configure key providers on the vSphere server. However, the updated approach involves the provider setting up connections to individual Key Management Servers (KMS), making the KMS accessible to organizations. Subsequently, the tenant administrator gains access to the KMS, goes through an authentication process, and allocates encryption keys to each of their Virtual Data Centers.

Architecture



Bill of Materials

Software	Release
VMware Cloud Director	10.4.2.1 https://customerconnect.vmware.com/downloads/details?downloadGroup=VSPP_VCD10421&productId=1312
	10.5.0 https://customerconnect.vmware.com/downloads/details?downloadGroup=VSPP_VCD105&productId=1449&rPId=108056
BYOEaaS Solution ISO	vmware-bring-your-own-encryption-0.9.0.iso https://customerconnect.vmware.com/downloads/get-download?downloadGroup=VSPP-SOVCLLOUD-BYOE-TP

Prerequisites

- vSphere

- A default key management server (KMS) must be defined. This KMS will be used if a VM is deployed with an encrypted storage policy and the tenant has not configured a KMS for the Org VDC. The KMS will also be used if you unpublish a BYOEaaS KMS from a tenant.

For vSphere 8.0 U1, a native or standard key provider may be configured as the default. For all other versions, a standard key provider must be configured as the default key provider. See <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-C0AF1F3A-67B4-41A6-A933-7E52A3603D9D.html#limitations-on-cloning-in-vsphere-virtual-machine-encryption-4> for more details about vSphere encryption support.

- VMware Cloud Director
 - Running version 10.4.2.1 or 10.5.0
 - A storage policy with encryption enabled (e.g., VM Encryption Policy) added to the Provider VDC and Organization VDCs
 - An organization to use for the solution landing zone with capacity to run VMs. The smallest appliance size is 2 vCPU & 4 GB memory. Larger sizes are available but are not needed unless you are supporting many VM encryptions.
- KMIP
 - Service credentials based on vendor documentation for vSphere integration.
 - Allow generation of AES-256 keys
 - Allow generated keys to be exported
 - vSphere access to the KMIP port. The default is 5696.

Installation

Configure Solution Landing Zone

This is the basic process to define a Solution Landing Zone in your Cloud Director. Complete documentation is available at <https://docs.vmware.com/en/VMware-Cloud-Director/10.4/VMware-Cloud-Director-Service-Provider-Admin-Portal-Guide/GUID-358B4812-6B45-4293-A179-3736718B9E85.html>.

1. Open the Cloud Director Tenant UI for the Solutions Org
2. Browse to Libraries -> Catalogs
3. Create a Catalog named "Solution Add-Ons" to hold Solution Add-On ISO files. Be sure to configure a storage policy for the catalog files.

×

You can use a catalog for sharing vApp templates and media with other users in your organization. You can also have a private catalog for vApp templates and media that you frequently use.

CANCEL OK

- Follow the prompts to complete the process. You will need to configure the selected organization VDC before continuing the next step. Click the three vertical dots next to the name and select a default entry for network, compute policy and storage policy. These selections are not used by BYOEaaS but they will be used by future solution add-ons. The SLZ does not support networks which are scoped to a data center group. You must decrease the scope of the network or create a new one if this applies to your environment.

10 1 - 1 of undefined organization VDC(s)

Installation with UI


1. Browse to the Cloud Director Provider UI
2. Browse to More -> Solution Add-On Management
3. Click "Upload"

- Upload the Solution Add-On ISO. Leave the “Create add-on instance” checkbox selected.

Upload Add-On

×

Upload File

 vmware-bring-your-own-encryption-0.9.0.iso (295 MB)

×

 REMOVE

☒ Create add-on instance after upload is completed

File Details

Name	Bring Your Own Encryption as a Service
Description	Solution add-on for VMware Cloud Director enabling your tenants to bring their own encryption keys and key providers to their cloud infrastructure.
Vendor	vmware
Version	0.9.0
Minimal Supported Cloud Director Version	10.4.2

Solution Add-On Elements

UI Plug-ins	ui
Defined Entity	rde

CANCEL

UPLOAD

- Click “Upload”

- Wait for the upload process to complete.

Upload Add-On ×

Upload File ✓ File uploaded successfully

☒ Create add-on instance after upload is completed

File Details

Name	Bring Your Own Encryption as a Service
Description	Solution add-on for VMware Cloud Director enabling your tenants to bring their own encryption keys and key providers to their cloud infrastructure.
Vendor	vmware
Version	0.9.0
Minimal Supported Cloud Director Version	10.4.2

Solution Add-On Elements

UI Plug-ins	ui
Defined Entity	rde
Role	back role

FINISH

- Click “Finish”
- Click “I Agree” to accept the VMware license.

9. Fill in the solution parameters and click “Next”.

Create Instance of Bring Your Own Encryption

- 1 Accept Licenses
- 2 Input Parameters
- 3 Review and Complete

Input Parameters

Add-On Instance Name *

The name of the add-on instance is used to uniquely identify this instance in case there are multiple add-on instances.

Deployment Configuraton *

Amount of CPU and memory resources allocated to the system VM.

CANCEL
BACK
NEXT

10. Review the details and click “Finish”.
11. The UI will show the solution install status as “Pending”. You can follow the installation progress by watching the VCD tasks. Wait for the installation to complete and the solution status to be “READY”.

Bring Your Own Encryption

General

Instances

+ NEW INSTANCE

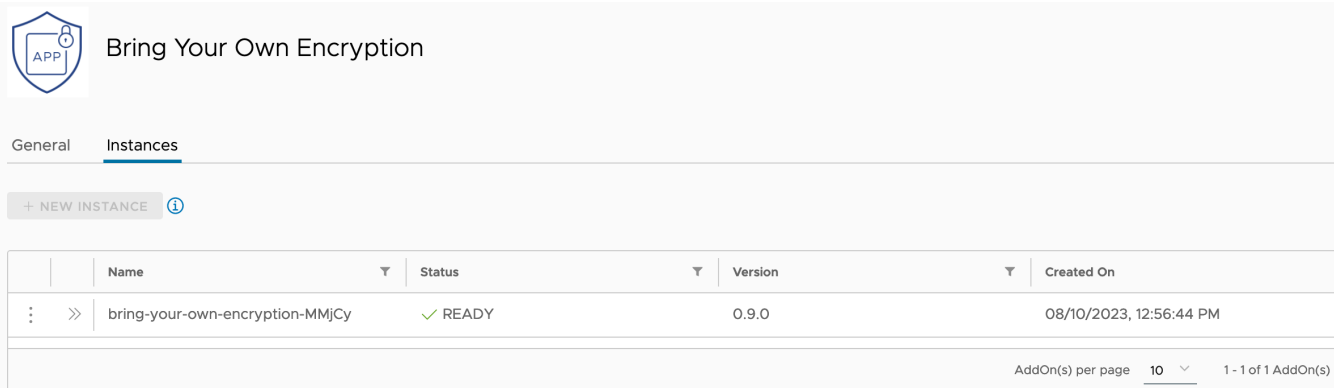
Name	Status	Version	Created On
bring-your-own-encryption-MMjCy	PENDING	0.9.0	08/10/2023, 12:56:44 PM

AddOn(s) per page 1 - 1 of 1 AddOn(s)

Recent Tasks

Task	Status	Type	Initiator	Start Time
Running vmware.solutions-agent-1.0.0-agent-vmware.bring-your-own-encryption-0...	✓ Succeed...	vapp	service-account-solutions-system-us...	08/10/2023, 12:57:17 PM
Created vmware.solutions-agent-1.0.0-agent-vmware.bring-your-own-encryption-0...	✓ Succeed...	vapp	service-account-solutions-system-us...	08/10/2023, 12:56:47 PM
Creating vmware.bring-your-own-enc...(urn:vcloud:entity:vmware:solutions_add_on_...	1% 1%	definedEntity	service-account-solutions-system-us...	08/10/2023, 12:56:44 PM
Creating vmware.solutions-agent-1...(urn:vcloud:entity:vmware:solutions_add_on_in...	1% 1%	definedEntity	service-account-solutions-system-us...	08/10/2023, 12:56:43 PM
Invoking vmware.bring-your-own-encryption-0...(urn:vcloud:entity:vmware:solutions...	1% 1%	definedEntity	administrator	08/10/2023, 12:56:28 PM

12. The solution is now installed and ready to use.



Bring Your Own Encryption

General Instances

+ NEW INSTANCE ⓘ

Name	Status	Version	Created On
bring-your-own-encryption-MMjCy	✓ READY	0.9.0	08/10/2023, 12:56:44 PM

AddOn(s) per page 10 1 - 1 of 1 AddOn(s)

Installation with CLI

1. Mount the solution ISO to a Linux host

```
# mount vmware-bring-your-own-encryption-0.9.0.iso /mnt/cdrom
```

2. Set environment variables with the desired configuration settings. These will be referenced in later commands or consumed by the Solution Add-On installation process. The environment variables prefixed with VCD_EXT_ will be loaded into command-line options with the same name.

```
# cat <<EOF > byoe-env.sh
export VCD_HOSTNAME=vcd.example.com
export VCD_USERNAME=administrator
export VCD_EXT_PASSWORD=password
export BYOE_INSTANCE_NAME=VALUE_REQUIRED
export BYOE_ENCRYPTION_KEY=$(uuidgen | base64)
EOF
```

```
# source byoe-env.sh
```

3. Download the VCD certificate to a file. It will be used to trust the connection in later commands. The linux.run command validates the contents of all files in the solution when it is executed. This can take several minutes the first time it runs but will be shorter during subsequent commands.

```
# sudo -E /mnt/cdrom/linux.run get certificates --host $VCD_HOSTNAME \
--output /tmp/vcd.pem \
--accept
```

4. Configure VCD to trust the BYOEaaS Solution Add-On.

```
# sudo -E /mnt/cdrom/linux.run trust --host $VCD_HOSTNAME \
--username $VCD_USERNAME \
--certificate-file /tmp/vcd.pem \
--accept
```

5. Create the solution add-on instance.

```
# sudo -E /mnt/cdrom/linux.run create instance --name $BYOE_INSTANCE_NAME \  
--host $VCD_HOSTNAME \  
--username $VCD_USERNAME \  
--certificate-file /tmp/vcd.pem \  
--encryption-key ${BYOE_ENCRYPTION_KEY} \  
--accept
```

Provider Operations

Configure KMS servers

1. Open the Cloud Director Provider UI for the Solution Org
2. Browse to More -> Bring Your Own Key to open the BYOEaaS dashboard.
3. An introduction page will be displayed until a key provider has been configured. Click “Get Started” to configure the first key provider.

4. Complete the details for the KMS based on the KMIP service you would like to use. The “Name” value is for display purposes in the Tenant UI.

1. Key Provider Information

Provide address and port for the key provider

Key Provider Information

Name *

Internal Key Provider

Description

Enter key provider description

Icon

BROWSE

Address *

192.168.111.4

Port *

5696

[PROXY SETTINGS >](#)

NEXT

CANCEL

5. Click “Next”

6. Select the vCenter server to associate this KMS server with.

2. vCenter Information
Provider vCenter scope and credentials

Select vCenter

Only IaaS vCenters are eligible for selection

	Name	Status	State	Connection	vCenter Server Host	Version
	vc.0	Normal	Enabled	Connected	https://vxlan-vm-111-107...	8.0.0.10100

vCenter(s) per page
5
1 - 1 of 1 vCenter(s)

The vCenter password is required the first time a KMS server is registered with each vCenter.

vCenter Credentials

Username

administrator@vsphere.local

Password *

.....

REGISTER

CANCEL

7. Click "Register"

8. You may be asked to trust the key provider certificate if it cannot be validated.

Trust certificate | Internal Key Provider
×

Server Certificate

Subject	
Common Name	Server Certificate
Organization Unit	-
Organization	Test, Inc.
Locality	-
State/Province	-
Country Code	-
Email Address	-

Issuer	
Common Name	Root CA
Organization Unit	-
Organization	Test, Inc.
Locality	-
State/Province	-
Country Code	-
Email Address	-

Details	
Fingerprint (SHA-256)	CD:2A:5F:20:04:51:A7:E4:16:09:9F:FF:8E:50:9E:69:EA:EB:A3:57:26:50:A6:49:BC:64:C4:CF:CE:9B:32:00
Serial Number	2C:CA:0B:2A:FA:12:75:97:86:6E:82:0B:AA:4F:53:71:C7:51:61:AE
Signature Algorithm	SHA256 with RSA
Expires On	08/06/2024, 10:10:47 AM
Subject Alternative Names	localhost

CANCEL
TRUST

9. Additional key providers may be added by clicking the “Register” button from the BYOEaaS dashboard.

Publish KMS servers

1. Open the Cloud Director Provider UI
2. Browse to More -> Bring Your Own Key
3. Click on the three dots next to a KMS instance and click “Publish”.

Key Providers

REGISTER

	▼	vCenter	Organizations	Connection Status	▼	Certificate Status	▼
⋮	Edit Trust Certificate Publish Remove	vc.0	0	Connected		Valid until 08/03/2024, 12:39:07 PM	
⋮		vc.0	0	Connected		Valid until 08/01/2024, 10:15:30 AM	

Key Provider(s) per page 5 1 - 2 of 2 key provider(s)

- Select the solutions which should have access to this KMS instance.

Publish | Internal KMS

When you publish, you provide the selected organizations with access to this key provider.

If you want to revoke the access of an organization to the key provider, you can use the actions menu for this specific organization.

☐ Name

☒ Acme Org

☐ Widgets Company

☒ solutions

☒ 2

Organization(s) per page 8 | 1 - 3 of 3 Organization(s)

CANCEL

PUBLISH

- Click "Publish"

Unpublish KMS servers

A KMS server may be unpublished from tenants if vSphere is configured with a default key provider; or if there are no encrypted VMs using the KMS. If vSphere is not configured with a default key provider; the tenant administrator must migrate all encrypted VMs to another KMS by changing the encryption policy for the organization VDC.

- Open the Cloud Director Provider UI
- Browse to More -> Bring Your Own Key
- Click on the name of the KMS you would like to unpublish.

- Click the three dots next to the name of the organization you would like to unpublish the KMS from and click “Unpublish”.

	Organization Name	Status	Organization VDCs	Encrypted Virtual Machines
⋮	Unpublish	⚠ Not Authenticated	0	0
⋮	solutions	✅ Authenticated	1	0
Organization(s) per page 5 1 - 2 of 2 Organization(s)				

- Confirm the action by moving the slider to the right and clicking the checkbox. Click “Unpublish”.

Unpublish | Acme Org

Unpublish Key Provider

Slide to the right to continue

☒ I confirm that I want to unpublish key provider Internal KMS from the above organization

CANCEL

UNPUBLISH

- The unpublish process will complete in the background by transitioning all encrypted VMs to use the default key provider from vSphere and then unpublishing the KMS from the organization.


Tenant Operations




Configure KMS servers

- Browse to the Cloud Director Tenant UI
- Browse to More -> Bring Your Own Key


- Each KMS will indicate if it can authenticate to the KMIP service. Click “Configure” for a KMS to configure the authentication credentials.

Key Providers

 Internal KMS

Encrypted Org VDCs	0
Connection	 Connected
Account	 Not Authenticated
Certificate	 Valid until 08/03/2024, 12:39:07 PM

-

 To get started please configure this key provider

CONFIGURE

- Select the Org VDCs which should use this key to encrypt VMs. Click “Submit” to complete the initial configuration of

this KMS.



Configure Internal KMS Server

Authenticate key provider



Configure Organization VDCs for Encryption

Encrypt Organization VDCs

Add Key

You can configure encryption with other Key IDs later

Key ID *

2

GENERATE KEY

Please note that only AES-256 encryption type is allowed.

Organization VDCs

When you encrypt an organization VCD, all existing encrypted VMs in it are encrypted with the new key. All existing non-encrypted VMs remain non-encrypted. All VMs that you create in this organization VDC in the future and that have an encryption-enabled storage policy or that have a TPM device will be encrypted with this key.


<input checked="" type="checkbox"/>	Name	Encryption State	Key Provider
<input checked="" type="checkbox"/>	solutions:ovdc.0	Not Encrypted	-
<div> <input checked="" type="checkbox"/> 1 </div> <div>Organization VDC(s) per page 8 1 - 1 of 1 organization VDC(s)</div>			




SUBMIT

CANCEL

6. The KMS is now ready to encrypt VMs in the selected VDCs. Any VMs eligible for encryption will automatically be reencrypted with the KMS.

Key Providers

 **Internal KMS**

Encrypted Org VDCs	1
Connection	 Connected
Account	 Authenticated
Certificate	 Valid until 08/03/2024, 12:39:07 PM
-	

ALL ACTIONS ▾

Configure VDC encryption

This process may be used to encrypt VDCs without an associated KMS or to take over encryption for a VDC which already has encryption configured.

1. Browse to the Cloud Director Tenant UI
2. Browse to More -> Bring Your Own Key
3. Click on the name of the KMS being used to encrypt the VDC.
4. Click "Encrypt Org VDCs"
5. Click "Generate Key" to have BYOEaaS generate an AES-256 key on the KMS. You can optionally paste the ID for a pre-generated key, but it is recommended to use the "Generate Key" button. The ID returned by the KMS is displayed, the format of this key may be different for each KMS vendor.

Select the Org VDCs which should use this key to encrypt VMs.

Click “Submit” to complete the initial configuration of this KMS.

Add Key

You can configure encryption with other Key IDs later

Key ID * GENERATE KEY

Please note that only AES-256 encryption type is allowed.

Organization VDCs

When you encrypt an organization VCD, all existing encrypted VMs in it are encrypted with the new key. All existing non-encrypted VMs remain non-encrypted. All VMs that you create in this organization VDC in the future and that have an encryption-enabled storage policy or that have a TPM device will be encrypted with this key.

<input checked="" type="checkbox"/>	Name	Encryption State	Key Provider
<input checked="" type="checkbox"/>	solutions:ovdc.0	Not Encrypted	-

☒ 1 Organization VDC(s) per page 8 | 1 - 1 of 1 organization VDC(s)

SUBMIT CANCEL

- The encryption process will continue in the background by transitioning all encrypted VMs to the newly generated key.

Rotate VDC encryption keys

- Browse to the Cloud Director Tenant UI
- Browse to More -> Bring Your Own Key
- Click on the name of the KMS being used to encrypt the VDC.
- Click the three dots next to the VDC you would like to modify and click “Change Key”.

	Encryption Status	Key ID	Encrypted Virtual Machines	All Virtual Machines
⋮	✓ Encrypted	5	0	1

Change Key
Remove Key From Org VDC
Retry Encrypt Org VDC

Organization VDC(s) per page 5 1 - 1 of 1 organization VDC(s)

- Click “Generate Key” to create a new AES-256 key and click the checkbox. Click “Submit”.

Change key | solutions:ovdc.0

Key ID *

6

GENERATE KEY

Please note that only AES-256 encryption type is allowed.

⚠ Changing the encryption key will result in reencryption of all virtual machines in the organization VDC

☒ I confirm that the I want to change the Encryption Key for org VDC solutions:ovdc.0

SUBMIT

CANCEL

- All encrypted VMs will be reencrypted with the new key in the background.

Disabling VDC encryption

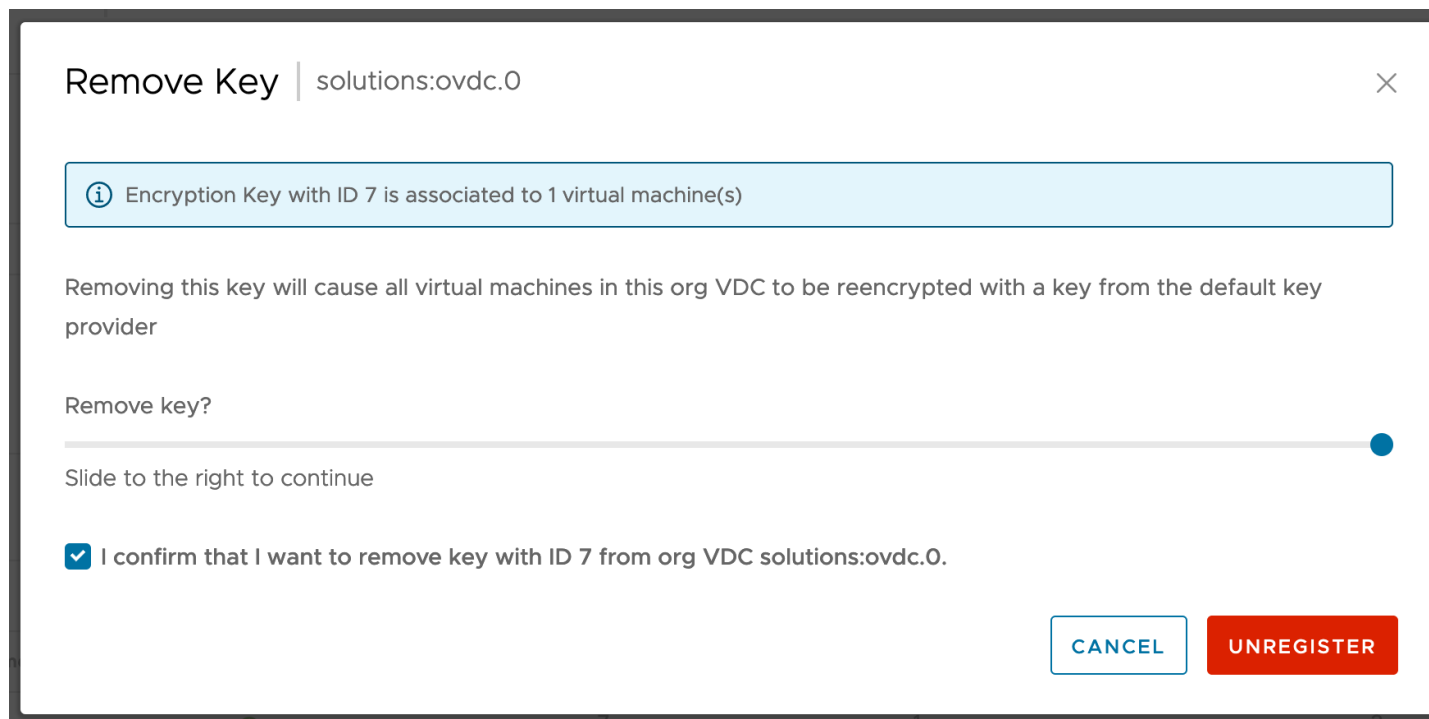
A VDC encryption may be disabled if vSphere is configured with a default key provider; or if there are no encrypted VMs in the VDC. If vSphere is not configured with a default key provider; the tenant administrator will not be able to disable VDC encryption. They may follow the VDC encryption procedure to change which KMS is used to provide encryption keys.

- Browse to the Cloud Director Tenant UI
- Browse to More -> Bring Your Own Key
- Click on the name of the KMS being used to encrypt the VDC.
- Click the three dots next to the VDC you would like to modify and click “Remove Key From Org VDC”.

	Encryption Status	Key ID	Encrypted Virtual Machines	All Virtual Machines
⋮	✓ Encrypted	7	1	2
⋮ solutions:vdc.1	✓ Encrypted	8	0	0

Organization VDC(s) per page 5 1 - 2 of 2 organization VDC(s)

- Confirm the action by moving the slider to the right and clicking the checkbox. Click “Unregister”.



- The unregister process will complete in the background by transitioning all encrypted VMs to use the default key provider from vSphere.

Encrypting a vApp or VM

Encryption is determined based on the storage policy for the VM and attached disks. The provider administrator should publish storage policies which enable encryption to the organization VDCs. The vApp owner must choose this encryption policy when creating or modifying the vApp or VM.

Encryption may not be enabled or disabled for a running VM. Stop the VM before switching it between unencrypted and encrypted storage policies. An encrypted VM may be changed to use a different encryption key while running.

Known Behavior

Unable to remove KMS without a default key provider

Unpublish | solutions
×

This key provider is associated with vCenter instance vc.0 that is not configured with a default key provider. Because of this, unpublishing the key provider from this tenant will cause all encrypted virtual machines with keys from this key provider to stop working. Before proceeding with unpublishing the key provider, configure a default key provider for the vCenter instance vc.0. See [Setting Up the Standard Key Provider](#)

OK

Remove Key | solutions:vdc.1
×

OK

These messages appear when vSphere is not configured with a default key provider and you are trying to remove a KMS server which is being used to provide encryption keys.

Consider defining a default key provider in vSphere or encrypting the affected VDCs with a different KMS.

Unable to encrypt a powered-on VM that isn't already encrypted

vSphere does not support encrypting an existing VM while it is running. To encrypt an existing VM, make sure it is powered off before modifying the storage policy.

Unable to specify an encryption key for a specific vApp or VM

The BYOEaaS solution provides the ability to configure an encryption key for each VDC. It does not support per-vApp or per-VM configuration of the encryption key.

New vApps or VMs are not encrypted by default

VMs will only be encrypted if they are assigned to a storage policy which enables the encryption functionality or has a vTPM device. The Org Administrator may set default storage policy for a VDC to one that enables encryption so that all future VMs are encrypted by default. The VM will be encrypted with the key assigned to the VDC. The default key provider configured in vSphere will be used if one has not been assigned to the VDC.

1. Browse to the Cloud Director Tenant UI
2. Click "Data Centers"

3. Open the VDC you would like to modify
4. Click “Storage Policies”
5. Select a storage policy with encryption enabled

	Name	Status	Default	Used	Limit	Capabilities
<input checked="" type="radio"/>	VM Encryption Policy	✓	–	0 MB	Unlimited	1
<input type="radio"/>	vSAN Default Storage Policy	✓	✓	55.98 GB	Unlimited	5

6. Click “Set As Default”
7. Click “Set” to confirm the change

Slow processing with many VMs

Depending on the number of VMs being managed, the BYOEaaS VM’s default sizing may not be large enough. The resources for BYOEaaS VM may be manually updated through VCD.

1. Browse to the Cloud Director Tenant UI for the Solution Org
2. Click “Applications”
3. Open the “vmware.bring-your-own-key-1.0.0-appliance” vApp
4. Browse to the “Virtual Machines” list for the vApp
5. Open the “byok” VM
6. Click “Actions” -> “Power” -> “Shut Down Guest OS”
7. Click “Shut Down”
8. Open the “Compute” menu for the VM
9. Click “Edit”
10. Modify the resources for the VM
11. Click “Save”
12. Click “Power On”

Failure cloning unencrypted VM to encrypted

Some versions of ESXi will fail when cloning an unencrypted VM to an encrypted storage policy. The error message will resemble “The operation is not supported on the object. The host <ESXI name> does not support clone rekey vTA or NKP vms.” This will only happen on versions below 8.0 U11 when the default key provider is a native vSphere key provider.

Consider upgrading to 8.0 U1 or changing the default key provider to use a standard KMIP server.


Troubleshooting

Removing the BYOEaaS solution

Before removing the BYOEaaS solution, all key providers must be removed.

1. Browse to the Cloud Director Provider UI
2. Browse to More -> Bring Your Own Encryption

3. Remove each key provider by clicking on the three dots and clicking “Remove”.
4. Browse to More -> Solution Add-On Management
5. Click on the three dots next to the solution instance. Click “Remove”. Confirm the action by moving the slider to the right and clicking the checkbox. Click “Remove”.
6. Click on the title of the Bring Your Own Encryption solution.



Bring Your Own Encryption

General
Instances

+ NEW INSTANCE
i

	Name	Status	Version	Created On	
⋮	Remove	bring-your-own-encryption-jOCjM	✓ READY	0.9.0	08/08/2023, 01:45:36 PM

AddOn(s) per page
10
1 - 1 of 1 AddOn(s)

7. Click “Remove” to confirm removal of this solution instance.

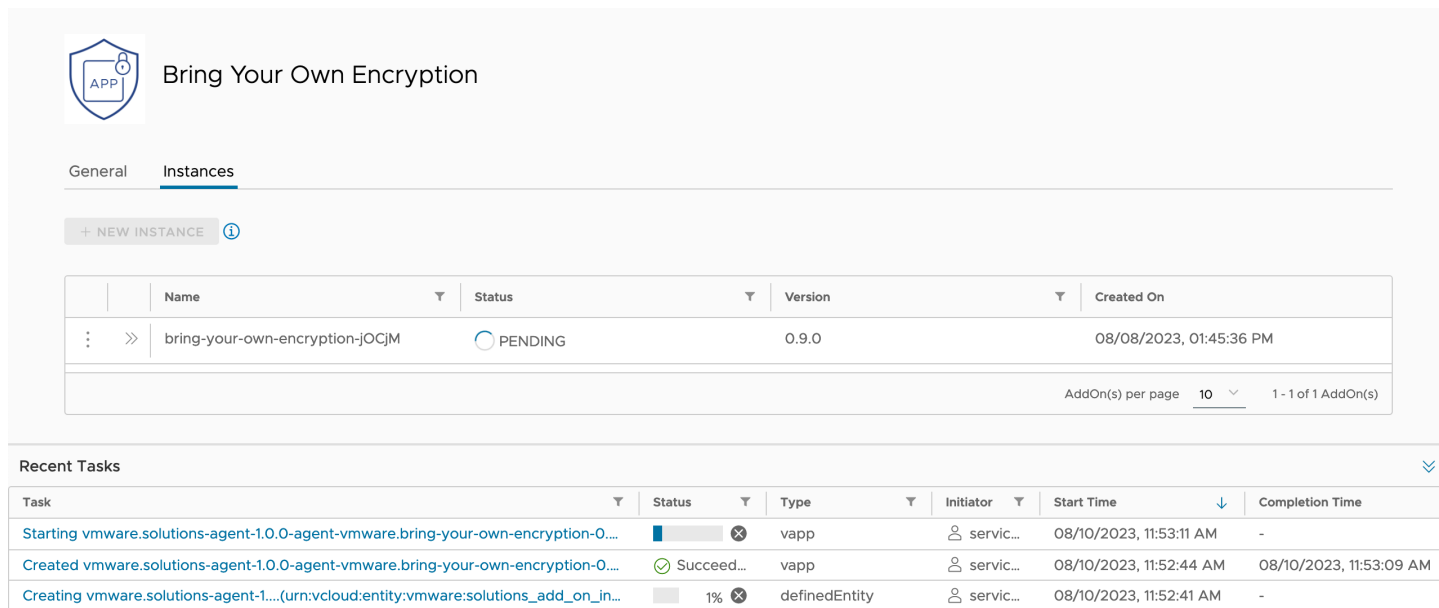
Remove bring-your-own-encryption-jOCjM

×

Remove of the solution add-on cannot be undone. Deleting the solution add-on permanently removes all its resources.

CANCEL
REMOVE

8. The UI will show the solution instance status as “PENDING” or “IN_PROGRESS”. You can follow the removal progress by watching the VCD tasks. The instance will be removed from the UI when complete.



The screenshot shows the VMware Cloud Director interface for the 'Bring Your Own Encryption' solution. The 'Instances' tab is active, displaying a table with one instance: 'bring-your-own-encryption-jOCjM' with a status of 'PENDING' and version '0.9.0'. Below the instances table, the 'Recent Tasks' section shows a list of tasks, including 'Starting vmware.solutions-agent-1.0.0-agent-vmware.bring-your-own-encryption-0...', 'Created vmware.solutions-agent-1.0.0-agent-vmware.bring-your-own-encryption-0...', and 'Creating vmware.solutions-agent-1...'. The tasks show progress bars and completion times.

Retrieving BYOEaaS logs

The root password for the appliance cannot be retrieved. You must reboot the appliance into rescue mode to change the root password to something known. The process is documented at

https://vmware.github.io/photon/assets/files/html/3.0/photon_troubleshoot/resetting-a-lost-root-password.html.

The service logs can be found in the `/opt/vmware/byok/logs` directory. Check the `byok-error.log` and `byok-debug.log` files for any issues.

Glossary

BYOE / BYOEaaS / BYOK

The VMware Sovereign Cloud Bring Your Own Encryption solution

KMIP

Key Management Interoperability Protocol

https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip

Key Management Server (KMS)

A server implementing KMIP. These servers are configured in vSphere through the BYOEaaS provider and tenant UI.

Solution Add-On

A solution add-on is the representation of a solution that is custom built for VMware Cloud Director in the VMware Cloud Director extensibility ecosystem.

See <https://docs.vmware.com/en/VMware-Cloud-Director/10.4/VMware-Cloud-Director-Service-Provider-Admin-Portal-Guide/GUID-4F12C8F7-7CD3-44E8-9711-A5F43F8DCEB5.html> for more details.

Solution Landing Zone (SLZ)

The Solution Add-On Landing Zone is a part of the provider management plane that represents a pool of compute, storage and networking resources dedicated to hosting, managing, and running solution add-ons on behalf of the cloud provider.

Solution Org	The Solution Org is a tenant organization used by the provider to host solution add-ons. It is configured in the solution landing zone as the source of compute, storage and networking resources.
Solution Add-On	<p>A solution add-on is the representation of a solution that is custom built for VMware Cloud Director in the VMware Cloud Director extensibility ecosystem.</p> <p>See https://docs.vmware.com/en/VMware-Cloud-Director/10.4/VMware-Cloud-Director-Service-Provider-Admin-Portal-Guide/GUID-4F12C8F7-7CD3-44E8-9711-A5F43F8DCEB5.html for more details.</p>
Solution Landing Zone (SLZ)	The Solution Add-On Landing Zone is a part of the provider management plane that represents a pool of compute, storage and networking resources dedicated to hosting, managing, and running solution add-ons on behalf of the cloud provider.



Copyright © 2023 VMware, Inc. All rights reserved. VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001

VMware and the VMware logo are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. VMware products are covered by one or more patents listed at [vmware.com/go/patents](https://www.vmware.com/go/patents).
Item No: vmw-wp-tech-temp-uslet-word-2023 1/23