QuickStart Guide

vSphere and vSAN Encryption with Entrust KeyControl

ENTRUST

SECURING A WORLD IN MOTION

Why VM encryption?

To fully unlock all of the advantages of virtualization, it's important to have a security posture in place that is uniquely designed to protect your virtualized environment. Encrypting VMs provides a high level of security you can count on to keep critical data safe.

Reduce Risk

In a virtualized environment – with the appropriate access to the hypervisor – it becomes quite easy to copy its full contents or send it through the wire. By using encryption technology, this still may be possible, but the resulting image file is unreadable without the encryption keys.

Guarantee Availability

Adequately protecting your virtual machines by encrypting them results in a more robust solution, especially if the key management solution is designed with a high-availability (HA) architecture.

Accelerate Savings

Cost savings are one of the main reasons to explore virtualization options, but poorly organized VM encryption can quickly cause any IT savings to disappear. Implementing VM encryption at the hypervisor eliminates the need for additional, specialized hardware to perform encryption – which shrinks encryption overhead costs.

Simplify Compliance

Implementing some form of VM encryption is a requirement to comply with many standards and regulations, including Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act (SOX), Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs), and Health Insurance Portability and Accountability Act (HIPAA). Virtualized environments face new vulnerabilities that can be effortlessly addressed with workload encryption.

Things to watch out for

Before implementing virtual machine encryption, there are several things to keep in mind. The following checklist can help you get started:

- ✓ **Are you ready to use the specific software version required for encryption?** To use the native encryption feature from VMware, it is necessary to upgrade to the latest version of vSphere (6.5 and later). You may not be able to turn on encryption for your customer if they are not ready to take this step for any reason, may it be compatibility or downtime.*

- ✓ **Is your workload uptime (24/7) critical?** Encrypting VMs requires some time to get the job done. It may be necessary to shut down the VMs before proceeding with the encryption, meaning the VM will be unavailable until the encryption process is complete. The processing time will vary, depending on the size of the files and the processing power available.*

- ✓ **Are you using platforms or cloud deployments from multiple vendors?** If you are using a variety of cloud solutions, it may be necessary to utilize several encryption methods, in which case you will end up with several systems to maintain and manage their encryption keys. If you have a VMware-only environment, vSphere 6.5 can be a good option.*

- ✓ **Are you using a VM-based backup technology?** Because of the way most VM backup systems work, backups are fetched from the open VM and the backup data is stored in its unencrypted form. An additional encryption tool may be required for the backups.*

- ✓ **Be sure to select your key management service (KMS)/encryption solution wisely.** Over time, it may be necessary to rekey or even revoke keys, like in the case of changing hosting providers or if there is a suspected data breach. Depending on the key management solution chosen, the simplicity of doing so may vary. In some cases, it may be necessary to completely decrypt and re-encrypt the VM with a new key, with subsequent downtime.*

- ✓ **Always use an active-active, high-availability KMS cluster.** If the encryption keys are not available at any point, data can become inaccessible. Key management has the potential to become a single point of failure. It is highly recommended that the key management cluster is implemented as an active-active, high-availability cluster with a disaster recovery site.

- ✓ **Be aware of recursive encryption, especially on the high-availability KMS cluster.** Locking your keys in the car is never a pleasant experience. So, it is strongly recommended to never store the KMS servers on a datastore or volume that is encrypted with the same keys managed by the KMS. The Entrust KeyControl appliance is already hardened and natively encrypted.

- ✓ **Test before you go live.** It is a good idea to clone an existing VM and go through the complete process. Since the time it takes to complete the encryption depends on the size of the files, testing the process on an actual VM will provide more accurate estimates.

* NOTE: For a list of encryption features between vSphere, vSAN, and Entrust DataControl encryption, please check the comparison table at the end of this Quick Start Guide.

Entrust KeyControl

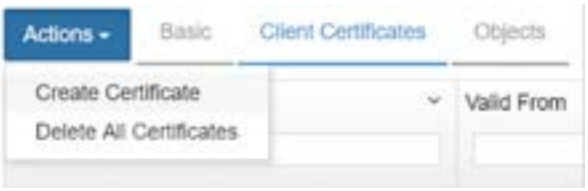
Entrust KeyControl includes a fully functional KMIP (Key Management Interoperability Protocol) server that can serve as a vSphere KMS.

Once a trusted connection between KeyControl and vSphere is established, KeyControl manages the encryption keys for virtual machines in the cluster that have been encrypted with vCenter Server for vSphere Virtual Machine Encryption or VMware vSAN Encryption. The procedure is nearly identical no matter which VMware encryption method you use.

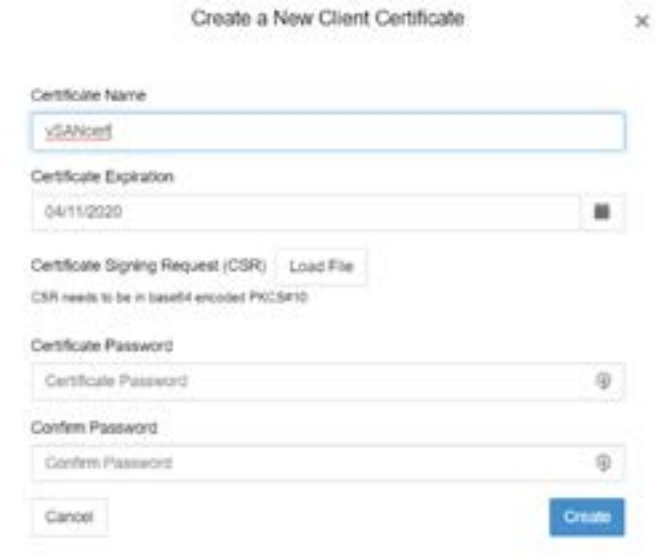
Enabling the KMIP Service

1. Log in to the KeyControl WebGUI using an account with Security Admin privileges
2. In the top menu bar, click KMIP and click the Basic tab
3. Click the State dropdown box and change it to Enable
4. Make sure the Protocol is set to version 1.1
5. Click Apply and confirm the changes when prompted

Create a KeyControl-Signed Certificate for KMS Trust Establishment

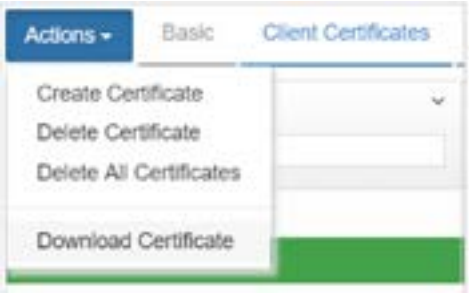


1. In the top menu bar, click KMIP and click the Client Certificates tab
2. Select Actions > Create Certificate
3. In the Create a New Client Certificate dialog box:
    a. Enter a name in the Certificate Name field
    b. Set the date on which you want the certificate to expire in the Certificate Expiration field. If the certificate expires, communication between vCenter and KeyControl will be disrupted until a new certificate is uploaded
    c. Important: Do not enter a password for the certificate. Due to a vCenter limitation, you cannot upload encrypted certificates
    d. Click Create



4. On the Client Certificates tab, select the certificate bundle you just created

5. Select Actions > Download Certificate. The WebGUI downloads <certname_ datetimestamp>.zip, which contains a user certification/key file called <certname>.pem and a server certification file called cacert.pem



6. Unzip the file so that you have the <certname>.pem file available to upload into vCenter. In the example above, the certificate file would be named vSANcert.pem

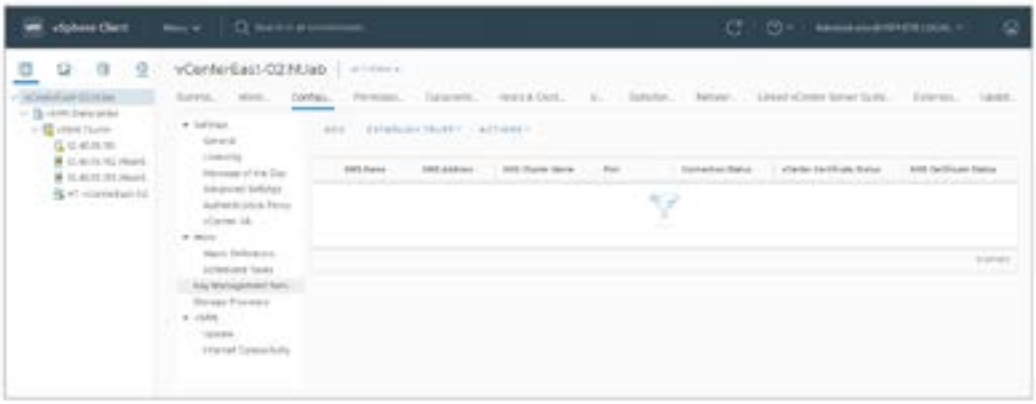
Add the KMS Cluster to vCenter

1. Log in to the vCenter server to which you want to add the Entrust KeyControl KMS cluster

2. Select the vCenter server in the Global Inventory Lists

3. Click the Configure tab for the server

4. Click More and select Key Management Servers



5. Click Add and set the following configuration options:

Option	Description
KMS cluster	Select <Create new cluster>
New cluster name	Enter a name for the cluster. This name is local to vCenter and is not used by KeyControl.
Server address	The IP address for the Entrust KMIP server. This IP address must match the KeyControl KMIP server Host Name shown in the KeyControl WebGUI. Important: Make sure that the KMIP server resides on a device that is not encrypted. The KMIP server must be available to provide the keys for the encrypted devices before the encrypted devices can be accessed.
Server port	The port number for the Entrust KMIP server. The KMIP standard port is 5696.
Proxy address and Proxy port	Enter this information if required by your network administrator.
Username and Password	**Important: Do not enter a username or password for the KMS cluster.**

6. Click OK

7. If prompted, click Yes to make this the default KMS cluster (see screen shot at left)

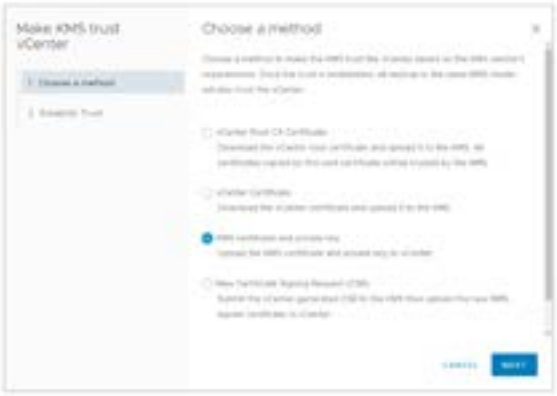
8. In the Trust Certificate dialog box, click Trust

This adds the KMS cluster to vCenter, but the connection status will state "Not Connected (Trust not established. View Details)." To fix this, the certificate that was created earlier must be uploaded.

Establish a KMS Trust Connection

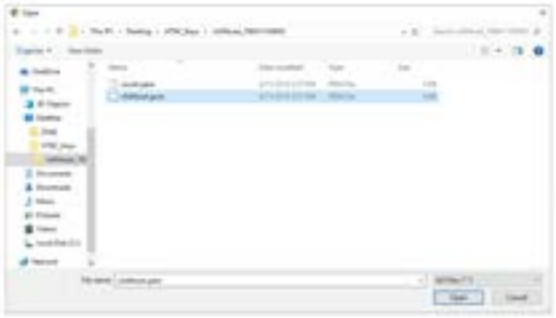
1. Click the View Details link for the KMS cluster node you previously added
2. Click the Make KMS Trust vCenter button

3. In the Make KMS trust vCenter dialog box, select KMS certificate and private key, then click Next



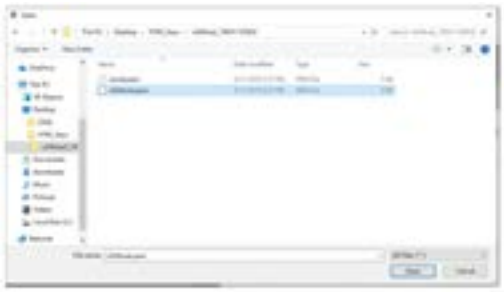
4. Click the KMS Certificate: Upload a File button

5. Select the <certname>.pem file that was previously created in the Create a KeyControl-Signed Certificate for KMS Trust Establishment section. Click Open



6. Click the KMS Private Key: Upload a File button

7. Select the <certname>.pem file that was previously created in the Create a KeyControl-Signed Certificate for KMS Trust Establishment section. Click Open



8. After uploading the KMS Certificate and KMS Private Key, click Establish Trust

9. Once the certificates are uploaded, the connection status of the KMS should change to connected and the KMS Trust Connection is established. Repeat this process again until all other KMS nodes of your HA cluster have been added

If you are required to use a vCenter Server certificate when establishing a KMS trust connection, please refer to the Entrust KeyControl online documentation section titled, Establishing a Trusted Connection with a vSphere-Generated CSR.

Enabling Encryption on a vSAN Cluster

1. Navigate to the VSAN-enabled cluster
2. Click the Configure tab
3. Under vSAN, select Services
4. Click the Encryption Edit button
5. On the vSAN Services dialog, enable Encryption, and select a KMS Cluster. Click Next

Optionally, you can also choose to wipe existing data from the disks as they are being encrypted. Just be aware that this can increase the time before a disk can receive data. This option removes any previous data stored on the disks.

Enabling vSphere Encryption on a VM

In order to use vSphere native encryption, you must be running vCenter/ESXi version 6.5.x or later. If you are running an earlier version of vCenter/ESXi, then you will not be able to follow this procedure. However, you can use Entrust DataControl to enable encryption inside a VM no matter where the VM is running.

There is already a default VM storage policy (VM Encryption Policy) for enabling encryption on a VM. Therefore, this is the procedure to follow to enable encryption on a VM. If you are interested in creating a custom VM storage encryption policy, refer to the VMware online documentation.

1. Right-click the VM you want to encrypt and select VM Policies, Edit VM Storage Policies

2. Select VM Encryption Policy in the VM storage policy drop-down menu and click OK

3. Optionally, if you prefer to only encrypt a specific disk attached to your VM, then toggle the Configure per disk option and select VM Encryption Policy for VM home and/or each disk you want to encrypt. Click OK

4. If the VM is powered on you will receive the following error. Power off the VM then attempt the operation again

NOTE: Using Entrust DataControl you can encrypt a VM or a specific disk while the VM is powered on. Reach out to your Entrust Account team to learn more.

5. Once the encryption process has completed, you will see the following icon in the Summary tab for the VM

Summary

This quick start guide describes the procedure on how to install and configure Entrust KeyControl for enabling encryption key management in a vSphere version 6.5 or later virtual environment. The procedure for enabling vSAN and vSphere VM-based encryption is also described.

Troubleshooting

If vSphere Virtual Machine encryption or VMware vSAN encryption fails with the error “Cannot generate key”, check the following:

- The Entrust KeyControl appliance must be powered on and operational. To verify this, log in to the appliance using the KeyControl WebGUI.
- The Entrust KMIP server must be enabled as described in Configuring a KMIP Server.
- The KeyControl nodes must be able to communicate with one another. Make sure the server status is not shown as Degraded in the KeyControl WebGUI.
- The KMIP client certificate and private key must be valid and current. You can verify the certificate status in the KeyControl WebGUI on the KMIP Servers Certificates tab or in the vCenter Web Client on the KMS tab. For details about creating a new certificate and key, see Creating a Certificate Bundle for VMware Encryption.
- If the vCenter Web Client reports that the KMIP connection status is Normal (green) but encryption fails, the KMS cluster could have been added with a username and password. To verify this:

    1. Check the Entrust DataControl Audit log for the message “KMIP response rate Operation Failed DENIED”.
    2. If you find that message, edit the properties of the Entrust KMS cluster in the vCenter Web Client and remove any username or password.

- If the KeyControl cluster is functioning properly and the certificates are valid but the vCenter Web Client reports that the Entrust KMS is not connected, you may need to remove the KMS instance and re-add it to vCenter in order to restore the Trusted connection. Select the Entrust KMS in vSphere Web Client and select All Actions > Remove KMS. Then add the KMS back as described in Creating the KMS Cluster in vSphere section.
- If everything shows as connected but encryption still fails, use the vCenter Web Client to verify that encryption is enabled for the ESXi host using ESXi-server-name > Configure > Security Profile > Host Encryption Mode.

	vSphere Encryption	vSphere Encryption	Entrust DataControl
Encryption Boundary	Hypervisor	Storage Driver	VM
Platforms Supported	vSphere	vSAN	vSphere/vSAN/Any Hypervisor Cloud
Granular VM Encryption	✓	X* *Per vSan Cluster	✓
Dedupe/Compression	X	✓	✓* *Partial Only
No Downtime	X	✓* *Can take considerable time to finish	✓
Public Cloud Support	X	X	✓
Encryption Travels with VM	✓* *Can take considerable time to finish	X	✓
Workload Boot/ Clone Protection	X	X	✓
Encrypted Backups	X	X	✓

For more information

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust is dedicated to securing a world in motion by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223