



# **Configure external key management**

## **ONTAP 9**

NetApp  
June 04, 2024

# Table of Contents

- Configure external key management . . . . . 1
  - Configure external key management overview . . . . . 1
  - Manage external key managers with System Manager . . . . . 1
  - Install SSL certificates on the cluster . . . . . 3
  - Enable external key management in ONTAP 9.6 and later (NVE) . . . . . 4
  - Enable external key management in ONTAP 9.5 and earlier . . . . . 7
  - Manage keys with a cloud provider . . . . . 9

# Configure external key management

## Configure external key management overview

You can use one or more external key management servers to secure the keys that the cluster uses to access encrypted data. An external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP).



For ONTAP 9.1 and earlier versions, node management LIFs must be assigned to ports that are configured with the node management role before you can use the external key manager.

NetApp Volume Encryption (NVE) supports Onboard Key Manager in ONTAP 9.1 and later. Beginning in ONTAP 9.3, NVE supports external key management (KMIP) and Onboard Key Manager. Beginning in ONTAP 9.10.1, you can use [Azure Key Vault or Google Cloud Key Manager Service](#) to protect your NVE keys. Beginning in ONTAP 9.11.1, you can configure multiple external key managers in a cluster. See [Configure clustered key servers](#).

## Manage external key managers with System Manager

Beginning with ONTAP 9.7, you can store and manage authentication and encryption keys with the Onboard Key Manager. Beginning with ONTAP 9.13.1, you can also use external key managers to store and manage these keys.

The Onboard Key Manager stores and manages keys in a secure database that is internal to the cluster. Its scope is the cluster. An external key manager stores and manages keys outside the cluster. Its scope can be the cluster or the storage VM. One or more external key managers can be used. The following conditions apply:

- If the Onboard Key Manager is enabled, an external key manager cannot be enabled at the cluster level, but it can be enabled at the storage VM level.
- If an external key manager is enabled at the cluster level, the Onboard Key Manager cannot be enabled.

When using external key managers, you can register up to four primary key servers per storage VM and cluster. Each primary key server can be clustered with up to three secondary key servers.

## Configure an external key manager



To add an external key manager for a storage VM, you should add an optional gateway when you configure the network interface for the storage VM. If the storage VM was created without the network route, you will have to create the route explicitly for the external key manager. See [Create a LIF \(network interface\)](#).



### Steps

You can configure an external key manager starting from different locations in System Manager.

1. To configure an external key manager, perform one of the following starting steps.

| Workflow | Navigation | Starting step |
|----------|------------|---------------|
|----------|------------|---------------|

|   |                                 |  |
|---|---------------------------------|--|
| Configure Key Manager                                       | <b>Cluster &gt; Settings</b>    | Scroll to the <b>Security</b> section. Under <b>Encryption</b> , select  . Select <b>External Key Manager</b> .             |
| Add local tier  | <b>Storage &gt; Tiers</b>       | Select <b>+ Add Local Tier</b> . Check the check box labeled "Configure Key Manager". Select <b>External Key Manager</b> .   |
| Prepare storage   | <b>Dashboard</b>                | In the <b>Capacity</b> section, select <b>Prepare Storage</b> . Then, select "Configure Key Manager". Select <b>External Key Manager</b> .   |
| Configure encryption (key manager at storage VM scope only) | <b>Storage &gt; Storage VMs</b> | Select the storage VM. Select the <b>Settings</b> tab. In the <b>Encryption</b> section under <b>Security</b> , select  . |



- To add a primary key server, select **+ Add**, and complete the **IP Address or Host Name** and **Port** fields.
- Existing installed certificates are listed in the **KMIP Server CA Certificates** and **KMIP Client Certificate** fields. You can perform any of the following actions:
  - Select  to select installed certificates that you want to map to the key manager. (Multiple service CA certificates can be selected, but only one client certificate can be selected.)
  - Select **Add New Certificate** to add a certificate that has not already been installed and map it to the external key manager.
  - Select  next to the certificate name to delete installed certificates that you do not want to map to the external key manager.
- To add a secondary key server, select **Add** in the **Secondary Key Servers** column, and provide its details.
- Select **Save** to complete the configuration.


## Edit an existing external key manager

If you have already configured an external key manager, you can modify its settings.

### Steps

- To edit the configuration of an external key manager, perform one of the following starting steps.

| Scope                                 | Navigation                      | Starting step   |
|---------------------------------------|---------------------------------|---|
| Cluster scope external key manager    | <b>Cluster &gt; Settings</b>    | Scroll to the <b>Security</b> section. Under <b>Encryption</b> , select  , then select <b>Edit External Key Manager</b> .  |
| Storage VM scope external key manager | <b>Storage &gt; Storage VMs</b> | Select the storage VM. Select the <b>Settings</b> tab. In the <b>Encryption</b> section under <b>Security</b> , select  , then select <b>Edit External Key Manager</b> . |

- Existing key servers are listed in the **Key Servers** table. You can perform the following operations:
  - Add a new key server by selecting **+ Add**.
  - Delete a key server by selecting  at the end of the table cell that contains the name of the key server.



The secondary key servers associated with that primary key server are also removed from the configuration.

## Delete an external key manager

An external key manager can be deleted if the volumes are unencrypted.

### Steps

1. To delete an external key manager, perform one of the following steps.

| Scope                                 | Navigation                      | Starting step   |
|---------------------------------------|---------------------------------|---|
| Cluster scope external key manager    | <b>Cluster &gt; Settings</b>    | Scroll to the <b>Security</b> section. Under <b>Encryption</b> , select select  , then select <b>Delete External Key Manager</b> .   |
| Storage VM scope external key manager | <b>Storage &gt; Storage VMs</b> | Select the storage VM. Select the <b>Settings</b> tab. In the <b>Encryption</b> section under <b>Security</b> , select  , then select <b>Delete External Key Manager</b> . |

## Migrate keys among key managers

When multiple key managers are enabled on a cluster, keys must be migrated from one key manager to another. This process is completed automatically with System Manager.

- If the Onboard Key Manager or an external key manager is enabled at a cluster level, and some volumes are encrypted, then when you configure an external key manager at the storage VM level, the keys must be migrated from the Onboard Key Manager or external key manager at the cluster level to the external key manager at the storage VM level. This process is completed automatically by System Manager.
- If volumes were created without encryption on a storage VM, then keys do not need to be migrated.

## Install SSL certificates on the cluster

The cluster and KMIP server use KMIP SSL certificates to verify each other's identity and establish an SSL connection. Before configuring the SSL connection with the KMIP server, you must install the KMIP client SSL certificates for the cluster, and the SSL public certificate for the root certificate authority (CA) of the KMIP server.

### About this task

In an HA pair, both nodes must use the same public and private KMIP SSL certificates. If you connect multiple HA pairs to the same KMIP server, all nodes in the HA pairs must use the same public and private KMIP SSL certificates.

### Before you begin

- The time must be synchronized on the server creating the certificates, the KMIP server, and the cluster.
- You must have obtained the public SSL KMIP client certificate for the cluster.
- You must have obtained the private key associated with the SSL KMIP client certificate for the cluster.
- The SSL KMIP client certificate must not be password-protected.

- You must have obtained the SSL public certificate for the root certificate authority (CA) of the KMIP server.
- In a MetroCluster environment, you must install the same KMIP SSL certificates on both clusters.



You can install the client and server certificates on the KMIP server before or after installing the certificates on the cluster.

### Steps

1. Install the SSL KMIP client certificates for the cluster:

```
security certificate install -vserver admin_svm_name -type client
```

You are prompted to enter the SSL KMIP public and private certificates.

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. Install the SSL public certificate for the root certificate authority (CA) of the KMIP server:

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

## Enable external key management in ONTAP 9.6 and later (NVE)

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. Beginning with ONTAP 9.6, you have the option to configure a separate external key manager to secure the keys that a data SVM uses to access encrypted data.

Beginning with ONTAP 9.11.1, you can add up to 3 secondary key servers per primary key server to create a clustered key server. For more information, see [Configure clustered external key servers](#).

### About this task

You can connect up to four KMIP servers to a cluster or SVM. A minimum of two servers is recommended for redundancy and disaster recovery.

The scope of external key management determines whether key management servers secure all the SVMs in the cluster or selected SVMs only:

- You can use a *cluster scope* to configure external key management for all the SVMs in the cluster. The cluster administrator has access to every key stored on the servers.
- Beginning with ONTAP 9.6, you can use an *SVM scope* to configure external key management for a data SVM in the cluster. That's best for multitenant environments in which each tenant uses a different SVM (or set of SVMs) to serve data. Only the SVM administrator for a given tenant has access to the keys for that tenant.
- For multitenant environments, install a license for *MT\_EK\_MGMT* by using the following command:

```
system license add -license-code <MT_EK_MGMT license code>
```

For complete command syntax, see the man page for the command.

You can use both scopes in the same cluster. If key management servers have been configured for an SVM, ONTAP uses only those servers to secure keys. Otherwise, ONTAP secures keys with the key management servers configured for the cluster.

You can configure onboard key management at the cluster scope and external key management at the SVM scope. You can use the `security key-manager key migrate` command to migrate keys from onboard key management at the cluster scope to external key managers at the SVM scope.

### Before you begin

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster or SVM administrator to perform this task.
- If you want to enable external key management for a MetroCluster environment, MetroCluster must be fully configured before enabling external key management.
- In a MetroCluster environment, you must install the KMIP SSL certificate on both clusters.

### Steps

1. Configure key manager connectivity for the cluster:

```
security key-manager external enable -vserver admin_SVM -key-servers  
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert  
server_CA_certificates
```



- The `security key-manager external enable` command replaces the `security key-manager setup` command. If you run the command at the cluster login prompt, `admin_SVM` defaults to the admin SVM of the current cluster. You must be the cluster administrator to configure cluster scope. You can run the `security key-manager external modify` command to change the external key management configuration.
- In a MetroCluster environment, if you are configuring external key management for the admin SVM, you must repeat the `security key-manager external enable` command on the partner cluster.

The following command enables external key management for `cluster1` with three external key servers. The first key server is specified using its hostname and port, the second is specified using an IP address and the default port, and the third is specified using an IPv6 address and port:

```
cluster1::> security key-manager external enable -vserver cluster1 -key  
-servers  
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234  
-client-cert AdminVserverClientCert -server-ca-certs  
AdminVserverServerCaCert
```

2. Configure a key manager an SVM:

```
security key-manager external enable -vserver SVM -key-servers  
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert  
server_CA_certificates
```



- If you run the command at the SVM login prompt, SVM defaults to the current SVM. You must be a cluster or SVM administrator to configure SVM scope. You can run the `security key-manager external modify` command to change the external key management configuration.
- In a MetroCluster environment, if you are configuring external key management for a data SVM, you do not have to repeat the `security key-manager external enable` command on the partner cluster.

The following command enables external key management for `svm1` with a single key server listening on the default port 5696:

```
svm11::> security key-manager external enable -vserver svm1 -key-servers  
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs  
SVM1ServerCaCert
```

3. Repeat the last step for any additional SVMs.



You can also use the `security key-manager external add-servers` command to configure additional SVMs. The `security key-manager external add-servers` command replaces the `security key-manager add` command. For complete command syntax, see the man page.

4. Verify that all configured KMIP servers are connected:

```
security key-manager external show-status -node node_name
```



The `security key-manager external show-status` command replaces the `security key-manager show -status` command. For complete command syntax, see the man page.



```
cluster1::> security key-manager external show-status
```

| Node  | Vserver  | Key Server                                   | Status    |
|-------|----------|--|-----------|
| ----- |          |  |           |
| node1 |          |  |           |
|       | svm1     | keyserver.svm1.com:5696                      | available |
|       | cluster1 | 10.0.0.10:5696                               | available |
|       |          | fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 | available |
|       |          | ks1.local:15696                              | available |
| node2 |          |  |           |
|       | svm1     | keyserver.svm1.com:5696                      | available |
|       | cluster1 | 10.0.0.10:5696                               | available |
|       |          | fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 | available |
|       |          | ks1.local:15696                              | available |

8 entries were displayed.

5. Optionally, convert plain text volumes to encrypted volumes.

```
volume encryption conversion start
```

An external key manager must be fully configured before you convert the volumes. In a MetroCluster environment, an external key manager must be configured on both sites.

## Enable external key management in ONTAP 9.5 and earlier

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. You can connect up to four KMIP servers to a node. A minimum of two servers is recommended for redundancy and disaster recovery.

### About this task

ONTAP configures KMIP server connectivity for all nodes in the cluster.

### Before you begin

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.
- In a MetroCluster environment, you must install the KMIP SSL certificate on both clusters.

### Steps

1. Configure key manager connectivity for cluster nodes:

```
security key-manager setup
```

The key manager setup starts.



In a MetroCluster environment, you must run this command on both clusters.

2. Enter the appropriate response at each prompt.

3. Add a KMIP server:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.1
```



In a MetroCluster environment, you must run this command on both clusters.

4. Add an additional KMIP server for redundancy:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.2
```



In a MetroCluster environment, you must run this command on both clusters.

5. Verify that all configured KMIP servers are connected:

```
security key-manager show -status
```

For complete command syntax, see the man page.

```
cluster1::> security key-manager show -status
```

| Node        | Port | Registered Key Manager | Status    |
|-------------|------|------------------------|-----------|
| -----       | ---- | -----                  | -----     |
| cluster1-01 | 5696 | 20.1.1.1               | available |
| cluster1-01 | 5696 | 20.1.1.2               | available |
| cluster1-02 | 5696 | 20.1.1.1               | available |
| cluster1-02 | 5696 | 20.1.1.2               | available |

6. Optionally, convert plain text volumes to encrypted volumes.

```
volume encryption conversion start
```

An external key manager must be fully configured before you convert the volumes. In a MetroCluster environment, an external key manager must be configured on both sites.

# Manage keys with a cloud provider

Beginning in ONTAP 9.10.1, you can use [Azure Key Vault \(AKV\)](#) and [Google Cloud Platform's Key Management Service \(Cloud KMS\)](#) to protect your ONTAP encryption keys in a cloud-hosted application. Beginning with ONTAP 9.12.0, you can also protect NVE keys with [AWS' KMS](#).

AWS KMS, AKV and Cloud KMS can be used to protect [NetApp Volume Encryption \(NVE\) keys](#) only for data SVMs.

## About this task

Key management with a cloud provider can be enabled with the CLI or the ONTAP REST API.

When using a cloud provider to protect your keys, be aware that by default a data SVM LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with the cloud provider's authentication services ([login.microsoftonline.com](#) for Azure; [oauth2.googleapis.com](#) for Cloud KMS). If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

When utilizing a cloud provider key management service, you should be aware of the following limitations:

- Cloud-provider key management is not available for NetApp Storage Encryption (NSE) and NetApp Aggregate Encryption (NAE). [External KMIPs](#) can be used instead.
- Cloud-provider key management is not available for MetroCluster configurations.
- Cloud-provider key management can only be configured on a data SVM.

## Before you begin

- You must have configured the KMS on the appropriate cloud provider.
- The ONTAP cluster's nodes must support NVE.
- [You must have installed the Volume Encryption \(VE\) and multi-tenant Encryption Key Management \(MTEKM\) licenses](#). These licenses are included with [ONTAP One](#).
- You must be a cluster or SVM administrator.
- The data SVM must not include any encrypted volumes or employ a key manager. If the data SVM includes encrypted volumes, you must migrate them before configuring the KMS.

## Enable external key management

Enabling external key management depends on the specific key manager you use. Choose the tab of the appropriate key manager and environment.

## AWS

### Before you begin

- You must create a grant for the AWS KMS key that will be used by the IAM role managing encryption. The IAM role must include a policy that allows the following operations:

- DescribeKey
- Encrypt
- Decrypt
- +

For more information, see AWS documentation for [grants](#).

### Enable AWS KMS on an ONTAP SVM

1. Before you begin, obtain both the access key ID and secret key from your AWS KMS.
2. Set the privilege level to advanced:  
`set -priv advanced`
3. Enable AWS KMS:  
`security key-manager external aws enable -vserver svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. When prompted, enter the secret key.
5. Confirm the AWS KMS was configured correctly:  
`security key-manager external aws show -vserver svm_name`

## Azure

### Enable Azure Key Vault on an ONTAP SVM

1. Before you begin, you need to obtain the appropriate authentication credentials from your Azure account, either a client secret or certificate.  
You must also ensure all nodes in the cluster are healthy. You can check this with the command `cluster show`.
2. Set privileged level to advanced  
`set -priv advanced`
3. Enable AKV on the SVM  
`security key-manager external azure enable -client-id client_id -tenant-id tenant_id -name -key-id key_id -authentication-method {certificate|client-secret}`  
When prompted, enter either the client certificate or client secret from your Azure account.
4. Verify AKV is enabled correctly:  
`security key-manager external azure show vserver svm_name`  
If the service reachability is not OK, establish the connectivity to the AKV key management service via the data SVM LIF.

## Google Cloud

### Enable Cloud KMS on an ONTAP SVM

1. Before you begin, obtain the private key for the Google Cloud KMS account key file in a JSON format. This can be found in your GCP account.  
You must also ensure all nodes in the cluster are healthy. You can check this with the command `cluster show`.

2. Set privileged level to advanced:

```
set -priv advanced
```

3. Enable Cloud KMS on the SVM

```
security key-manager external gcp enable -vserver svm_name -project-id  
project_id-key-ring-name key_ring_name -key-ring-location key_ring_location  
-key-name key_name
```

When prompted, enter the contents of the JSON file with the Service Account Private Key

4. Verify that Cloud KMS is configured with the correct parameters:

```
security key-manager external gcp show vserver svm_name
```

The status of `kms_wrapped_key_status` will be "UNKNOWN" if no encrypted volumes have been created.

If the service reachability is not OK, establish the connectivity to the GCP key management service via data SVM LIF.

If one or more encrypted volumes is already configured for a data SVM and the corresponding NVE keys are managed by the admin SVM onboard key manager, those keys should be migrated to the external key management service. To do this with the CLI, run the command:

```
security key-manager key migrate -from-Vserver admin_SVM -to-Vserver data_SVM
```

New encrypted volumes cannot be created for the tenant's data SVM until all NVE keys of the data SVM are successfully migrated.

#### Related information

- [Encrypting volumes with NetApp encryption solutions for Cloud Volumes ONTAP](#)

## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.