# NetApp

# Manage security with System Manager

ONTAP 9

NetApp
June 26, 2023

# Table of Contents

# Manage security with System Manager

## Security management overview with System Manager

Beginning with ONTAP 9.7, you can manage cluster security with System Manager.

With System Manager, you use ONTAP standard methods to secure client and administrator access to storage and to protect against viruses. Advanced technologies are available for encryption of data at rest and for WORM storage.

If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), refer to System Manager Classic (ONTAP 9.0 to 9.7)

### Client authentication and authorization

ONTAP authenticates a client machine and user by verifying their identities with a trusted source. ONTAP authorizes a user to access a file or directory by comparing the user's credentials with the permissions configured on the file or directory.

### Administrator authentication and RBAC

Administrators use local or remote login accounts to authenticate themselves to the cluster and storage VM. Role-Based Access Control (RBAC) determines the commands to which an administrator has access.

### Virus scanning

You can use integrated antivirus functionality on the storage system to protect data from being compromised by viruses or other malicious code. ONTAP virus scanning, called *Vscan*, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

### Encryption

ONTAP offers both software- and hardware-based encryption technologies for ensuring that data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen.

### WORM storage

*SnapLock* is a high-performance compliance solution for organizations that use *write once*, *read many (WORM)* storage to retain critical files in unmodified form for regulatory and governance purposes.

## Set up multifactor authentication

Security Assertion Markup Language (SAML) authentication allows users to log in to an application by using a secure identity provider (IdP).

In System Manager, in addition to standard ONTAP authentication, SAML-based authentication is provided as an option for multifactor authentication.

Security Assertion Markup Language (SAML) is an XML-based framework for authentication and authorization between two entities: a service provider and an identity provider.

# Enable SAML authentication



To enable SAML authentication, perform the following steps:

**Steps**

1. Click **Cluster > Settings**.

2. Next to **SAML Authentication**, click ⚙.

3. Ensure there is a check in the **Enable SAML Authentication** checkbox.

4. Enter the URL of the IdP URI (including "https://").

5. Modify the host system address, if needed.

6. Ensure the correct certificate is being used:
   - If your system was mapped with only one certificate with type "server", then that certificate is considered the default and it isn't displayed.
   - If your system was mapped with multiple certificates as type "server", then one of the certificates is displayed. To select a different certificate, click **Change**.

7. Click **Save**. A confirmation window displays the metadata information, which has been automatically copied to your clipboard.

8. Go to the IdP system you specified and copy the metadata from your clipboard to update the system metadata.

9. Return to the confirmation window (in System Manager) and check the checkbox **I have configured the IdP with the host URI or metadata**.

10. Click **Logout** to enable SAML-based authentication. The IdP system will display an authentication screen.

11. In the IdP system, enter your SAML-based credentials. After your credentials are verified, you will be directed to the System Manager home page.

# Disable SAML authentication

To disable SAML authentication, perform the following steps:

**Steps**

1. Click **Cluster > Settings**.
2. Under **SAML Authentication**, click the **Enabled** toggle button.
3. *Optional*: You can also click ⚙ next to **SAML Authentication**, and then uncheck the **Enable SAML Authentication** checkbox.

# Control administrator access

The role assigned to an administrator determines which functions the administrator can perform with System Manager. Predefined roles for cluster administrators and storage VM administrators are provided by System Manager. You assign the role when you create the administrator's account, or you can assign a different role later.

Depending on how you have enabled account access, you might need to perform any of the following:

- Associate a public key with a local account.
- Install a CA-signed server digital certificate.
- Configure AD, LDAP, or NIS access.

You can perform these tasks before or after enabling account access.

## Assigning a role to an administrator

Assign a role to an administrator, as follows:

**Steps**

1. Select **Cluster > Settings**.
2. Select → next to **Users and Roles**.
3. Select ＋ Add under **Users**.
4. Specify a user name, and select a role in the drop-down menu for **Role**.
5. Specify a login method and password for the user.

## Changing an administrator's role

Change the role for an administrator, as follows:

**Steps**

1. Click **Cluster > Settings**.
2. Select the name of user whose role you want to change, then click the ⋮ that appears next to the user name.
3. Click **Edit**.
4. Select a role in the drop-down menu for **Role**.

# Diagnose and correct file access issues

**Steps**

1. In System Manager, select **Storage > Storage VMs**.

2. Select the storage VM on which you want to perform a trace.

3. Click ⋮ **More**.

4. Click **Trace File Access**.

5. Provide the user name and client IP address, then click **Start Tracing**.

   The trace results are displayed in a table. The **Reasons** column provides the reason why a file could not be accessed.

6. Click ⌄ in the left column of the results table to view the file access permissions.

# Manage certificates with System Manager

Beginning with ONTAP 9.10.1, you can use System Manager to manage trusted certificate authorities, client/server certificates, and local (onboard) certificate authorities.

With System Manager, you can manage the certificates received from other applications so you can authenticate communications from those applications. You can also manage your own certificates that identify your system to other applications.

## View certificate information

With System Manager, you can view trusted certificate authorities, client/server certificates, and local certificate authorities that are stored on the cluster.

**Steps**

1. In System Manager, click **Cluster > Settings**.

2. Scroll to the **Security** area.
   In the **Certificates** section, the following details are displayed:

   ◦ The number of stored trusted certificate authorities.

   ◦ The number of stored client/server certificates.

   ◦ The number of stored local certificate authorities.

3. Click any number to view details about a category of certificates, or click → to view the **Certificates** page, which contains information about all categories.
   The list displays the information for the entire cluster. If you want to display information for only a specific storage VM, perform the following steps:

   a. Click **Storage > Storage VMs**.

   b. Select the storage VM.

   c. View the **Settings** tab.

   d. Click a number shown in the **Certificate** section.

**What to do next**

- From the **Certificates** page, you can Generate a certificate signing request.

- The certificate information is separated into three tabs, one for each category. You can perform the following tasks from each tab:

| On this tab… | You can perform these procedures… |
|---|---|
| **Trusted certificate authorities** | • Install (add) a trusted certificate authority<br>• Delete a trusted certificate authority<br>• Renew a trusted certificate authority |
| **Client/server certificates** | • Install (add) a client/server certificate<br>• Generate (add) a self-signed client/server certificate<br>• Delete a client/server certificate<br>• Renew a client/server certificate |
| **Local certificate authorities** | • Create a new local certificate authority<br>• Sign a certificate using a local certificate authority<br>• Delete a local certificate authority<br>• Renew a local certificate authority |

## Generate a certificate signing request

You can generate a certificate signing request (CSR) with System Manager from any tab of the **Certificates** page. A private key and a corresponding CSR are generated, which can be signed using a certificate authority to generate a public certificate.

**Steps**

1. View the **Certificates** page. See View certificate information.

2. Click **+Generate CSR**.

3. Complete the information for the subject name:

    a. Enter a **common name**.

    b. Select a **country**.

    c. Enter an **organization**.

    d. Enter an **organization unit**.

4. If you want to override defaults, select **More Options** and provide additional information.

## Install (add) a trusted certificate authority

You can install additional trusted certificate authorities in System Manager.

**Steps**

1. View the **Trusted Certificate Authorities** tab. See View certificate information.

2. Click + Add .

3. On the **Add Trusted Certificate Authority** panel, perform the following:

    ◦ Enter a **name**.

    ◦ For the **scope**, select a storage VM.

- Enter a **common name**.

- Select a **type**.

- Enter or import **certificate details**.

## Delete a trusted certificate authority

With System Manager, you can delete a trusted certificate authority.

ⓘ | You cannot delete trusted certificate authorities that were preinstalled with ONTAP.

**Steps**

1. View the **Trusted Certificate Authorities** tab. See View certificate information.

2. Click the name of the trusted certificate authority.

3. Click ⁝ next to the name, then click **Delete**.

## Renew a trusted certificate authority

With System Manager, you can renew a trusted certificate authority that has expired or is about to expire.

**Steps**

1. View the **Trusted Certificate Authorities** tab. See View certificate information.

2. Click the name of the trusted certificate authority.

3. Click ⁝ next to the name, then click **Renew**.

## Install (add) a client/server certificate

With System Manager, you can install additional client/server certificates.

**Steps**

1. View the **Client/Server Certificates** tab. See View certificate information.

2. Click **+ Add**.

3. On the **Add Client/Server Certificate** panel, perform the following:

- Enter a **certificate name**.

- For the **scope**, select a storage VM.

- Enter a **common name**.

- Select a **type**.

- Enter or import **certificate details**.
  You can either write in or copy and paste in the certificate details from a text file or you can import the text from a certificate file by clicking **Import**.

- Enter a the **private key**.
  You can either write in or copy and paste in the private key from a text file or you can import the text from a private key file by clicking **Import**.

## Generate (add) a self-signed client/server certificate

With System Manager, you can generate additional self-signed client/server certificates.

**Steps**

1. View the **Client/Server Certificates** tab. See View certificate information.

2. Click **+Generate Self-signed Certificate**.

3. On the **Generate Self-Signed Certificate** panel, perform the following:

   ◦ Enter a **certificate name**.

   ◦ For the **scope**, select a storage VM.

   ◦ Enter a **common name**.

   ◦ Select a **type**.

   ◦ Select a **hash function**.

   ◦ Select a **key size**.

   ◦ Select a **storage VM**.

## Delete a client/server certificate

With System Manager, you can delete client/server certificates.

**Steps**

1. View the **Client/Server Certificates** tab. See View certificate information.

2. Click the name of the client/server certificate.

3. Click ⋮ next to the name, then click **Delete**.

## Renew a client/server certificate

With System Manager, you can renew a client/server certificate that has expired or is about to expire.

**Steps**

1. View the **Client/Server Certificates** tab. See View certificate information.

2. Click the name of the client/server certificate.

3. Click ⋮ next to the name, then click **Renew**.

## Create a new local certificate authority

With System Manager, you can create a new local certificate authority.

**Steps**

1. View the **Local Certificate Authorities** tab. See View certificate information.

2. Click **+ Add** .

3. On the **Add Local Certificate Authority** panel, perform the following:

   ◦ Enter a **name**.

   ◦ For the **scope**, select a storage VM.

- Enter a **common name**.

4. If you want to override defaults, select **More Options** and provide additional information.

## Sign a certificate using a local certificate authority

In System Manager, you can use a local certificate authority to sign a certificate.

**Steps**

1. View the **Local Certificate Authorities** tab. See View certificate information.
2. Click the name of the local certificate authority.
3. Click ⋮ next to the name, then click **Sign a certificate**.
4. Complete the **Sign a Certificate Signing Request** form.
   - You can either paste in the certificate signing content or import a certificate signing request file by clicking **Import**.
   - Specify the number of days for which the certificate will be valid.

## Delete a local certificate authority

With System Manager, you can delete a local certificate authority.

**Steps**

1. View the **Local Certificate Authority** tab. See View certificate information.
2. Click the name of the local certificate authority.
3. Click ⋮ next to the name, then click **Delete**.

## Renew a local certificate authority

With System Manager, you can renew a local certificate authority that has expired or is about to expire.

**Steps**

1. View the **Local Certificate Authority** tab. See View certificate information.
2. Click the name of the local certificate authority.
3. Click ⋮ next to the name, then click **Renew**.

# Manage external key managers

Beginning with ONTAP 9.13.1, you can use System Manager to manage external key managers to store and manage authentication and encryption keys.

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 use both the Onboard Key Manager and external key managers to store and manage authentication and encryption keys.

The Onboard Key Manager is used to store and manage keys in a secure database that is internal to the cluster. An external key manager stores and manages keys, but it is external to the cluster. One or more external key managers can be used to store and manage keys.

The scope of the Onboard Key Manager is at the cluster level; however, the scope of external key managers

can be either at the cluster level or at a storage VM level.

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. Conversely, 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

### Before you start

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

2. To add a primary key server, click ➕ Add , and complete the **IP Address or Host Name** and **Port** fields.

3. Existing installed certificates are listed in the **KMIP Server CA Certificates** and **KMIP Client Certificate** fields. You can perform any of the following actions:

   ◦ Click ⌄ 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.

   ◦ Click ✕ next to the certificate name to delete installed certificates that you do not want to map to the external key manager.

4. To add a secondary key server, click **Add** in the **Secondary Key Servers** column, and provide its details.

5. Click **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**

1. 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 | **Cluster** > **Settings** | Scroll to the **Security** section. Under **Encryption**, select ⋮, then select **Edit External Key Manager**. |
| Storage VM scope external key manager | **Storage** > **Storage VMs** | Select the storage VM. Click the **Settings** tab. In the **Encryption** section under **Security**, select ⋮, then select **Edit External Key Manager**. |

2. Existing key servers are listed in the **Key Servers** table. You can perform the following operations:

   ◦ Add a new key server by clicking ➕ Add .

   ◦ Delete a key server by clicking ⋮ 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 | **Cluster** > **Settings** | Scroll to the **Security** section. Under **Encryption**, select select ⋮, then select **Delete External Key Manager**. |
| Storage VM scope external key manager | **Storage** > **Storage VMs** | Select the storage VM. Click the **Settings** tab. In the **Encryption** section under **Security**, select ⋮, then select **Delete External Key Manager**. |

## 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.