Use array certificates

SANtricity 11.7

NetApp
February 12, 2024

Table of Contents

Use array certificates . . . 1
- Import certificates for arrays . . . 1
- Delete trusted certificates . . . 1
- Resolve untrusted certificates . . . 2

Use array certificates

Import certificates for arrays

If necessary, you can import certificates for the storage arrays so they can authenticate with the system hosting Unified Manager. Certificates can be signed by a certificate authority (CA) or can be self-signed.

Before you begin

- You must be logged in with a user profile that includes Security admin permissions. Otherwise, certificate functions do not appear.
- If you are importing trusted certificates, the certificates must be imported for the storage array controllers using System Manager.

Steps

1. Select **Certificate Management**.
2. Select the **Trusted** tab.

   This page shows all certificates reported for the storage arrays.

3. Select either **Import › Certificates** to import a CA certificate or **Import › Self-signed storage array certificates** to import a self-signed certificate.

   To limit the view, you can use the **Show certificates that are…** filtering field or you can sort the certificate rows by clicking one of the column heads.

4. In the dialog box, select the certificate and then click **Import**.

   The certificate is uploaded and validated.

Delete trusted certificates

You can delete one or more certificates that are no longer needed, such as an expired certificate.

Before you begin

Import the new certificate before deleting the old one.

Be aware that deleting a root or intermediate certificate can impact multiple storage arrays, since these arrays can share the same certificate files.

Steps

1. Select **Certificate Management**.
2. Select the **Trusted** tab.
3. Select one or more certificates in the table, and then click **Delete**.

The **Delete** function is not available for pre-installed certificates.

The Confirm Delete Trusted Certificate dialog box opens.

4. Confirm the deletion, and then click **Delete**.

   The certificate is removed from the table.

Resolve untrusted certificates

Untrusted certificates occur when a storage array attempts to establish a secure connection to Unified Manager, but the connection fails to confirm as secure.

From the Certificate page, you can resolve untrusted certificates by importing a self-signed certificate from the storage array or by importing a certificate authority (CA) certificate that has been issued by a trusted third party.

Before you begin

- You must be logged in with a user profile that includes Security Admin permissions.
- If you plan to import a CA-signed certificate:
  - You have generated a certificate signing request (.CSR file) for each controller in the storage array and sent it to the CA.
  - The CA returned trusted certificate files.
  - The certificate files are available on your local system.

About this task

You might need to install additional trusted CA certificates if any of the following are true:

- You recently added a storage array.
- One or both certificates are expired.
- One or both certificates are revoked.
- One or both certificates are missing a root or intermediate certificate.

Steps

1. Select **Certificate Management**.
2. Select the **Trusted** tab.

   This page shows all certificates reported for the storage arrays.

3. Select either **Import › Certificates** to import a CA certificate or **Import › Self-Signed storage array certificates** to import a self-signed certificate.

   To limit the view, you can use the **Show certificates that are…** filtering field or you can sort the certificate rows by clicking one of the column heads.

4. In the dialog box, select the certificate, and then click **Import**.

   The certificate is uploaded and validated.

Copyright information

Trademark information