Manage certificates

E-Series Systems

NetApp
July 14, 2022

Table of Contents

Manage certificates

Certificates overview

Certificate Management in the Storage Plugin for vCenter allows you to create certificate signing requests (CSRs), import certificates, and manage existing certificates.

What are certificates?

Certificates are digital files that identify online entities, such as websites and servers, for secure communications on the internet. They ensure that web communications are transmitted in encrypted form, privately and unaltered, only between the specified server and client. Using the Storage Plugin for vCenter, you can manage certificates for the browser on a host management system and the controllers in the discovered storage arrays.

A certificate can be signed by a trusted authority, or it can be self-signed. "Signing" simply means that someone validated the owner's identity and determined that their devices can be trusted.

Storage arrays ship with an automatically generated self-signed certificate on each controller. You can continue to use the self-signed certificates, or you can obtain CA-signed certificates for a more secure connection between the controllers and the host systems.

> ⓘ Although CA-signed certificates provide better security protection (for example, preventing man-in-the-middle attacks), they also require fees that can be expensive if you have a large network. In contrast, self-signed certificates are less secure, but they are free. Therefore, self-signed certificates are most often used for internal testing environments, not in production environments.

Signed certificates

A signed certificate is validated by a certificate authority (CA), which is a trusted third-party organization. Signed certificates include details about the owner of the entity (typically, a server or website), date of certificate issue and expiration, valid domains for the entity, and a digital signature composed of letters and numbers.

When you open a browser and enter a web address, your system performs a certificate-checking process in the background to determine if you are connecting to a website that includes a valid, CA-signed certificate. Generally, a site that is secured with a signed certificate includes a padlock icon and an https designation in the address. If you attempt to connect to a website that does not contain a CA-signed certificate, your browser displays a warning that the site is not secure.

The CA takes steps to verify your identity during the application process. They might send an email to your registered business, verify your business address, and perform an HTTP or DNS verification. When the application process is complete, the CA sends you digital files to load on a host management system. Typically, these files include a chain of trust, as follows:

- **Root** — At the top of the hierarchy is the root certificate, which contains a private key used to sign other certificates. The root identifies a particular CA organization. If you use the same CA for all your network devices, you need only one root certificate.
- **Intermediate** — Branching off from the root are the intermediate certificates. The CA issues one or more intermediate certificates to act as middlemen between a protected root and server certificates.

- **Server** — At the bottom of the chain is the server certificate, which identifies your specific entity, such as a website or other device. Each controller in a storage array requires a separate server certificate.

Self-signed certificates

Each controller in the storage array includes a pre-installed, self-signed certificate. A self-signed certificate is similar to a CA-signed certificate, except that it is validated by the owner of the entity instead of a third party. Like a CA-signed certificate, a self-signed certificate contains its own private key, and also ensures that data is encrypted and sent over an HTTPS connection between a server and client.

Self-signed certificates are not "trusted" by browsers. Each time you attempt to connect to a website that contains only a self-signed certificate, the browser displays a warning message. You must click a link in the warning message that allows you to proceed to the website; by doing so, you are essentially accepting the self-signed certificate.

Management certificate

When you open the plugin, the browser attempts to verify that the management host is a trusted source by checking for a digital certificate. If the browser does not locate a CA-signed certificate, it opens a warning message. From there, you can continue to the website to accept the self-signed certificate for that session. You can also obtain signed, digital certificates from a CA so you no longer see the warning message.

Trusted certificates

During a plugin session, you might see additional security messages when you attempt to access a controller that does not have a CA-signed certificate. In this event, you can permanently trust the self-signed certificate or you can import the CA-signed certificates for the controllers so the plugin can authenticate incoming client requests from these controllers.

Use CA-signed certificates

You can obtain and import CA-signed certificates for secure access to the management system hosting the Storage Plugin for vCenter.

Using CA-signed certificates is a three-step procedure:

- Step 1: Complete a CSR file.
- Step 2: Submit CSR file.
- Step 3: Import management certificates.

Step 1: Complete a CSR file

You must first generate a certificate signing request (CSR) file, which identifies your organization and the host system where the plugin is running. Alternatively, you can generate a CSR file using a tool such as OpenSSL and skip to Step 2: Submit CSR file.

Steps

1. Select **Certificate Management**.
2. From the **Management** tab, select **Complete CSR**.
3. Enter the following information, and then click **Next**:

- **Organization** — The full, legal name of your company or organization. Include suffixes, such as Inc. or Corp.
        - **Organizational unit (optional)** — The division of your organization that is handling the certificate.
        - **City/Locality** — The city where your host system or business is located.
        - **State/Region (optional)** — The state or region where your host system or business is located.
        - **Country ISO code** — Your country's two-digit ISO (International Organization for Standardization) code, such as US.
4. Enter the following information about the host system where the plugin is running:
        - **Common name** — The IP address or DNS name of the host system where the plugin is running. Make sure this address is correct; it must match exactly what you enter to access the plugin in the browser. Do not include http:// or https://. The DNS name cannot begin with a wildcard.
        - **Alternate IP addresses** — If the common name is an IP address, you can optionally enter any additional IP addresses or aliases for the host system. For multiple entries, use a comma-delimited format.
        - **Alternate DNS names** — If the common name is a DNS name, enter any additional DNS names for the host system. For multiple entries, use a comma-delimited format. If there are no alternate DNS names, but you entered a DNS name in the first field, copy that name here. The DNS name cannot begin with a wildcard.
5. Make sure that the host information is correct. If it is not, the certificates returned from the CA will fail when you try to import them.
6. Click **Finish**.

Step 2: Submit CSR file

After you create a certificate signing request (CSR) file, you send the generated CSR file to a CA to receive signed, management certificates for the system hosting the plugin.

E-Series systems require PEM format (Base64 ASCII encoding) for signed certificates, which includes the following file types: .pem, .crt, .cer, or .key.

Steps

1. Locate the downloaded CSR file.

   The folder location of the download depends on your browser.

2. Submit the CSR file to a CA (for example, Verisign or DigiCert), and request signed certificates in PEM format.

   ⚠️   After you submit a CSR file to the CA, do NOT regenerate another CSR file.

Whenever you generate a CSR, the system creates a private and public key pair. The public key is part of the CSR, while the private key is kept in the system's keystore. When you receive the signed certificates and import them, the system ensures that both the private and public keys are the original pair. If the keys do not match, the signed certificates will not work and you must request new certificates from the CA.

Step 3: Import management certificates

After you receive signed certificates from the Certificate Authority (CA), import the certificates into the host system where the plugin is installed.

Before you begin

- You must have the signed certificates from the CA. These files include the root certificate, one or more intermediate certificates, and the server certificate.

- If the CA provided a chained certificate file (for example, a .p7b file), you must unpack the chained file into individual files: the root certificate, one or more intermediate certificates, and the server certificate. You can use the Windows certmgr utility to unpack the files (right-click and select **All Tasks › Export**). Base-64 encoding is recommended. When the exports are complete, a CER file is shown for each certificate file in the chain.

- You must copy the certificate files to the host system where the plugin is running.

Steps

1. Select **Certificate Management**.

2. From the **Management** tab, select **Import**.

   A dialog box opens for importing the certificate files.

3. Click **Browse** to first select the root and intermediate certificate files, and then select the server certificate. If you generated the CSR from an external tool, you must also import the private key file that was created along with the CSR.

   The filenames are displayed in the dialog box.

4. Click **Import**.

Result

The files are uploaded and validated. The certificate information displays on the Certificate Management page.

Reset management certificates

For the management system hosting the Storage Plugin for vCenter, you can revert the management certificate to the original, factory self-signed state.

About this task

This task deletes the current management certificate from the host system where the Storage Plugin for vCenter is running. After the certificate is reset, the host system reverts to using the self-signed certificate.

Steps

1. Select **Certificate Management**.

2. From the **Management** tab, select **Reset**.

   A Confirm Reset Management Certificate dialog box opens.

3. Type reset in the field, and then click **Reset**.

   After your browser refreshes, the browser might block access to the destination site and report that the site is using HTTP Strict Transport Security. This condition arises when you switch back to self-signed certificates. To clear the condition that is blocking access to the destination, you must clear the browsing data from the browser.

Result

The system reverts to using the self-signed certificate from the server. As a result, the system prompts users to manually accept the self-signed certificate for their sessions.

Import certificates for arrays

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

Before you begin

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.

4. 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.

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

   The certificate is uploaded and validated.

View certificates

You can view summary information for a certificate, which includes the organization using the certificate, the authority that issued the certificate, the period of validity, and the fingerprints (unique identifiers).

Steps

1. Select **Certificate Management**.

2. Select one of the following tabs:

   - **Management** — Shows the certificate for the system hosting the plugin. A management certificate can be self-signed or approved by a certificate authority (CA). It allows secure access to the plugin.

   - **Trusted** — Shows certificates that the plugin can access for storage arrays and other remote servers, such as an LDAP server. The certificates can be issued from a certificate authority (CA) or can be self-signed.

3. To see more information about a certificate, select its row, select the ellipses at the end of the row, and then click **View** or **Export**.

Export certificates

You can export a certificate to view its complete details.

Before you begin

To open the exported file, you must have a certificate viewer application.

Steps

1. Select **Certificate Management**.

2. Select one of the following tabs:

   - **Management** — Shows the certificate for the system hosting the plugin. A management certificate can be self-signed or approved by a certificate authority (CA). It allows secure access to the plugin.

   - **Trusted** — Shows certificates that the plugin can access for storage arrays and other remote servers, such as an LDAP server. The certificates can be issued from a certificate authority (CA) or can be self-signed.

3. Select a certificate from the page, and then click the ellipses at the end of the row.

4. Click **Export**, and then save the certificate file.

5. Open the file in your certificate viewer application.

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**.

   > ℹ️ 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

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

If you plan to import a CA-signed certificate, make sure that:

- 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

Untrusted certificates occur when a storage array attempts to establish a secure connection to the plugin, but the connection fails to confirm as secure. 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 or 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.
4. 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.
5. In the dialog box, select the certificate, and then click **Import**.

   The certificate is uploaded and validated.