Use certificates

SANtricity 11.7

NetApp
February 12, 2024

Table of Contents

Use certificates

Use CA-signed certificates for controllers

You can obtain CA-signed certificates for secure communications between the controllers and the browser used for accessing System Manager.

Before you begin

- You must be logged in with a user profile that includes Security admin permissions. Otherwise, certificate functions do not appear.
- You must know the IP address or DNS names of each controller.

About this task

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

Step 1: Complete CSRs for the controllers

You must first generate a certificate signing request (CSR) file for each controller in the storage array.

About this task

This task describes how to generate a CSR file from System Manager. The CSR provides information about your organization, and either the IP address or DNS name of the controller. During this task, one CSR file is generated if the storage array has one controller and two CSR files if it has two controllers.

> Alternatively, you can generate a CSR file using a tool such as OpenSSL and can skip to Step 2: Submit the CSR files.

Steps

1. Select **Settings › Certificates**.
2. From the Array Management tab, select **Complete CSR**.

> If you see a dialog box prompting you to accept a self-signed certificate for the second controller, click **Accept Self-Signed Certificate** to proceed.

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 storage array or business is located.
   - **State/Region (optional)** — The state or region where your storage array or business is located.
   - **Country ISO code** — Your country's two-digit ISO (International Organization for Standardization) code, such as US.

Some fields might be pre-populated with the appropriate information, such as the IP address of the controller. Do not change prepopulated values unless you are certain they are incorrect. For example, if you have not yet completed a CSR, the controller IP address is set to “localhost.” In this case, you must change “localhost” to the DNS name or IP address of the controller.

4. Verify or enter the following information about controller A in your storage array:
   - **Controller A common name** — The IP address or DNS name of controller A is displayed by default. Make sure this address is correct; it must match exactly what you enter to access System Manager in the browser. The DNS name cannot begin with a wildcard.
   - **Controller A alternate IP addresses** — If the common name is an IP address, you can optionally enter any additional IP addresses or aliases for controller A. For multiple entries, use a comma-delimited format.
   - **Controller A alternate DNS names** — If the common name is a DNS name, enter any additional DNS names for controller A. 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. If the storage array has only one controller, the **Finish** button is available.

     If the storage array has two controllers, the **Next** button is available.

Do not click the **Skip this step** link when you are initially creating a CSR request. This link is provided in error-recovery situations. In rare cases, a CSR request might fail on one controller, but not on the other. This link allows you to skip the step for creating a CSR request on controller A if it is already defined, and continue to the next step for re-creating a CSR request on controller B.

5. If there is only one controller, click **Finish**. If there are two controllers, click **Next** to enter information for controller B (same as above), and then click **Finish**.

   For a single controller, one CSR file is downloaded to your local system. For dual controllers, two CSR files are downloaded. The folder location of the download depends on your browser.

6. Go to Step 2: Submit the CSR files.

Step 2: Submit the CSR files

After you create the certificate signing request (CSR) files, send the files to a certificate authority (CA). 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 files.
2. Submit the CSR files 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.

3. When the CA returns the signed certificates, go to Step 3: Import signed certificates for controllers.

Step 3: Import signed certificates for controllers

After you receive signed certificates from the Certificate Authority (CA), import the files for the controllers.

Before you begin

- The CA returned signed certificate files. These files include the root certificate, one or more intermediate certificates, and the server certificates.
- 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 certificates that identify the controllers. 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 have copied the certificate files to the host system where you access System Manager.

Steps

1. Select **Settings › Certificates**
2. From the Array Management tab, select **Import**.

   A dialog box opens for importing the certificate file(s).

3. Click the **Browse** buttons to first select the root and intermediate certificate files, and then select each server certificate for the controllers. The root and intermediate files are the same for both controllers. Only the server certificates are unique for each controller. 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 file names are displayed in the dialog box.

4. Click **Import**.

   The files are uploaded and validated.

Result

The session is automatically terminated. You must log in again for the certificates to take effect. When you log in again, the new CA-signed certificates are used for your session.

Reset management certificates

You can revert the certificates on the controllers from using CA-signed certificates back to the factory-set, self-signed certificates.

Before you begin

- You must be logged in with a user profile that includes Security admin permissions. Otherwise, certificate functions do not appear.
- CA-signed certificates must be previously imported.

About this task

The Reset function deletes the current CA-signed certificate files from each controller. The controllers will then revert to using self-signed certificates.

Steps

1. Select **Settings › Certificates**.
2. From the Array Management tab, select **Reset**.

   A Confirm Reset Management Certificates 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.

Results

The controllers revert to using self-signed certificates. As a result, the system prompts users to manually accept the self-signed certificate for their sessions.

View imported certificate information

From the Certificates page, you can view the certificate type, issuing authority, and the valid date range of certificates for the storage array.

Before you begin

You must be logged in with a user profile that includes Security admin permissions. Otherwise, certificate functions do not appear.

Steps

1. Select **Settings › Certificates**.
2. Select one of the tabs to view information about the certificates.

Tab	Description
Array Management	View information about the CA-signed certificates imported for each controller, including the root file, intermediate file(s), and the server file(s).

Tab	Description
Trusted	View information about all other types of certificates imported for the controllers. Use the filter field under **Show certificates that are…** to view either user-installed or pre-installed certificates. • **User-installed** — Certificates that a user uploaded to the storage array, which can include trusted certificates when the controller acts as a client (instead of a server), LDAPS certificates, and Identity Federation certificates. • **Pre-installed** — Self-signed certificates included with the storage array.
Key Management	View information about the CA-signed certificates imported for an external key management server.

Import certificates for controllers when acting as clients

If the controller rejects a connection because it cannot validate the chain of trust for a network server, you can import a certificate from the Trusted tab that allows the controller (acting as a client) to accept communications from that server.

Before you begin

- You must be logged in with a user profile that includes Security admin permissions. Otherwise, certificate functions do not appear.
- The certificate files are installed on your local system.

About this task

Importing certificates from the Trusted tab might be necessary if you want to allow another server to contact the controllers (for example, an LDAP server or a syslog server that uses TLS).

Steps

1. Select **Settings › Certificates**.
2. From the Trusted tab, select **Import**.

   A dialog box opens for importing the trusted certificate files.
3. Click **Browse** to select the certificate files for the controllers.

   The file names display in the dialog box.
4. Click **Import**.

Results

The files are uploaded and validated.

Enable certificate revocation checking

You can enable automatic checks for revoked certificates, so that an Online Certificate

Status Protocol (OCSP) server blocks users from making non-secure connections.

Before you begin

- You must be logged in with a user profile that includes Security admin permissions. Otherwise, certificate functions do not appear.
- A DNS server is configured on both controllers, which enables use of a fully qualified domain name for the OCSP server. This task is available from the Hardware page.
- If you want to specify your own OCSP server, you must know the URL of that server.

About this task

Automatic revocation checking is helpful in cases where the CA improperly issued a certificate, or a private key is compromised.

During this task, you can configure an OCSP server or use the server specified in the certificate file. The OCSP server determines if the CA has revoked any certificates before their scheduled expiration date, and then blocks the user from accessing a site if the certificate is revoked.

Steps

1. Select **Settings › Certificates**.
2. Select the **Trusted** tab.

   You can also enable revocation checking from the **Key Management** tab.

3. Click **Uncommon Tasks**, and then select **Enable Revocation Checking** from the drop-down menu.
4. Select **I want to enable revocation checking**, so that a checkmark appears in the checkbox and additional fields appear in the dialog box.
5. In the **OCSP responder address** field, you can optionally enter a URL for an OCSP responder server. If you do not enter an address, the system uses the OCSP server's URL from the certificate file.
6. Click **Test Address** to make certain the system can open a connection to the specified URL.
7. Click **Save**.

Results

If the storage array attempts to connect to a server with a revoked certificate, the connection is denied and an event is logged.

Delete trusted certificates

You can delete the user-installed certificates previously imported from the Trusted tab.

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 updating a trusted certificate with a new version, the updated certificate must be imported before you delete the old certificate.

You might lose access to a system if you delete a certificate used to authenticate the controllers and another server, such as an LDAP server, before you import a replacement certificate.

About this task

This task describes how to delete user-installed certificates. The pre-installed, self-signed certificates cannot be deleted.

Steps

1. Select **Settings › Certificates**.
2. Select the **Trusted** tab.

   The table shows the storage array's trusted certificates.

3. From the table, select the certificate you want to remove.
4. Click **Uncommon Tasks › Delete**.

   A Confirm Delete Trusted Certificate dialog box opens.

5. Type `delete` in the field, and then click **Delete**.

Use CA-signed certificates for authentication with a key management server

For secure communications between a key management server and the storage array controllers, you must configure the appropriate sets of certificates.

Before you begin

You must be logged in with a user profile that includes Security admin permissions. Otherwise, certificate functions do not appear.

About this task

Authenticating between the controllers and a key management server is a two-step procedure.

Step 1: Complete and submit CSR for authentication with a key management server

You must first generate a certificate signing request (CSR) file, and then use the CSR to request a signed client certificate from a certificate authority (CA) that is trusted by the key management server. You can also create and download a client certificate from the key management server using the downloaded CSR file. A client certificate validates the storage array's controllers, so the key management server can trust their Key Management Interoperability Protocol (KMIP) requests.

Steps

1. Select **Settings › Certificates**.
2. From the Key Management tab, select **Complete CSR**.
3. Enter the following information:
   - **Common name** — A name that identifies this CSR, such as the storage array name, which will be displayed in the certificate files.
   - **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 or locality where your organization is located.
- **State/Region (optional)** — The state or region where your organization is located.
- **Country ISO code** — The two-digit ISO (International Organization for Standardization) code, such as US, where your organization is located.

4. Click **Download**.

   A CSR file is saved to your local system.

5. Request a signed client certificate from a CA that is trusted by the key management server.
6. When you have a client certificate, go to Step 2: Import certificates for the key management server.

Step 2: Import certificates for the key management server

As the next step, you import certificates for authentication between the storage array and the key management server. There are two types of certificates: the client certificate validates the storage array's controllers, while the key management server certificate validates the server. You must load both the client certificate file for the controllers and the server certificate file for the key management server.

Before you begin

- You have a signed client certificate file (see Step 1: Complete and submit CSR for authentication with a key management server), and you have copied that file to the host where you are accessing System Manager. A client certificate validates the storage array's controllers, so the key management server can trust their Key Management Interoperability Protocol (KMIP) requests.
- You must retrieve a certificate file from the key management server, and then copy that file to the host where you are accessing System Manager. A key management server certificate validates the key management server, so the storage array can trust its IP address. You can use a root, intermediate, or server certificate for the key management server.

> For more information about the server certificate, consult the documentation for your key management server.

Steps

1. Select **Settings › Certificates**.
2. From the Key Management tab, select **Import**.

   A dialog box opens for importing the certificate files.

3. Next to **Select client certificate**, click the **Browse** button to select the client certificate file for the storage array's controllers.

   The file name displays in the dialog box.

4. Next to **Select key management server's server certificate**, click the **Browse** button to select the server certificate file for your key management server. You can choose a root, intermediate, or server certificate for the key management server.

   The file name displays in the dialog box.

5. Click **Import**.

The files are uploaded and validated.

Export key management server certificates

You can save a certificate for a key management server to your local machine.

Before you begin

- You must be logged in with a user profile that includes Security admin permissions. Otherwise, certificate functions do not appear.
- Certificates must be previously imported.

Steps

1. Select **Settings** › **Certificates**.
2. Select the **Key Management** tab.
3. From the table, select the certificate you want to export, and then click **Export**.

   A Save dialog box opens.

4. Enter a filename and click **Save**.

Copyright information

Trademark information