Certificates

SANtricity 11.6

NetApp
February 12, 2024

Table of Contents

Certificates

Concepts

How certificates work

Certificates are digital files that identify online entities, such as websites and servers, for secure communications on the internet.

Certificates ensure that web communications are transmitted in encrypted form, privately and unaltered, only between the specified server and client. Using System Manager, you can manage certificates between the browser on a host management system (acting as the client) and the controllers in a storage system (acting as the servers).

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 an 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. However, a self-signed certificate does not use the same chain of trust as a CA-signed certificate.

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.

Certificates used for key management server

If you are using an external key management server with the Drive Security feature, you can also manage certificates for authentication between that server and the controllers.

Certificate terminology

The following terms apply to certificate management.

Term	Description
CA	A certificate authority (CA) is a trusted entity that issues electronic documents, called digital certificates, for Internet security. These certificates identify website owners, which allows for secure connections between clients and servers.
CSR	A Certificate Signing Request (CSR) is a message that is sent from an applicant to a certificate authority (CA). The CSR validates the information the CA requires to issue a certificate.
Certificate	A certificate identifies the owner of a site for security purposes, which prevents attackers from impersonating the site. The certificate contains information about the site owner and the identity of the trusted entity who certifies (signs) this information.
Certificate chain	A hierarchy of files that adds a layer of security to the certificates. Typically, the chain includes one root certificate at the top of the hierarchy, one or more intermediate certificates, and the server certificates that identify the entities.
Client certificate	For security key management, a client certificate validates the storage array’s controllers, so the key management server can trust their IP addresses.
Intermediate certificate	One or more intermediate certificates branch off from the root in the certificate chain. The CA issues one or more intermediate certificates to act as middlemen between a protected root and server certificates.
Key management server certificate	For security key management, a key management server certificate validates the server, so the storage array can trust its IP address.

Term	Description
Keystore	A keystore is a repository on your host management system that contains private keys, along with their corresponding public keys and certificates. These keys and certificates identify your own entities, such as the controllers.
OCSP server	The Online Certificate Status Protocol (OCSP) server determines if the certificate authority (CA) has revoked any certificates before their scheduled expiration date, and then blocks the user from accessing a server if the certificate is revoked.
Root certificate	The root certificate is at the top of the hierarchy in the certificate chain, and 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.
Signed certificate	A certificate that is validated by a certificate authority (CA). This data file contains a private key and ensures that data is sent in encrypted form between a server and a client over an HTTPS connection. In addition, a signed certificate includes details about the owner of the entity (typically, a server or website) and a digital signature composed of letters and numbers. A signed certificate uses a chain of trust, and therefore is most often used in production environments. Also referred to as a "CA-signed certificate" or a "management certificate."
Self-signed certificate	A self-signed certificate is validated by the owner of the entity. This data file contains a private key and ensures that data is sent in encrypted form between a server and a client over an HTTPS connection. It also includes a digital signature composed of letters and numbers. A self-signed certificate does not use the same chain of trust as a CA-signed certificate, and therefore is most often used in test environments. Also referred to as a "preinstalled" certificate.
Server certificate	The server certificate is at the bottom of the certificate chain. It identifies your specific entity, such as a website or other device. Each controller in a storage system requires a separate server certificate.

How tos

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.

About this task

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

Step 1: Complete and submit a CSR for the controllers

You must first generate a certificate signing request (CSR) file for each controller in the storage array, and then submit the file(s) to a certificate authority (CA).

Before you begin

- You must know the IP address or DNS name of each controller.

About this task

The CSR provides information about your organization, the IP address or DNS name of the controller, and a key pair that identifies the web server in the controller. During this task, one CSR file is generated if there is only one controller in the storage array and two CSR files if there are two controllers.

> Do not generate a new CSR after submission to the CA. When 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 keystore. When you receive the signed certificates and import them into the keystore, the system ensures that both the private and public keys are the original pair. Therefore, you must not generate a new CSR after submitting one to the CA. If you do, the controllers generate new keys, and the certificates you receive from the CA will not work.

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.
   - **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. 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. Locate the downloaded CSR file(s). The folder location depends on your browser.
7. Submit the CSR file(s) to a CA and request signed certificates in PEM format.
8. Wait for the CA to return the certificates, and then go to Step 2: Import signed certificates for controllers.

Step 2: Import signed certificates for controllers

After you receive signed certificates, you import the files for the controllers.

Before you begin

- The CA returned signed certificate files.
- The files are available on your local system.
- If the CA provided a chained certificate (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**). When the exports are complete, a CER file is shown for each certificate file in the chain.

About this task

This task describes how to upload the certificate files.

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 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.

   The file names are displayed in the dialog box.

4. Click **Import**.

   The file(s) are uploaded and validated.

Results

The session is automatically terminated. You must log in again for the certificate(s) to take effect. When you log in again, the new CA-signed certificate is 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).
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.

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

This task describes how to generate the CSR file, which you will then use to request a signed client certificate from a CA that is trusted by the key management server. A client certificate validates the storage array's controllers, so the key management server can trust their Key Management Interoperability Protocol (KMIP) requests. During this task, you must provide information about your organization.

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.

Before you begin

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

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

About this task

This task describes how to upload certificate files for authentication between the storage array controllers and the key management server. You must load both the client certificate file for the controllers and the server certificate file for the 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.

   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**.

FAQs

Why does the Cannot Access Other Controller dialog box appear?

When you perform certain operations related to CA certificates (for example, importing a certificate), you might see a dialog box prompting you to accept a self-signed certificate for the second controller.

In storage arrays with two controllers (duplex configurations), this dialog box sometimes appears if SANtricity System Manager cannot communicate with the second controller or if your browser cannot accept the certificate during a certain point in an operation.

If this dialog box opens, click **Accept Self-Signed Certificate** to proceed. If another dialog box prompts you for a password, enter your Administrator password used for accessing System Manager.

If this dialog box appears again and you cannot complete a certificate task, try one of the following procedures:

- Use a different browser type to access this controller, accept the certificate, and continue.
- Access the second controller withSystem Manager, accept the self-signed certificate, and then return to the first controller and continue.

How do I know what certificates need to be uploaded to System Manager for external key management?

For external key management, you import two types of certificates for authentication between the storage array and the key management server so the two entities can trust each other.

A client certificate validates the storage array's controllers, so the key management server can trust their Key Management Interoperability Protocol (KMIP) requests. To obtain a client certificate, you use System Manager to complete a CSR for the storage array. You can then upload the CSR to a key management server and generate a client certificate from there. Once you have a client certificate, 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. Retrieve the server certificate file from the key management server, and then copy that file to the host where you are accessing System Manager.

What do I need to know about certificate revocation checking?

System Manager allows you to check for revoked certificates by using an Online Certificate Status Protocol (OCSP) server, instead of uploading Certificate Revocation Lists (CRLs).

Revoked certificates should no longer be trusted. A certificate might be revoked for several reasons; for example, if the Certificate Authority (CA) improperly issued the certificate, a private key was compromised, or the identified entity did not adhere to policy requirements.

After you establish a connection to an OCSP server in System Manager, the storage array performs revocation checking whenever it connects to an AutoSupport server, External Key Management Server (EKMS), Lightweight Directory Access Protocol over SSL (LDAPS) server, or a Syslog server. The storage array attempts to validate these servers' certificates to ensure that they have not been revoked. The server then returns a value of "good," "revoked," or "unknown" for that certificate. If the certificate is revoked or the array cannot contact the OCSP server, the connection is refused.

Specifying an OCSP responder address in System Manager or in the command line interface (CLI) overrides the OCSP address found in the certificate file.

What types of servers will revocation checking be enabled for?

The storage array performs revocation checking whenever it connects to an AutoSupport server, External Key Management Server (EKMS), Lightweight Directory Access Protocol over SSL (LDAPS) server, or a Syslog server.

Copyright information

Trademark information