# Certificates

SANtricity 11.5

NetApp
October 22, 2024

# Table of Contents

# Certificates

## Concepts

### How CA certificates work

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.

When you open a browser and try connecting to System Manager through the controller management port, the browser attempts to verify that the storage array's controller is a trusted source. If the browser cannot locate a digital certificate for the controller, it alerts you that the certificate is not signed by a recognized authority and asks if you want to continue. If you no longer want to see this alert, you must get a signed, digital certificate from a CA.

If you are using an external key management server with the Drive Security feature, you can also create certificates for authentication between that server and the controllers or you can accept the self-signed certificate(s) from the storage array.

The following steps are required for using a digital certificate from a trusted authority:

1. Go to **Settings › Certificates**. Your user login must include Security Admin permissions; otherwise, **Certificates** does not appear on the page.
2. Create a Certificate Signing Request (CSR) for each controller or for a key management server.
3. Send the .CSR file(s) to a CA, and then wait for them to send you the certificates.
4. Import the trusted (intermediate and root) certificate from the CA. These certificates establish a point of trust for a CA hierarchy.
5. Import the signed, management certificates for each controller or the key management server.

### Certificate terminology

Learn how the certificate terms apply to your storage array.

| 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. |

| Term | Description |
| --- | --- |
| 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. |
| 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. |
| 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. |
| Management certificate | A management certificate is approved by a certificate authority (CA) and allows secure access to the web application. Also referred to as a "signed certificate." |
| 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. |
| Self-signed certificate | A self-signed certificate is pre-loaded on the controller. If the site connection is self-signed, a warning message opens before you can proceed to the web application. |
| Trusted certificate | A trusted certificate from a certificate authority (CA) is a known certificate at the top of the certificate hierarchy. Also referred to as a "root certificate." |

# How tos

## Complete a CA certificate signing request (CSR) for the controllers

To receive a certificate authority (CA) certificate for the storage array's controllers, you must first generate a certificate signing request (CSR) file for each controller in 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.

**About this task**

This task describes how to generate the .CSR files (certificate signing requests) that you send to a CA to

receive signed, management certificates for the controllers. You must provide information about your organization, plus the IP address or DNS name of the controller(s). 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.

**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. Send the .CSR file(s) to your CA.

**After you finish**

When you receive the digital certificates, import the appropriate certificate files that the CA sent to you.

## Import trusted certificates for controllers

After receiving digital certificates from a certificate authority (CA), you can import the certificate chain (intermediate and root) for the controllers.

**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 generated a certificate signing request (.CSR file) and sent it to the CA.
- The CA returned trusted certificate files.
- The certificate files are installed on your local system.

**About this task**

This task describes how to upload the trusted certificates for the storage array's controllers.

**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.

**After you finish**

Import the management certificate.

## Import a management certificate for controllers

After importing the trusted certificate chain, you import a management (signed) certificate file for each controller in 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.
- The trusted certificates have been imported.

- The CA returned a management certificate file for each controller.
- The management certificate file(s) are available on your local system.

**About this task**

This task describes how to upload the management certificate files for controller authentication.

**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 **Browse** to select the file for controller A. If there are two controllers, click the second **Browse** button to select the file for controller B.

   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.

## View imported certificate information

From the Certificates page, you can view the certificate type, issuing authority, and the valid date range of certificates you previously imported.

**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 view information for user-installed or pre-installed certificates.

**Steps**

1. Select **Settings › Certificates**.
2. Select one of the tabs to view information about management certificates for the controllers, trusted certificates, and certificates for a key management server.

| Tab | Description |
| --- | --- |
| Array Management | View information about all the server certificates imported for the controllers. |

| Tab | Description |
| --- | --- |
| Trusted | View information about all the trusted (root) certificates imported for the controllers. Use the filter field under **Show certificates that are…** to view either user-installed or pre-installed certificates.<br>• **User-installed**. Certificates that a user uploaded to the storage array (includes trusted certificates, LDAPS certificates, and Identity Federation certificates).<br>• **Pre-installed**. Certificates included with the storage array. |
| Key Management | View information about all the management (signed) certificates imported for an external key management server. |

## Delete trusted certificates

You can delete any of the user-imported certificates.

**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 the system if you delete a certificate used to authenticate the storage array's management certificates or LDAP server before you import a replacement certificate.

**About this task**

This task describes how to delete user-imported certificates. Predefined 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**.

## Reset management certificates

You can revert the management certificates on the storage array back to the factory self-signed state.

**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.

**About this task**

Resetting the management certificates on the storage array deletes the current management certificates from each of the controllers. After the certificates are reset, the controllers 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 click **Reset**.

**Results**

After your browser refreshes, 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.

## Complete CA certificate signing request (CSR) for a key server

To receive a certificate authority (CA) certificate for a key management server, you must first generate a certificate signing request (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 files (certificate signing requests) that you send to a CA to receive signed certificates for a key management server. 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. Send the .CSR file(s) to your CA.

**After you finish**

When you obtain the client and server certificates from the key management server, import them for authentication with the storage array controllers.

## Import key management server certificates

For external key management, you import certificates for authentication between the storage array and the key management server so the two entities can trust each other. There are two types of certificates: the client certificate validates the 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.
- A client certificate is available for the storage array.

  A client certificate validates the storage array's controllers, so the key management server can trust their IP addresses. To obtain a client certificate, you must complete a CSR for the storage array and then upload it to the key management server. From the server, generate a client certificate.

- The key management server certificate is available.

  A key management server certificate validates the server, so the storage array can trust its IP address. To obtain a key management server certificate, you must generate it from the 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.

**Steps**

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

   A dialog box opens for importing the certificate files.

3. Click the **Browse** buttons to select the files.

   The file names display in the dialog box.

4. Click **Import**.

   The file(s) 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**.

## 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. Automatic revocation checking is helpful in cases where the Certificate Authority (CA) improperly issued a certificate or if a private key is compromised.

**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**

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**.

**Result**

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

# 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 with System 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, 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 IP addresses. To obtain a client certificate, you must complete a CSR for the storage array and then upload it to the key management server. From the server, generate a client certificate, and then use System Manager to import it.

A key management server certificate validates the key management server, so the storage array can trust its IP address. To obtain a key management server certificate, you must generate it from the key management server.

## 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