Technical Report

Managing certificates for NetApp E-Series storage systems

Jolie Gallagher and Jason Hennessy, NetApp

March 2022 | TR-4813

Abstract

This document describes how to manage security certificates with the latest NetApp® E-Series controllers and applications.

TABLE OF CONTENTS

LIST OF TABLES

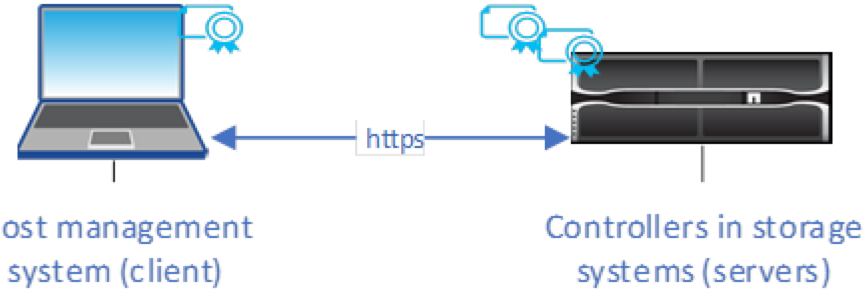
LIST OF FIGURES

Overview of certificate management

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.

In networks with NetApp® E-Series storage systems, 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).

Figure 1) Certificates used in clients and servers.


https
Host management system (client)
Controllers in storage systems (servers)

Document scope

This document describes how to manage certificates with the following NetApp SANtricity® versions and controller models:

- SANtricity applications:
  - System Manager, OS version 11.40 or later
  - Web Services Proxy and Unified Manager, version 3.0 or later
- Controller models:
  - EF280 and E2800 storage systems
  - EF570 and E5700 storage systems
  - EF300 and EF600 storage systems

Note: This document does not describe older SANtricity versions, older controller models, or other types of SANtricity management applications, such as CLI and API. Also, it does not describe configuring certificates with mirroring operations. For detailed information about certificate management with these other products and methods, see TR-4712 - NetApp SANtricity Management Security.

Certificate basics

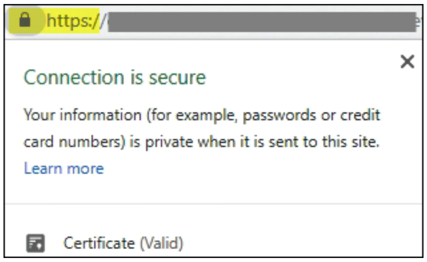
A certificate can be signed by a trusted authority, or it can be self-signed. Signing simply means that someone validated the owner's identity and determined that their devices can be trusted.

What are 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. Essentially, signed certificates act like ID cards; they validate that the owners are whom they claim to be.

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, similar to the following example.

Figure 2) Example of a website with a signed certificate.



https://[redacted]

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

Learn more

Certificate (Valid)

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.

What is a certificate authority?

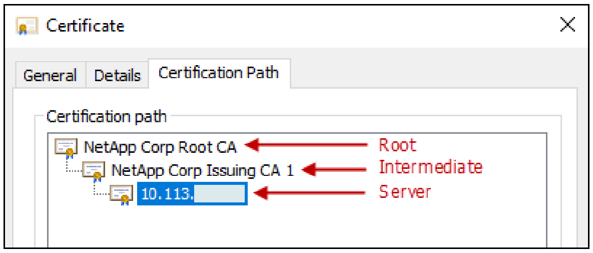
A certificate authority (CA) is a trusted third-party organization, such as Verisign or DigiCert, that issues digital certificates for websites and other devices. To become an issuing authority, a CA must meet strict criteria to be trusted by major browsers, operating systems, and mobile devices. You can find a list of authorized CAs on the internet, from private companies to government agencies.

When you apply for a digital certificate, the CA takes steps to verify your identity. In this process, the CA might send an email to your registered business, verify your business address, and perform an HTTP or DNS verification. Similar to organizations that issue valid IDs, such as a drivers' license bureau, a CA verifies the identity of an entity that wants to operate on the internet.

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 E-Series storage system requires a separate server certificate.

Figure 3) Example of a certificate chain.



NetApp Corp Root CA ← Root

NetApp Corp Issuing CA 1 ← Intermediate

10.113.[redacted] ← Server

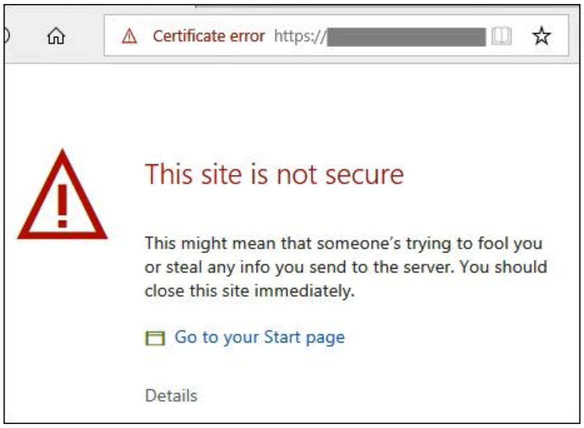
A certificate chain helps minimize damage if a security event occurs. The CA can revoke the intermediate files so that all their associated signed certificates are also revoked. This action is necessary because the chain can no longer be trusted.

What are self-signed certificates?

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. In the following example, you must click Details to access a link that allows you to proceed to the website; by doing so, you are essentially accepting the self-signed certificate.

Figure 4) Example of a website without a signed certificate.



Certificate error https://[redacted]

This site is not secure

This might mean that someone’s trying to fool you or steal any info you send to the server. You should close this site immediately.

Go to your Start page

Details

Which should you use: CA-signed or self-signed certificates?

The type of certificate that is best for your environment depends on your security requirements and budget.

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.

Table 1) Differences between certificate types.

Type	Advantages and disadvantages
CA-signed	• Validated by a trusted third party • Provides better security • Can be expensive • Best used in production environments
Self-signed	• Validated by your own organization • Provides limited security • Free • Best used in test environments

Certificate terminology

Table 2 defines terms used in this document.

Table 2) Certificate terms.

Term	Definition
Certificate	A digital file that identifies the owner of a website or network device for security purposes.
Certificate authority (CA)	A trusted third-party organization, such as Verisign or DigiCert, that manages and issues digital certificates.
Certificate chain (root, intermediate, server)	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.
Certificate signing request (CSR)	A data file that you send to a CA to request certificates for your devices. The CSR includes your organization's details, as well as IPs or DNS names of the devices. When you create the CSR from a SANtricity application, a self-signed certificate is generated to be used until the signed certificate is returned from the CA. In addition, a private key is generated and used to encrypt the data. The certificate itself has a subject ID (also called a distinguished name), which identifies the device or entity.
Keystore, truststore	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 E-Series controllers. A truststore is a repository that contains certificates from trusted third parties, such as CAs. Essentially, a keystore is used to store your own credentials (server or client), and a truststore is used to store credentials from other trusted sources.
Preinstalled certificate	A term used in SANtricity applications to refer to the self-signed certificate that is shipped with a controller.
Self-signed certificate	A certificate that 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.
Signed certificate	A certificate that is validated by a 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.
User-installed certificate	A term used in SANtricity applications to refer to either the CA-signed certificate stored on a controller or the certificates that you have imported into the truststore.

How certificates work with E-Series systems

The latest models of NetApp E-Series storage systems 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.

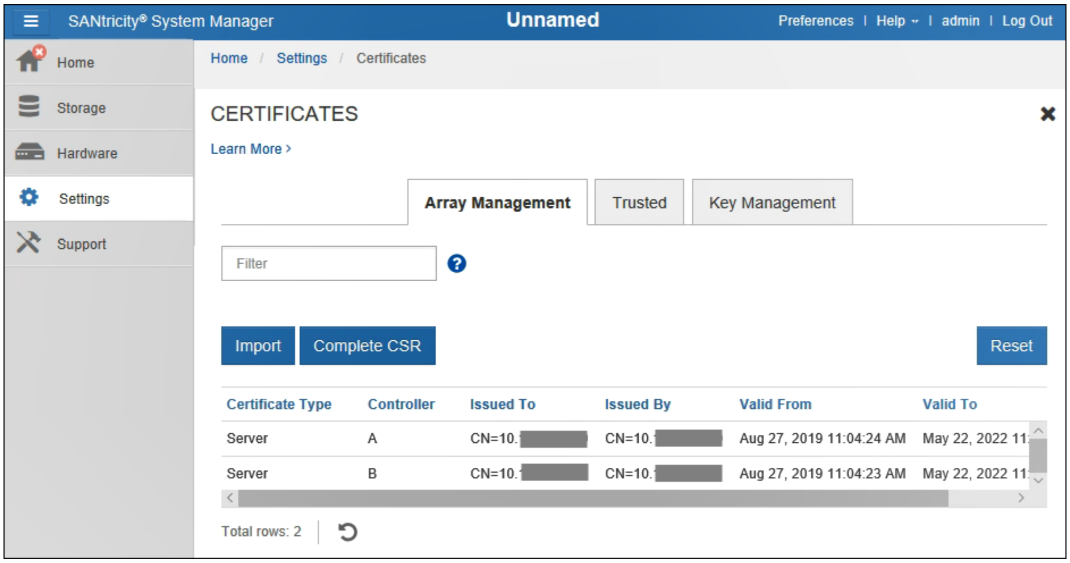
To manage certificates, use the following SANtricity applications:

- **System Manager for a single controller.** System Manager is a storage-provisioning application that is included with the controller's operating system. To use System Manager, you open a browser from a host connected to the controller's management port and then enter the controller's IP address or domain name. From its web interface, you can manage one of the two controllers in the storage system, generate CSRs, and import CA-signed certificates for the controllers.

- **Unified Manager for multiple controllers.** Unified Manager is part of a web service proxy that is installed separately on a networked Windows or Linux host. To use Unified Manager, you open a browser from the host and then enter the URL for Unified Manager. From its web interface, you can manage all discovered arrays in the network. However, you must use System Manager to import CA-signed certificates for the individual controllers.

  Note: If you plan to use other methods for managing controllers and certificates, such as CLI commands or API commands, see TR-4712 - NetApp SANtricity Management Security.

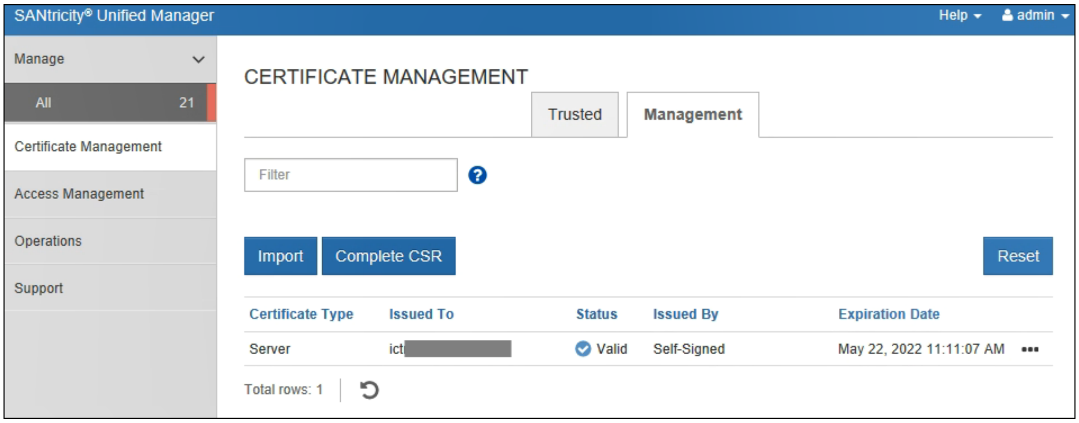
Figure 5) System Manager application interface.



Certificate Type	Controller	Issued To	Issued By	Valid From	Valid To
Server	A	CN=10.[redacted]	CN=10.[redacted]	Aug 27, 2019 11:04:24 AM	May 22, 2022 11:
Server	B	CN=10.[redacted]	CN=10.[redacted]	Aug 27, 2019 11:04:23 AM	May 22, 2022 11:

Total rows: 2

Figure 6) Unified Manager application interface.



Certificate Type	Issued To	Status	Issued By	Expiration Date
Server	ict[redacted]	✓ Valid	Self-Signed	May 22, 2022 11:11:07 AM •••

Total rows: 1

Certificate standards and requirements

Table 3 describes important information about certificates used in E-Series systems.

Table 3) Certificate standards and requirements.

Item	Description
Format standard	The format for certificates is specified by the International Telecommunications Union's Standardization (ITU-T) X.509 international standard.
Encoding format	E-Series systems require PEM (Base64 ASCII encoding) format, which includes the following certificate file types: .pem, .crt, .cer, or .key.

Certificate management in System Manager

System Manager is the storage-provisioning application included with the controller’s operating system. With System Manager, you have two options for managing certificates between the controllers and the host management system:

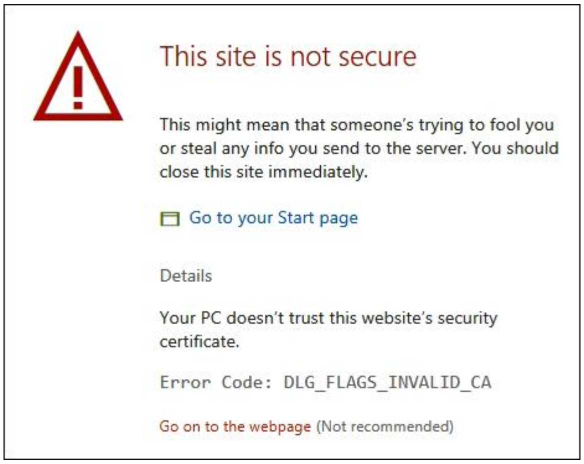
- Continue to accept self-signed certificates for the controllers.
- Obtain CA-signed certificates for the controllers.

Using self-signed certificates in System Manager

Because E-Series controllers include self-signed certificates, the browser used to access System Manager does not trust the controllers and therefore displays warning messages that the connection is not secure.

Trusting the controller connection at login

To access System Manager, you open a browser from a host connected to the controller’s management port and then enter the controller’s IP address or domain name. Before the browser displays the System Manager login screen, it determines whether the controller is a trusted source. If the browser does not locate a CA-signed certificate for the controller, it opens a warning message similar to the following example. From there, you can continue to the website. By continuing, you are accepting the controller’s self-signed certificate for that session.



This site is not secure

This might mean that someone’s trying to fool you or steal any info you send to the server. You should close this site immediately.

Go to your Start page

Details

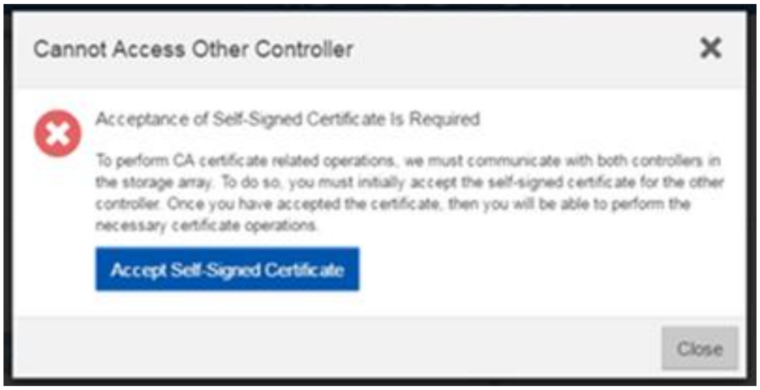
Your PC doesn’t trust this website’s security certificate.

Error Code: DLG_FLAGS_INVALID_CA

Go on to the webpage (Not recommended)

Trusting dual controllers during sessions (older systems)

For some older E-series models with two controllers (a duplex configuration), a dialog box might appear if System Manager attempts to communicate with the second controller or if your browser cannot accept the certificate at a certain point in an operation. If a dialog box similar to the one shown below opens, click Accept Self-Signed Certificate to proceed.



Cannot Access Other Controller

Acceptance of Self-Signed Certificate Is Required

To perform CA certificate related operations, we must communicate with both controllers in the storage array. To do so, you must initially accept the self-signed certificate for the other controller. Once you have accepted the certificate, then you will be able to perform the necessary certificate operations.

Using CA-signed certificates for the controllers

To obtain CA-signed certificates for secure communications between the controller (acting as the server) and the browser used for System Manager (acting as the client), follow this workflow:

1. **Generate CSR files.** Using System Manager, create a certificate signing request (CSR) for each controller in the storage system.
2. **Submit the CSR files to a CA.** Download and send the CSR files to a CA, then wait for the certificates to be returned.
3. **Unpack the certificate chain** (if necessary). When the CA delivers the certificates, you might need to unpack the chain into three or more separate files: root, intermediate, and server certificates.
4. **Import CA-signed certificates.** Using System Manager, import the certificate files from the CA.

Step 1: Generate the CSR

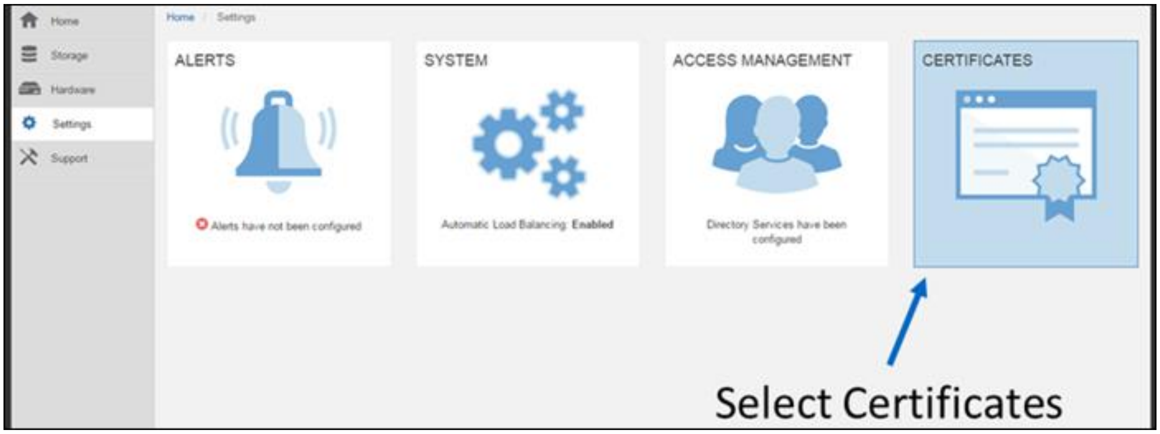
The CSR provides information about your organization, the IP address or DNS name of the controller, and a key pair that identifies the web server in the controller.

Note: **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.

This task describes how to generate a CSR file from System Manager. Alternatively, you can generate a CSR file using a tool such as OpenSSL and can skip to Step 2.

To create a CSR file for one or both controllers using System Manager, follow these steps:

1. Log in to System Manager: Open a browser and enter either the IP address of the controller or the domain name and port number (defaults to 8443) of the controller; for example, `https://<domainname>:8443`.
2. Enter your user name and password. You must log in with a user profile that includes Security admin permissions. Otherwise, certificate functions do not appear.
3. Select Settings > Certificates.



Alerts have not been configured

Automatic Load Balancing: Enabled

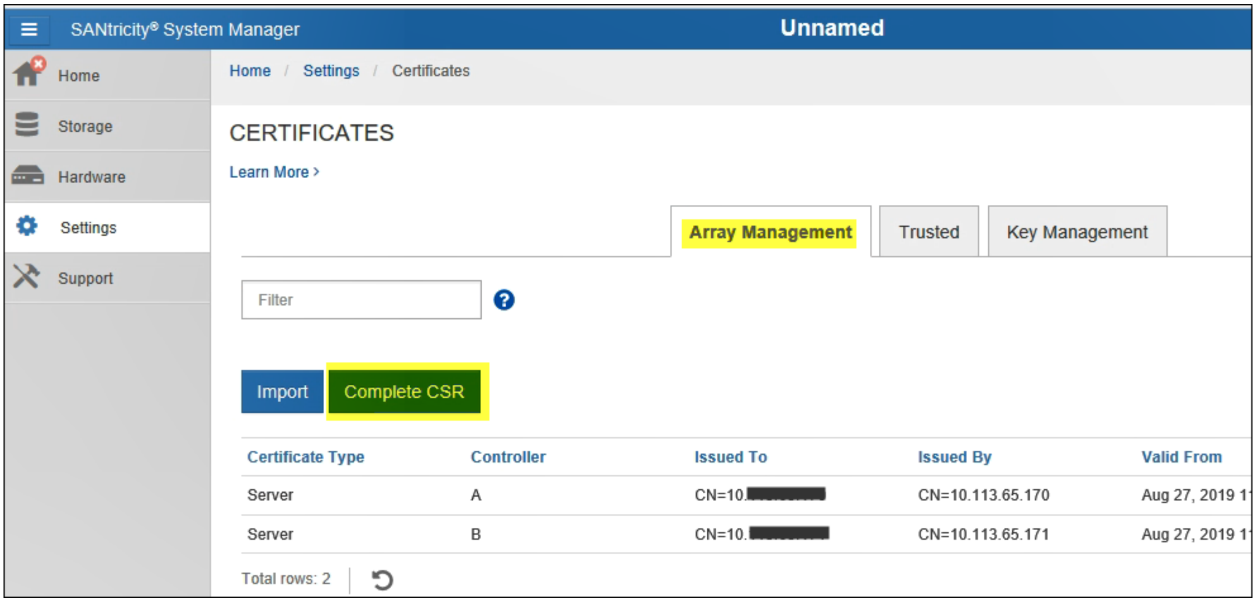
Directory Services have been configured

Select Certificates

4. If a dialog box prompts you to accept a self-signed certificate for the second controller, click Accept Self-Signed Certificate to proceed.
5. Make sure that the Array Management tab is selected.

   Note: (Optional) After you install and configure the storage system, you can select Reset to regenerate the controller's self-signed certificates. This command restarts the process in a clean state following the storage system installation.

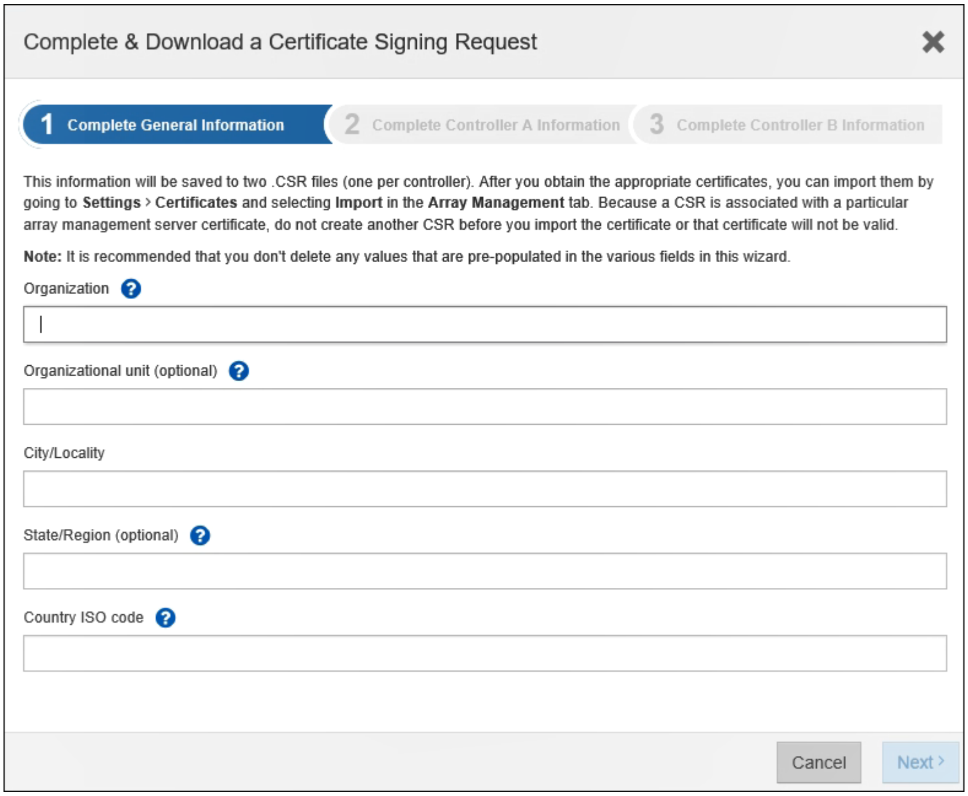
6. Click Complete CSR.



Certificate Type	Controller	Issued To	Issued By	Valid From
Server	A	CN=10.[redacted]	CN=10.113.65.170	Aug 27, 2019 1
Server	B	CN=10.[redacted]	CN=10.113.65.171	Aug 27, 2019 1

Total rows: 2

7. In the first dialog box, enter your organization's information and location.



Complete & Download a Certificate Signing Request

✖
1 Complete General Information
2 Complete Controller A Information
3 Complete Controller B Information

This information will be saved to two .CSR files (one per controller). After you obtain the appropriate certificates, you can import them by going to **Settings** › **Certificates** and selecting **Import** in the **Array Management** tab. Because a CSR is associated with a particular array management server certificate, do not create another CSR before you import the certificate or that certificate will not be valid.

Note: It is recommended that you don't delete any values that are pre-populated in the various fields in this wizard.

Organization

Organizational unit (optional)

City/Locality

State/Region (optional)

Country ISO code

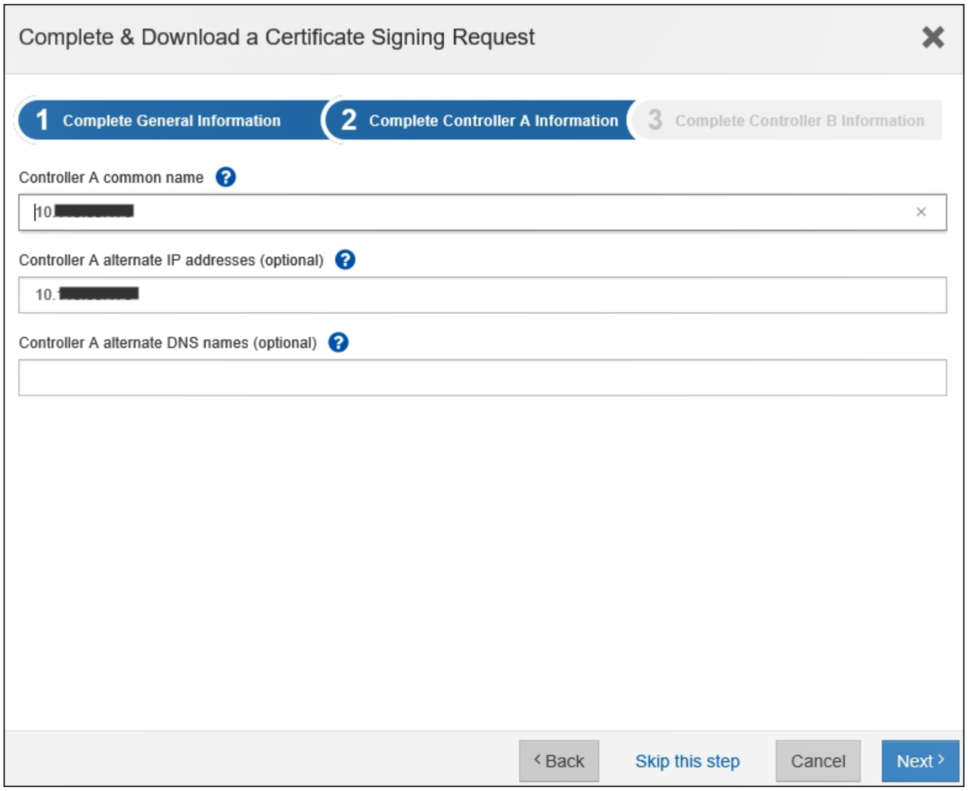
8. Click Next to display the dialog box for the first controller (controller A).

   Do not change prepopulated values unless the ones displayed are incorrect. If you are using a DNS server, you can determine the address by running the `nslookup` command from a server command prompt in the array's management network, as shown in the following example:

```
C:\Users\admin>nslookup 192.13.85.213
Server:  DNS1.location.group.company.com
Address:  192.11.102.130

Name:    ICTM0904C1-A.group.company.com
Address:  192.13.85.213


C:\Users\admin>nslookup 192.13.85.214
Server:  DNS1.location.group.company.com
Address:  192.11.102.130

Name:    ICTM0904C1-B.group.company.com
Address:  192.13.85.214
```

9. For controller A, verify that the prepopulated values are correct or enter the correct information.
   - **Controller A common name.** The IP address or DNS name of controller A is displayed by default. NetApp recommends that you enter the fully qualified domain name (FQDN); for example, `name.domain.com`. Make sure that this address is correct; it must match exactly what you enter to access System Manager in the browser. Do not include http:// or https://. The DNS name is restricted to 63 characters, must start and end with a letter or digit, and can include only letters, digits, and a hyphen for the interior characters. The DNS name cannot begin with a wildcard.
   - **Controller A alternate IP addresses.** (Optional) You can list any alternate IP addresses or aliases for controller A. For multiple entries, use a comma-delimited format.

- **Controller A alternate DNS names.** If you entered an FQDN in the first field, copy that name here. In addition, you can list any alternate FQDNs of the controller. For multiple entries, use a comma-delimited format. The DNS name cannot begin with a wildcard.



Complete & Download a Certificate Signing Request

✖
1 Complete General Information
2 Complete Controller A Information
3 Complete Controller B Information

Controller A common name

10[redacted]

Controller A alternate IP addresses (optional)

10.[redacted]

Controller A alternate DNS names (optional)

‹ Back
Skip this step
Cancel
Next ›

10. Double-check the controller information to make sure that the addresses are correct. If they are not, the certificates returned from the CA will fail when you try to import them.

    If the storage system has only one controller, the Finish button is available. If the storage system has two controllers, the Next button is available.

    Note: 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.

11. If there is only one controller, click Finish. If there are two controllers, click Next to enter information for controller B (same as the previous dialog box), and then click Finish.

Step 2: Submit the CSR files

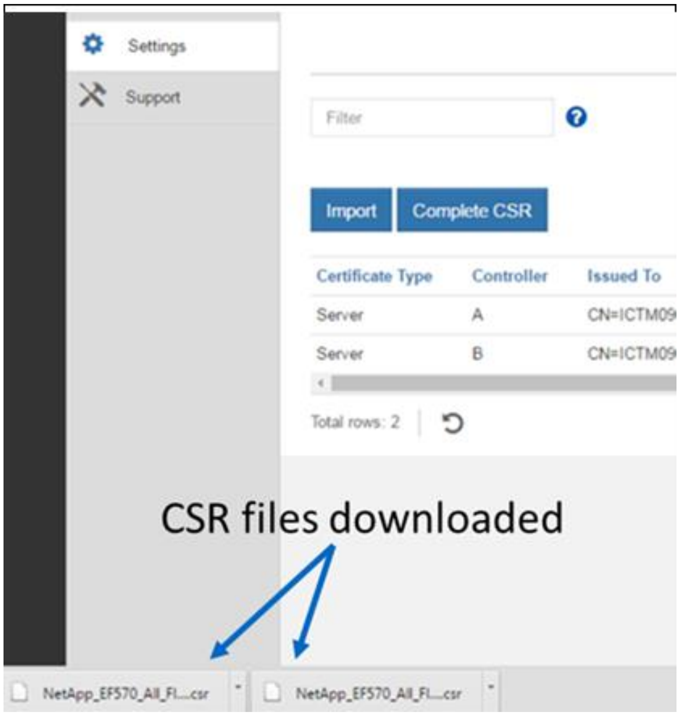
To submit the CSR files to a CA, follow these steps:

1. Locate the downloaded CSR files.

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

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

3. Wait for the CA to return the certificates.



Certificate Type	Controller	Issued To
Server	A	CN=ICTM09
Server	B	CN=ICTM09

Total rows: 2

CSR files downloaded

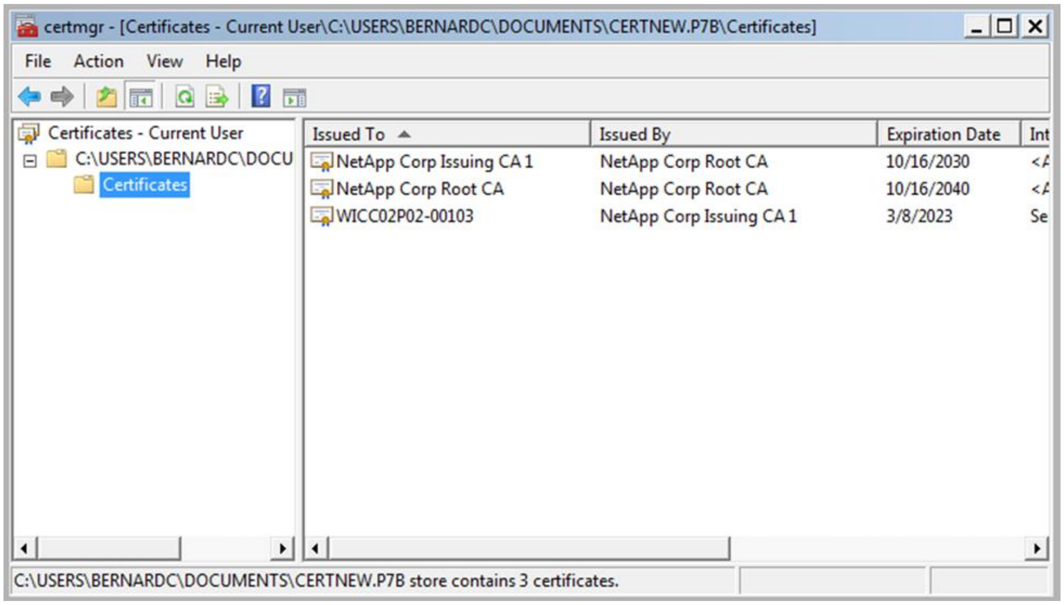
NetApp_EF570_All_Fl....csr

NetApp_EF570_All_Fl....csr

Step 3: Unpack the certificate chain

If the CA provides a chained certificate instead of individual certificates, follow these steps to break up the certificate chain:

1. Using the Windows `certmgr` utility, double-click the `.p7b – PKCS #7` certificate file (Windows recognizes the file type).
2. In the Windows Cert Manager, expand the Certificates tree to display the certificates in the right pane.

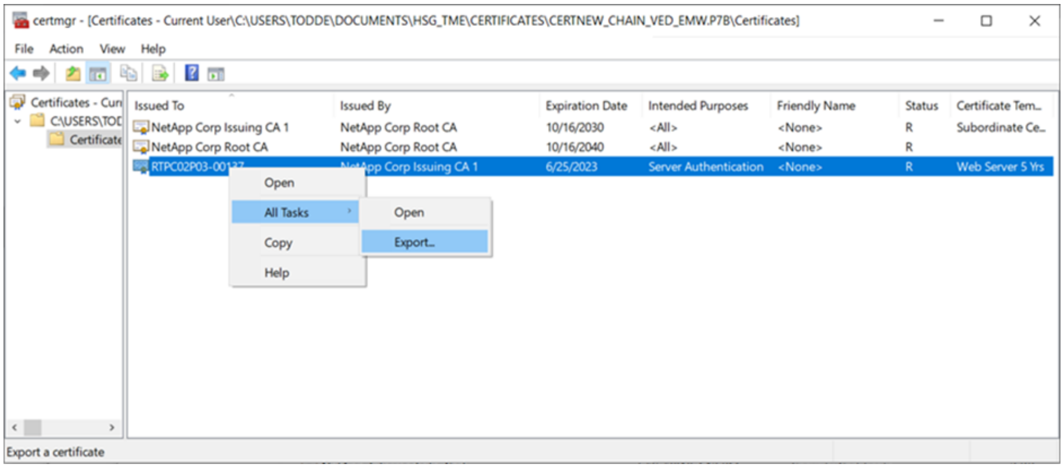


certmgr - [Certificates - Current User\C:\USERS\BERNARDC\DOCUMENTS\CERTNEW.P7B\Certificates]

Issued To	Issued By	Expiration Date	Int
NetApp Corp Issuing CA 1	NetApp Corp Root CA	10/16/2030	<A
NetApp Corp Root CA	NetApp Corp Root CA	10/16/2040	<A
WICC02P02-00103	NetApp Corp Issuing CA 1	3/8/2023	Se

C:\USERS\BERNARDC\DOCUMENTS\CERTNEW.P7B store contains 3 certificates.

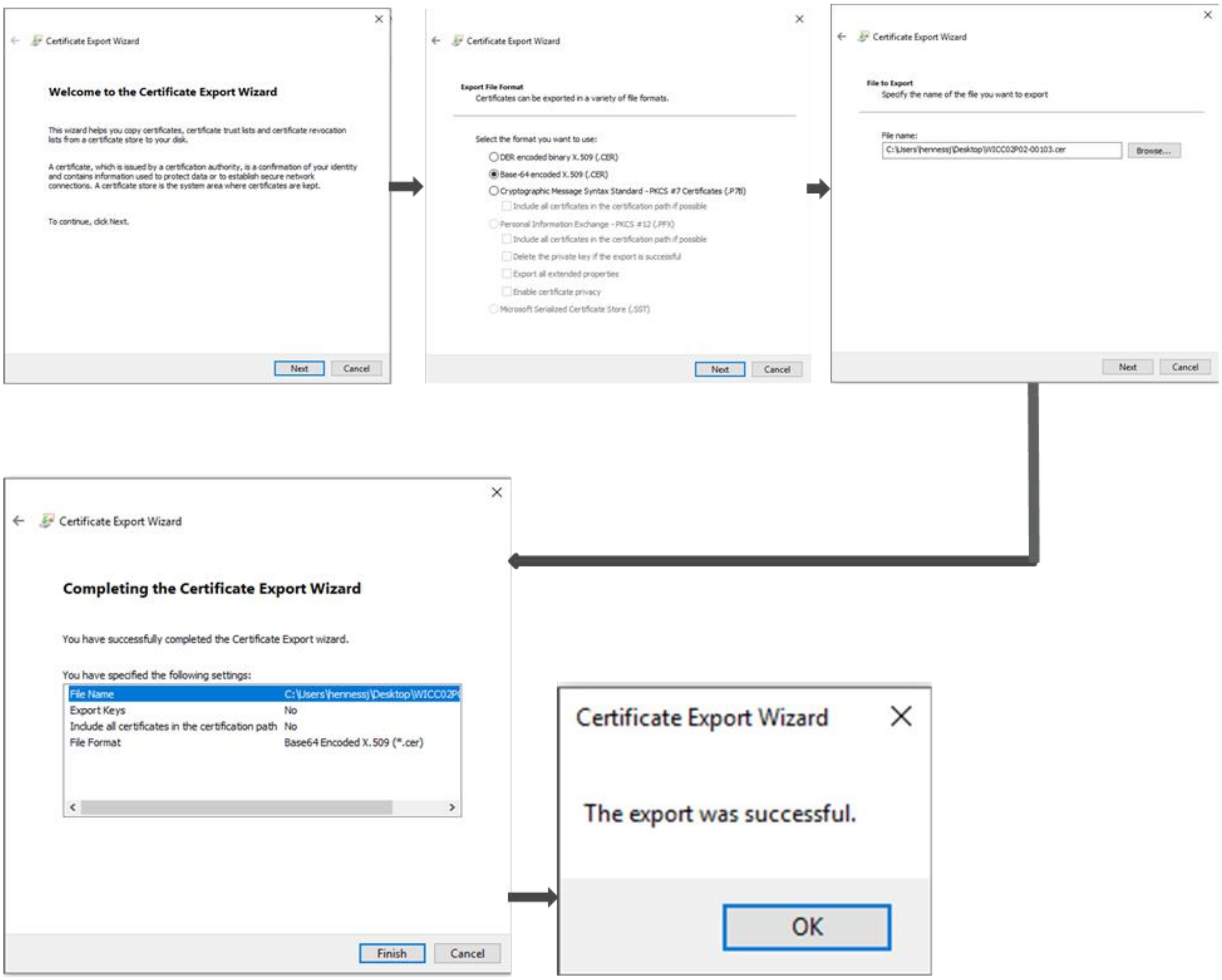
3. For each certificate, right-click and select All Tasks > Export.


certmgr - [Certificates - Current User\C:\USERS\TODDE\DOCUMENTS\HSG_TME\CERTIFICATES\CERTNEW_CHAIN_VED_EMW.P7B\Certificates]
File
Action
View
Help
Certificates - Curr
C:\USERS\TOD
Certificate
Open
All Tasks
Copy
Help
Open
Export...
Export a certificate

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
NetApp Corp Issuing CA 1	NetApp Corp Root CA	10/16/2030	<All>	<None>	R	Subordinate Ce...
NetApp Corp Root CA	NetApp Corp Root CA	10/16/2040	<All>	<None>	R	
RTPC02P03-00127	NetApp Corp Issuing CA 1	6/25/2023	Server Authentication	<None>	R	Web Server 5 Yrs

4. Follow the wizard to export each certificate in the chain to a local directory on the host where you generated the CSR.

   Note: Be sure to select the desired certificate file type. NetApp recommends Base-64 Encoded format, which makes it easy to validate keys by using common decoder software.



Certificate Export Wizard

Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)
● Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Delete the private key if the export is successful
□ Export all extended properties
□ Enable certificate privacy
○ Microsoft Serialized Certificate Store (.SST)

Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name: C:\Users\hennessj\Desktop\WICC02P02-00103.cer

Certificate Export Wizard

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\hennessj\Desktop\WICC02P
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)

Certificate Export Wizard

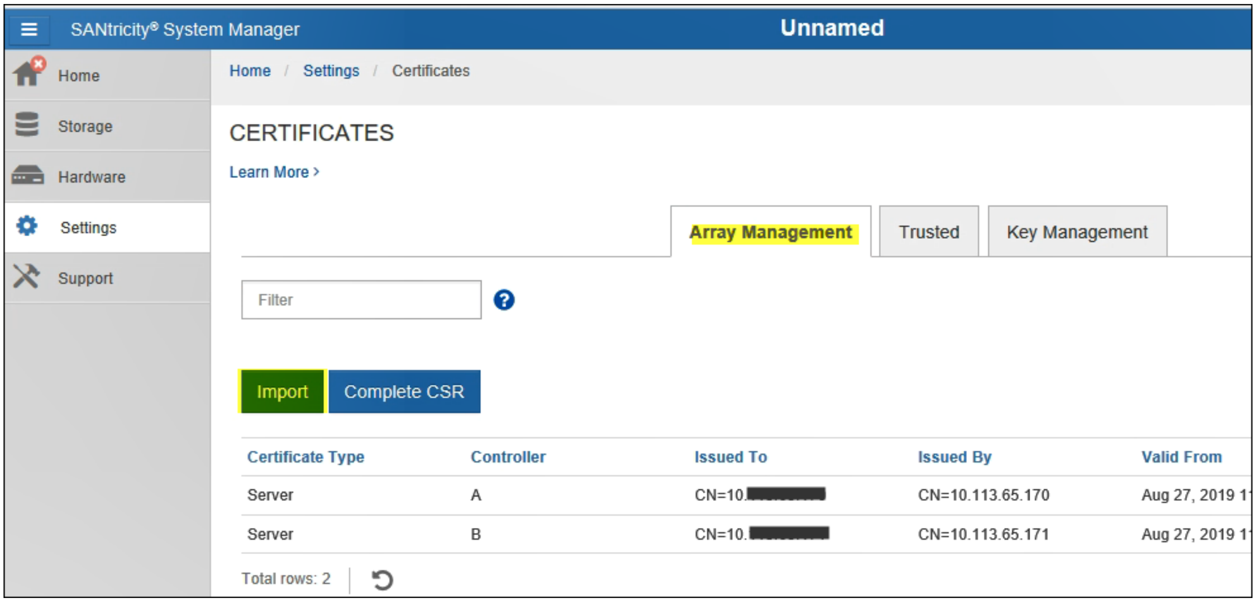
The export was successful.

When the exports are complete, a CER file is shown for each certificate file in the chain.

Step 4: Import CA-signed certificates for the controllers

To import the certificates, follow these steps:

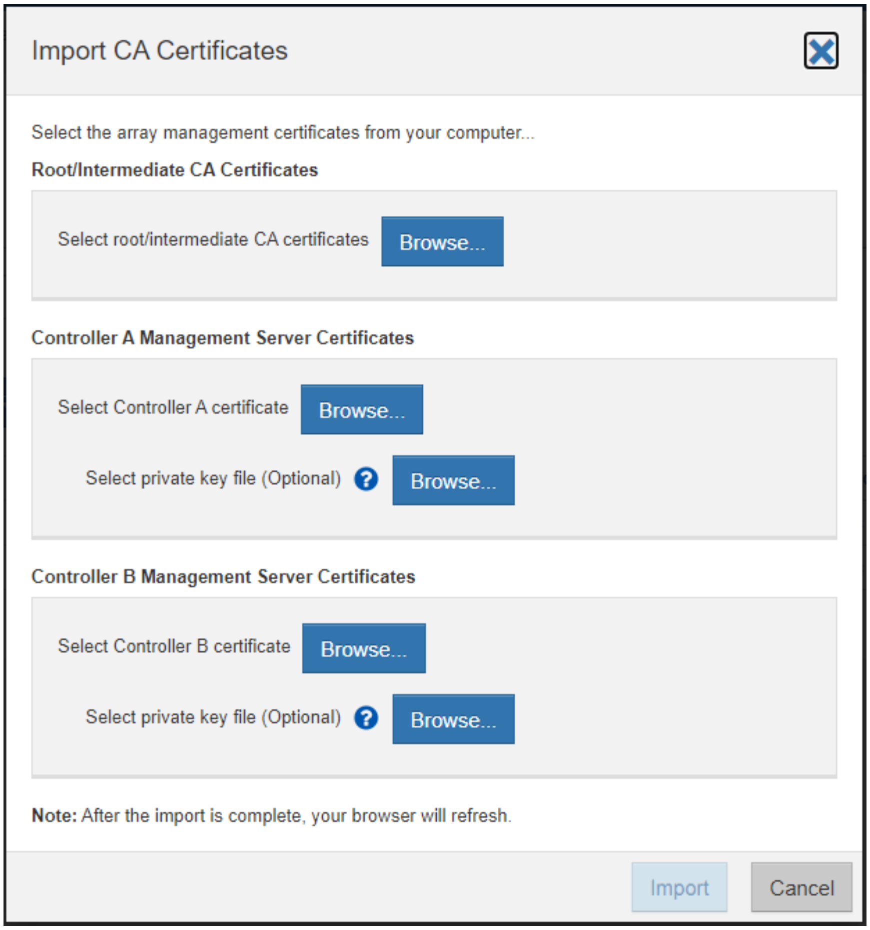
1. Load the certificate files on the host system that is connected to the controllers.
2. Log in to System Manager. You must log in with a user profile that includes Security admin permissions. Otherwise, certificate functions do not appear.
3. Select Settings > Certificates.
4. From the Array Management tab, click Import.



Certificate Type	Controller	Issued To	Issued By	Valid From
Server	A	CN=10.[redacted]	CN=10.113.65.170	Aug 27, 2019 1
Server	B	CN=10.[redacted]	CN=10.113.65.171	Aug 27, 2019 1

Total rows: 2

5. In the Import CA Certificates dialog box, 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. If you generated the CSR from an external tool, you must also import the private key file that was created along with the CSR.



Select the array management certificates from your computer...

Root/Intermediate CA Certificates

Select root/intermediate CA certificates

Controller A Management Server Certificates

Select Controller A certificate

Select private key file (Optional)

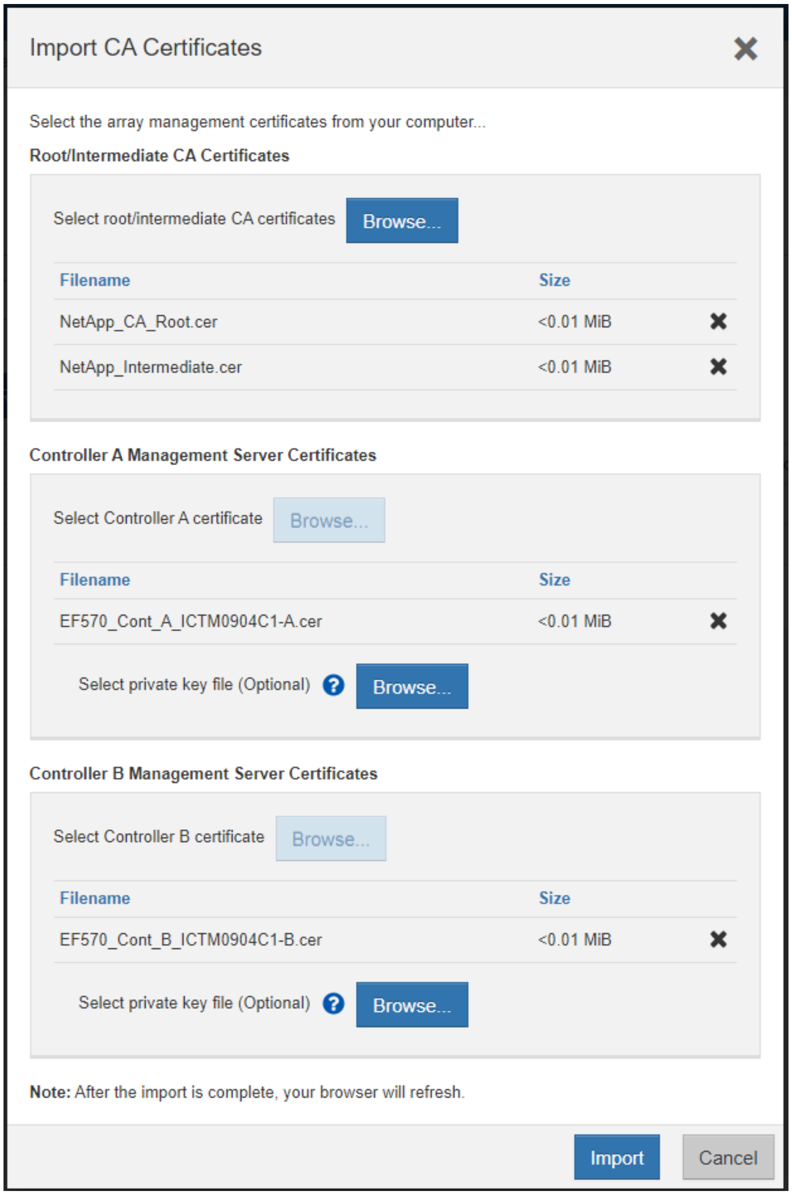
Controller B Management Server Certificates

Select Controller B certificate

Select private key file (Optional)

Note: After the import is complete, your browser will refresh.

6. When you have selected each file, click Import.



Import CA Certificates

Select the array management certificates from your computer...

Root/Intermediate CA Certificates

Select root/intermediate CA certificates

Filename	Size
NetApp_CA_Root.cer	<0.01 MiB
NetApp_Intermediate.cer	<0.01 MiB

Controller A Management Server Certificates

Select Controller A certificate

Filename	Size
EF570_Cont_A_ICTM0904C1-A.cer	<0.01 MiB

Select private key file (Optional)

Controller B Management Server Certificates

Select Controller B certificate

Filename	Size
EF570_Cont_B_ICTM0904C1-B.cer	<0.01 MiB

Select private key file (Optional)

Note: After the import is complete, your browser will refresh.

7. When prompted, enter your admin credentials.
8. When prompted, refresh the browser session.

   After you close the browser session and start a new System Manager session, the new session should indicate a secure browser connection.

Certificate management in Unified Manager

Unified Manager is an application included with the Web Services Proxy (WSP), which is installed on a Linux or Windows host to manage multiple controllers in a network. Unified Manager offers the following options for managing certificates between the controllers and the WSP server:

- Continue to accept self-signed certificates for the WSP server and storage system controllers.
- Obtain CA-signed certificates for the WSP server.

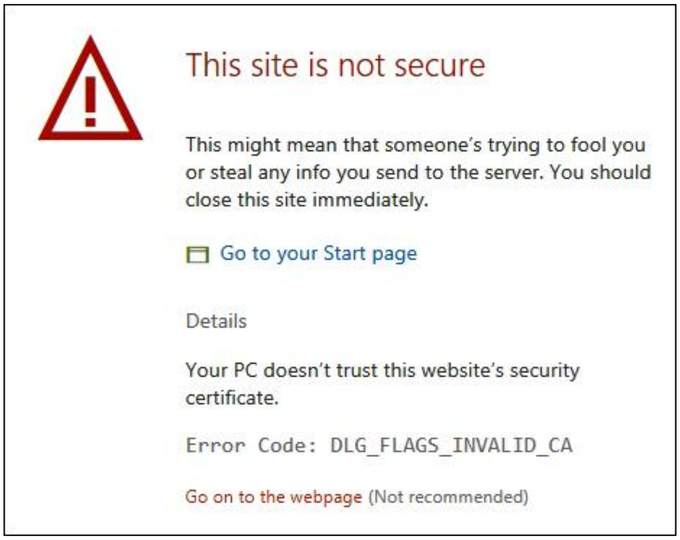
- Import signed certificates for the controllers.

Using self-signed certificates in Unified Manager

If you continue to use self-signed certificates, be aware that the browser used to access Unified Manager displays warning messages about the connection not being secure.

Trusting the WSP server connection at login

To access Unified Manager, you open a browser from the WSP's host and then enter the URL and your login credentials. Before the browser displays the Unified Manager login screen, it determines whether the WSP's web server is a trusted source. If the browser does not locate a CA-signed certificate for the server, it opens a warning message similar to the example below. From there, you can continue to the website. By continuing, you are accepting the self-signed certificate for that session.



This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Go to your Start page

Details

Your PC doesn't trust this website's security certificate.

Error Code: DLG_FLAGS_INVALID_CA

Go on to the webpage (Not recommended)

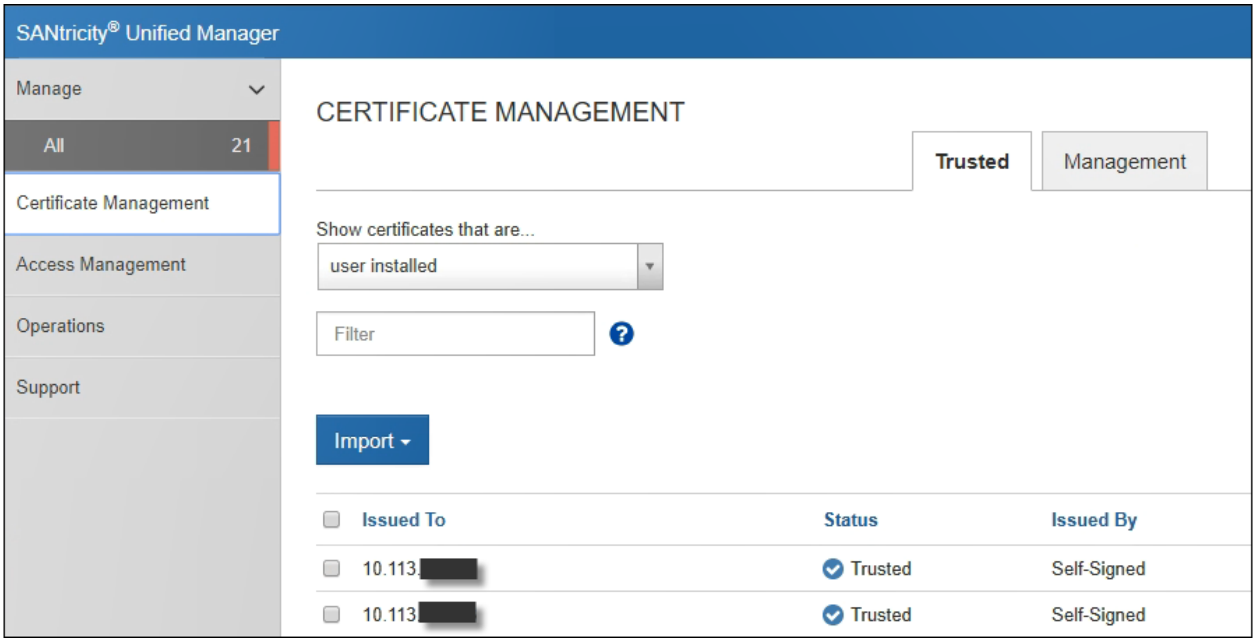
Trusting the controller connection during sessions

During a Unified Manager 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. Your selection is written to the user-managed truststore and persists across Unified Manager sessions.

To trust the controller connection, follow these steps:

1. Navigate to Unified Manager: Open a browser and then enter:
   `https://<WSP Server FQDN>:<port>/um`
2. Log in with your user name and password. You must log in with a user profile that includes Security admin permissions. Otherwise, certificate functions do not appear.
3. Select Certificate Management > Trusted tab.

   The Trusted page shows all certificates reported for the storage systems, both self-signed and CA-signed.



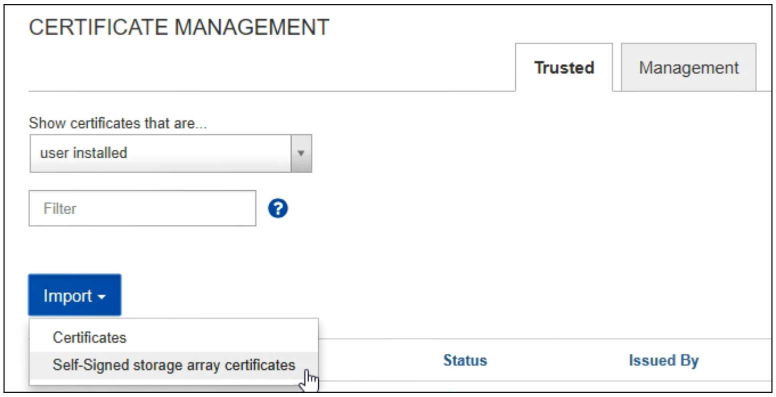
CERTIFICATE MANAGEMENT

Show certificates that are... user installed

Filter

	Issued To	Status	Issued By
□	10.113[redacted]	✓ Trusted	Self-Signed
□	10.113[redacted]	✓ Trusted	Self-Signed

4. Select Import > Self-Signed Storage Array Certificates.



CERTIFICATE MANAGEMENT

Show certificates that are... user installed

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

   The certificate is uploaded and validated.

Using CA-signed certificates for the WSP server

To obtain CA-signed certificates for secure communications between the controllers and the WSP server, follow this workflow:

1. **Generate a CSR file.** Use Unified Manager to create a certificate signing request (CSR).
2. **Submit the CSR file to a CA.** Download and send the CSR file to a CA and then wait for the certificates to be returned.
3. **Unpack the certificate chain** (if necessary). When the CA delivers the certificates, you might need to unpack the chain into three or more separate files: root, intermediate, and server certificates.
4. **Import the CA-signed certificates.** Using Unified Manager, import the certificate files from the CA.

Step 1: Generate a CSR file for the WSP server

The CSR provides information about your organization and includes a public key identifying the web server.

Note: **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 server generates a new private key, and the certificates you receive from the CA will not work.

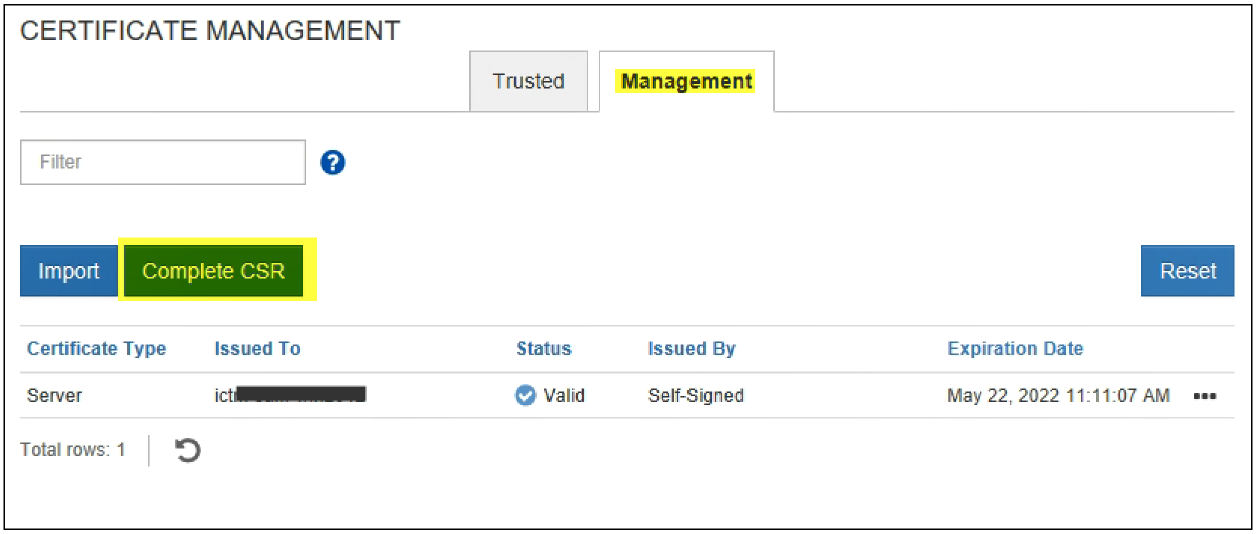
This task describes how to generate a CSR file from Unified Manager. Alternatively, you can generate a CSR file using a tool such as OpenSSL and can skip to Step 2.

To generate a CSR file using Unified Manager, follow these steps:

1. Navigate to Unified Manager: Open a browser and enter `https://<WSP Server FQDN>:<port>/um`
2. Enter your user name and password. You must log in with a user profile that includes Security admin permissions. Otherwise, certificate functions do not appear.
3. Go to the Certificate Management > Management tab.

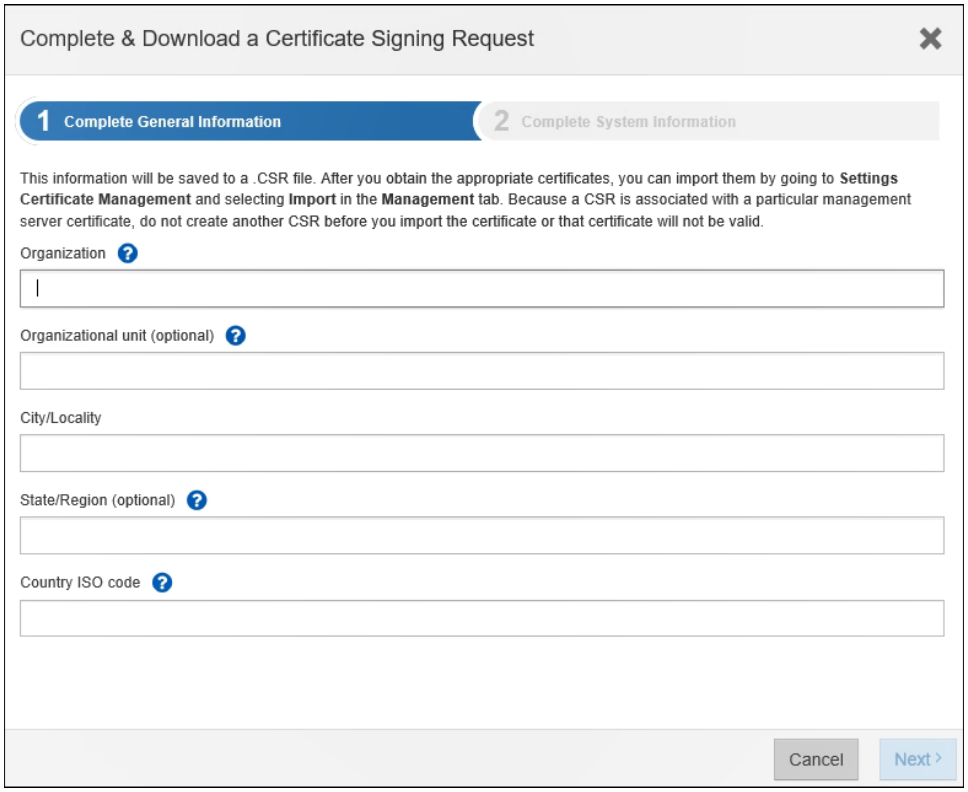
   Note: (Optional) After you install and configure the storage system, you can select Reset to regenerate the controller's self-signed certificates. This command restarts the process in a clean state following the storage system installation.

4. Select Complete CSR.



Certificate Type	Issued To	Status	Issued By	Expiration Date
Server	ict[redacted]	✓ Valid	Self-Signed	May 22, 2022 11:11:07 AM

5. In the first dialog box, enter your organization's information and location. Click Next.



Complete & Download a Certificate Signing Request

This information will be saved to a .CSR file. After you obtain the appropriate certificates, you can import them by going to **Settings** **Certificate Management** and selecting **Import** in the **Management** tab. Because a CSR is associated with a particular management server certificate, do not create another CSR before you import the certificate or that certificate will not be valid.

Organization ?

Organizational unit (optional) ?

City/Locality

State/Region (optional) ?

Country ISO code ?

6. In the second dialog box, enter the following information:
   - **Common name.** The IP address or DNS name of the host system where the Web Services Proxy is installed. NetApp recommends that you enter the fully qualified domain name (FDQN); for example, `name.domain.com`. Make sure that this address is correct; it must match exactly what you enter to access Unified Manager in the browser. Do not include http:// or https://. The DNS name is restricted to 63 characters, must start and end with a letter or digit, and can include only letters, digits, and a hyphen for the interior characters. The DNS name cannot begin with a wildcard.
   - **Alternate IP addresses.** (Optional). You can list any alternate IP addresses or aliases for the host system. For multiple entries, use a comma-delimited format.
   - **Alternate DNS names.** If you entered an FQDN in the first field, copy that name here. In addition, you can list any alternate FQDNs of the host system. For multiple entries, use a comma-delimited format. The DNS name cannot begin with a wildcard.
7. Double-check the host information to make sure that it is correct. If it is not, the certificates returned from the CA will fail when you try to import them.
8. Click Finish.

Step 2: Submit the CSR file

To submit the CSR file to a CA, follow these 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.
3. Wait for the CA to return the certificates.

Step 3: Unpack the certificate chain

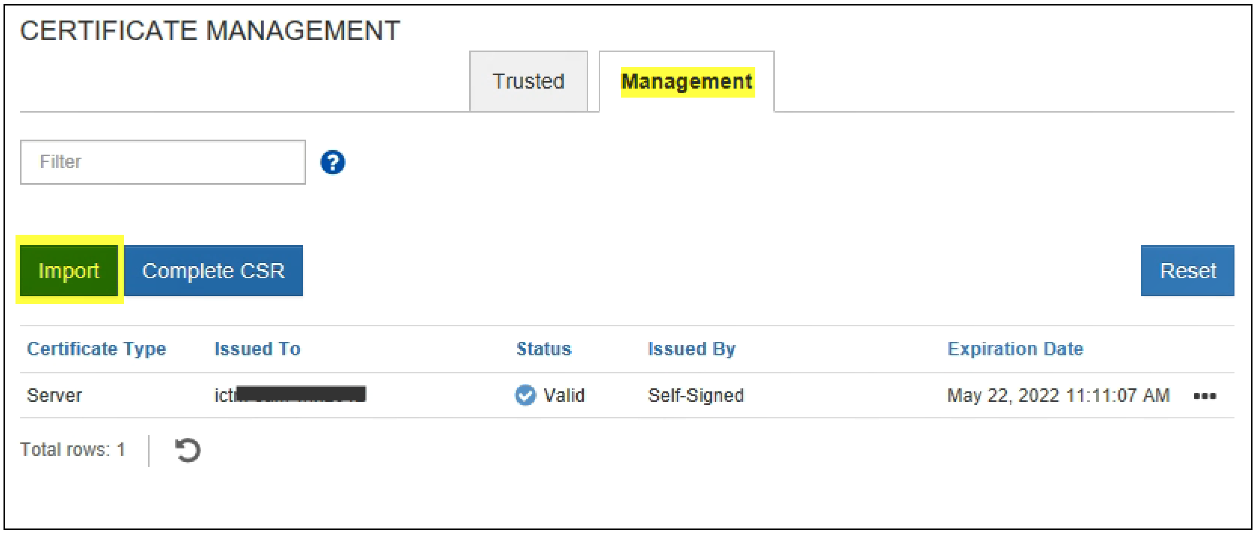
If the CA provides a chained certificate instead of individual certificates, break up the chain using the Windows Cert Manager tool. NetApp recommends that you use base-64 encoding when breaking up the cert chain. For instructions, see section 0, Step 3: Unpack the certificate chain.

Note: If you already requested certificates from this CA, you can use the same root and intermediate files that you obtained previously. Only the WSP server certificate will be unique.

Step 4: Import CA-signed certificates for the WSP server

To import the certificates, follow these steps:

1. Load the certificate files on the host system where the WSP server is installed.
2. Navigate to Unified Manager: Open a browser and enter `https://<WSP Server FQDN>:<port>/um`
3. Log in with your user name and password. You must log in with a user profile that includes Security admin permissions. Otherwise, certificate functions do not appear.
4. Go to the Certificate Management > Management tab.
5. Click Import.

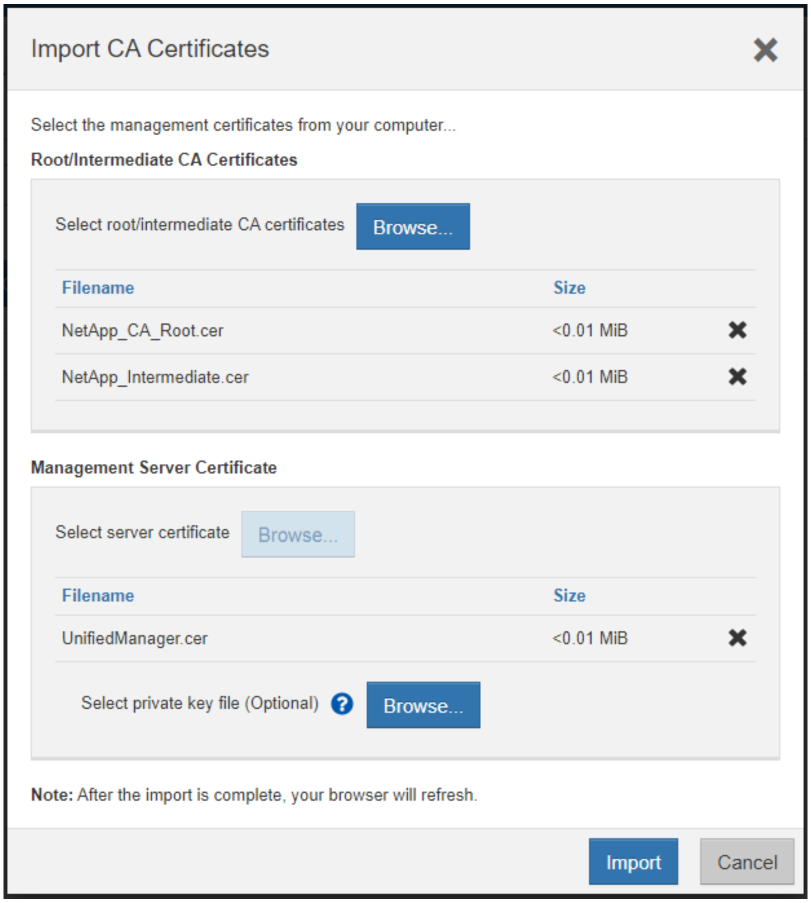


Certificate Type	Issued To	Status	Issued By	Expiration Date	
Server	ict[redacted]	✓ Valid	Self-Signed	May 22, 2022 11:11:07 AM	•••

Total rows: 1

6. In the Import dialog box, click the Browse buttons to first select the root and intermediate 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.
7. Click Import.



Import CA Certificates

Select the management certificates from your computer...

Root/Intermediate CA Certificates

Select root/intermediate CA certificates

Filename	Size
NetApp_CA_Root.cer	<0.01 MiB
NetApp_Intermediate.cer	<0.01 MiB

Management Server Certificate

Select server certificate

Filename	Size
UnifiedManager.cer	<0.01 MiB

Select private key file (Optional)

Note: After the import is complete, your browser will refresh.

The web server restarts and the browser refreshes. You can close the browser and start a new, secure browsing session.

Importing CA-signed certificates for the controllers

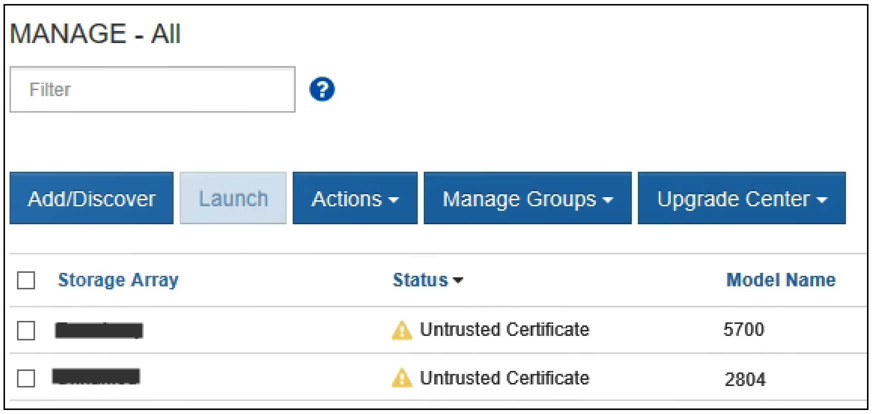
If you have previously obtained CA-signed certificates for the controllers, you can import these files in Unified Manager so the Web Services Proxy (WSP) server can authenticate incoming client requests from these controllers. Importing certificates for the controllers might also be necessary if you have your own CA, or if you use a CA that is not well known.

Note: If you do not have CA-signed certificates for the controllers, you must use System Manager to create the CSRs, and then import the certificate files when you receive them from the CA. For instructions, see section 0, “Using CA-signed certificates for the Controllers.”

To import signed certificates for the controllers in Unified Manager:

1. Navigate to Unified Manager: Open a browser and enter `https://<WSP Server FQDN>:<port>/um`
2. Log in with your user name and password. You must log in with a user profile that includes Security admin permissions. Otherwise, certificate functions do not appear.

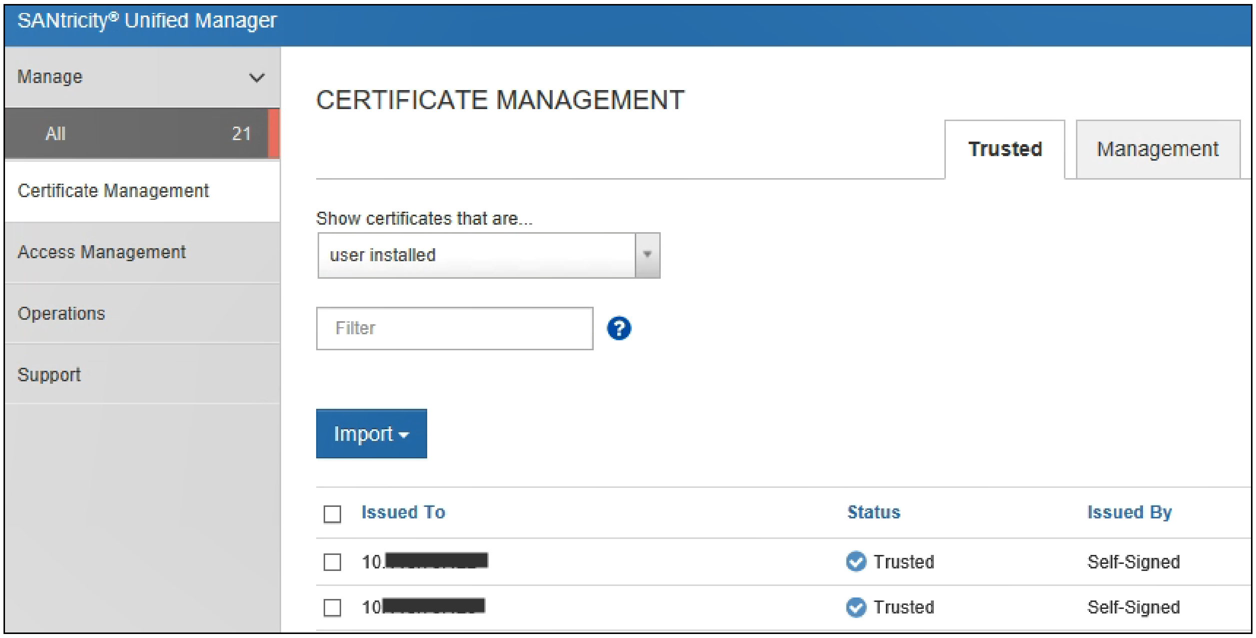
   Discovered storage systems are displayed on the Manage page, along with their status.



MANAGE - All

□	Storage Array	Status ▾	Model Name
□	[redacted]	⚠ Untrusted Certificate	5700
□	[redacted]	⚠ Untrusted Certificate	2804

3. Select the Certificate Management > Trusted tab.

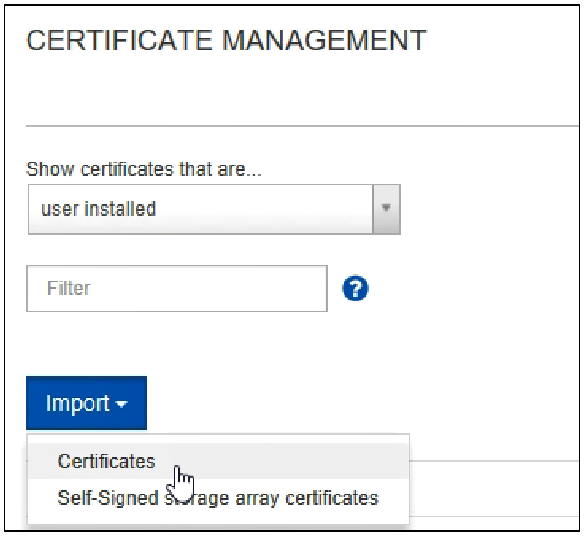


CERTIFICATE MANAGEMENT

Show certificates that are... user installed

□	Issued To	Status	Issued By
□	10.[redacted]	✓ Trusted	Self-Signed
□	10[redacted]	✓ Trusted	Self-Signed

4. Select Import > Certificates to import a CA-signed certificate.



CERTIFICATE MANAGEMENT

Show certificates that are...

user installed

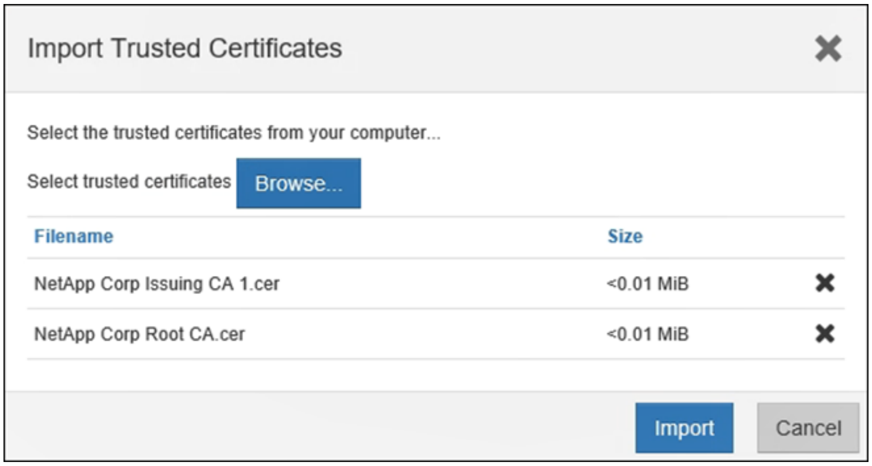
Filter

Import

Certificates

Self-Signed storage array certificates

5. In the dialog box, select the root and intermediate certificate files and then click Import.



Import Trusted Certificates

Select the trusted certificates from your computer...

Select trusted certificates Browse...

Filename	Size	
NetApp Corp Issuing CA 1.cer	<0.01 MiB	✖
NetApp Corp Root CA.cer	<0.01 MiB	✖

The certificate files are uploaded and validated, including the signed certificates associated with the root and intermediate files you selected. Their status is shown in the Certificate Management page.

Additional certificate management tasks

This section describes two additional tasks that are related to certificates:

- Importing trusted certificates for controllers
- Configuring revocation settings

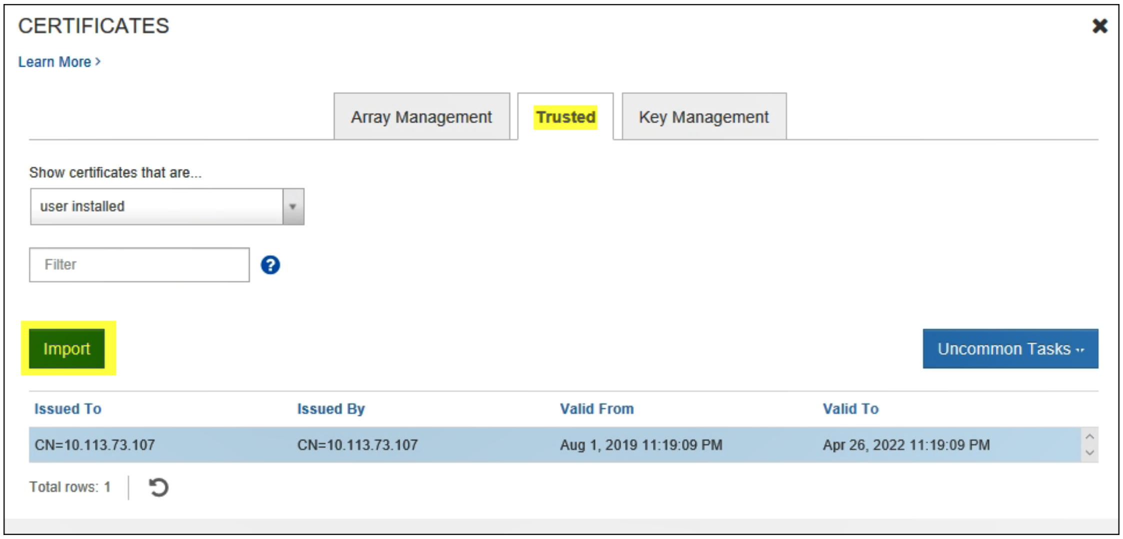
Importing trusted certificates for controllers that are acting as clients

Importing certificates for the controllers might be necessary if you have your own CA, or if you use a CA that is not well known, and you are attempting to set up a syslog server that uses TLS. In this case, the controllers are acting as a client instead of the server.

If the controller rejects a connection because it cannot validate the chain of trust for a server, follow these steps:

1. Select Settings > Certificates.

2. Select the Trusted tab and then click Import.



CERTIFICATES

Show certificates that are... user installed

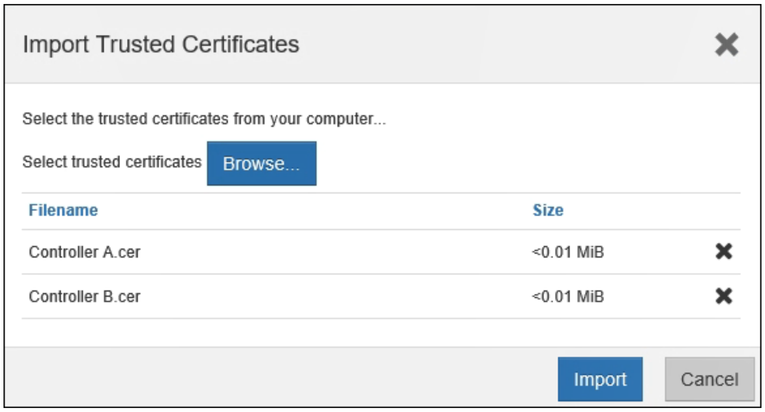
Issued To	Issued By	Valid From	Valid To
CN=10.113.73.107	CN=10.113.73.107	Aug 1, 2019 11:19:09 PM	Apr 26, 2022 11:19:09 PM

Total rows: 1

A dialog box opens in which you can import the trusted certificate files.

3. Click Browse to select the certificate files for the controllers.

The file names are displayed in the dialog box.



Import Trusted Certificates

Select the trusted certificates from your computer...

Select trusted certificates

Filename	Size
Controller A.cer	<0.01 MiB
Controller B.cer	<0.01 MiB

4. Click Import.

Configuring revocation settings for CA certificates

Automatic revocation checking is helpful in cases where the CA improperly issued a certificate, or a private key is compromised. If the storage system attempts to connect to a server with a revoked certificate, the connection is denied, and an event is logged.

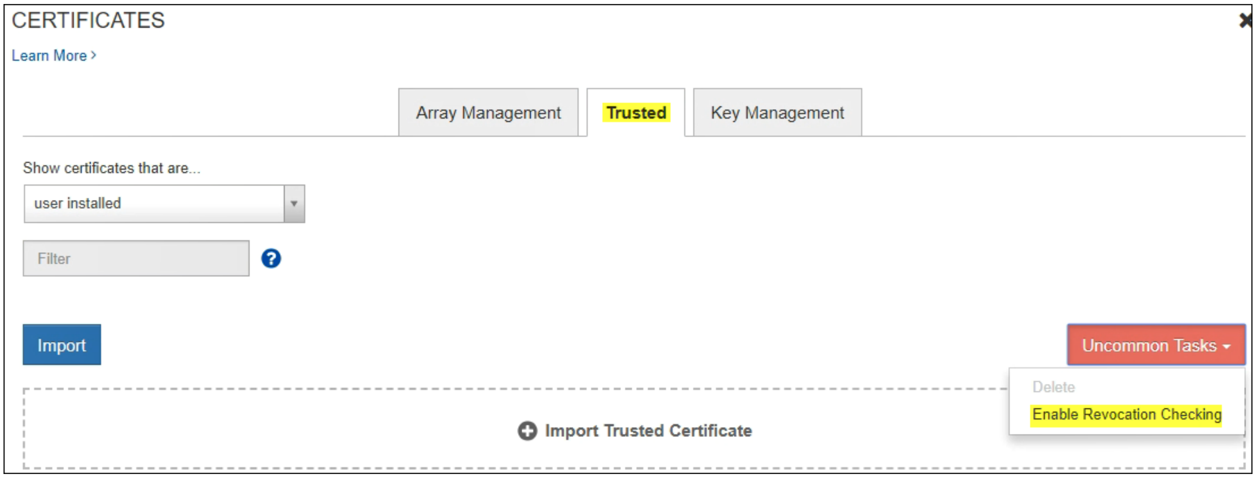
When you enable revocation, System Manager locates the URL for the Online Certificate Status Protocol (OCSP) server from the certificate file. You can continue to use this OCSP server, or you can configure your own OCSP.

Note: When revocation checking is enabled, you must have a DNS server configured on both controllers to enable use of an FQDN for the OCSP server. DNS configuration is available from the Hardware page in System Manager.

To configure revocation settings:

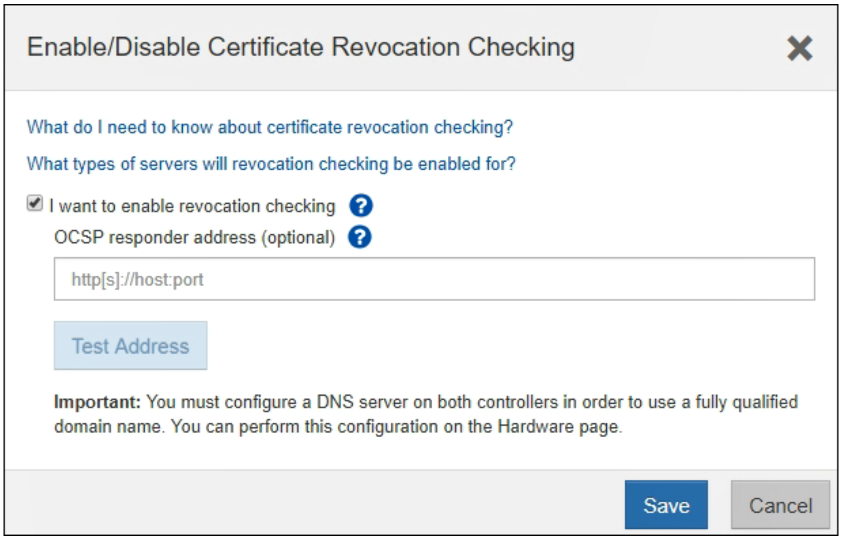
1. In System Manager, select Settings > Certificates.

2. Select the Trusted tab.
3. Click Uncommon Tasks and then select Enable Revocation Checking from the drop-down menu.



4. Select I Want to Enable Revocation Checking.

   A checkmark appears in the checkbox and additional fields appear in the dialog box.



Enable/Disable Certificate Revocation Checking

What do I need to know about certificate revocation checking?

What types of servers will revocation checking be enabled for?

☑ I want to enable revocation checking

OCSP responder address (optional)

http[s]://host:port

Important: You must configure a DNS server on both controllers in order to use a fully qualified domain name. You can perform this configuration on the Hardware page.

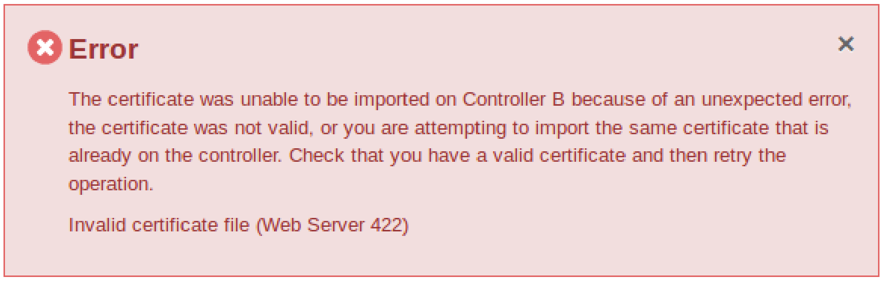
5. By default, System Manager uses the OCSP server URL that is specified in the certificate file. If you want to use your own server, enter its URL in the OCSP Responder Address field.

   Note: Specifying an OCSP responder address in System Manager overrides the OCSP address found in the certificate file.

6. Click Test Address to make certain that the system can open a connection to the specified URL.
7. Click Save.

Troubleshooting an invalid certificate error

When importing CA-signed certificates, you might see an Invalid Certificate File (Web Server 422) error similar to the example.



Error

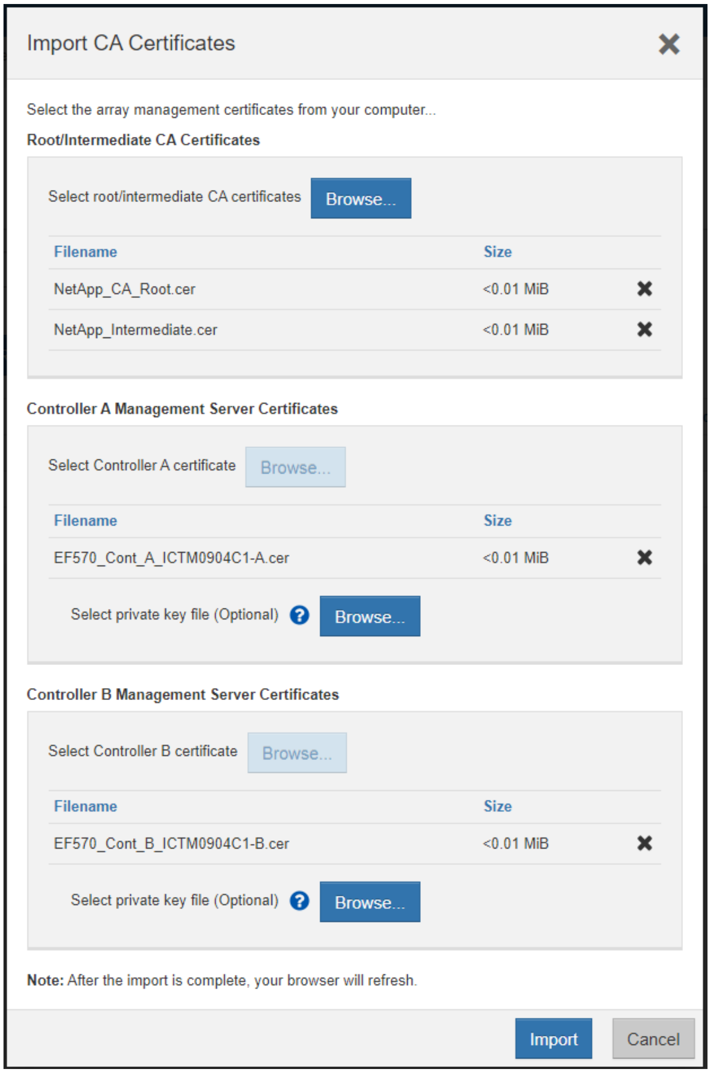
The certificate was unable to be imported on Controller B because of an unexpected error, the certificate was not valid, or you are attempting to import the same certificate that is already on the controller. Check that you have a valid certificate and then retry the operation.

Invalid certificate file (Web Server 422)

If you see this error message, follow the checklist in Table 4 to troubleshoot the issue.

Table 4) Checklist to determine whether a certificate is valid.

Checklist question	Explanation and resolution
1. Did you generate another CSR file after you sent the original CSR to the CA?	**Explanation.** Whenever you generate a certificate signing request (CSR), the system creates a new public/private key pair. If you generate another CSR after sending the original to a CA, the system overwrites the key pairs and generates new ones. As a result, when you try to import the CA-signed certificates, which are based on the old private key pair, the import attempt fails. **Resolution.** Resubmit the latest CSR file to the CA and request new certificates.
2. Did you enter the correct controller addresses in the CSR?	**Explanation.** When you populate the CSR form, the Subject Alternative Names (or IP addresses) for the controllers must be accurate. Otherwise, the import attempt fails. **Resolution.** Review the CSR file and check that the Common Name and Subject Alternative Names for the controllers are accurate. To read the CSR file, you can use a free CSR decoder, available on the Internet; for example, https://www.sslshopper.com/csr-decoder.html. If the controller addresses are inaccurate, you need to regenerate a CSR and send it to the CA for new certificates.
3. Did the CA return certificate files in a supported format?	**Explanation.** Certificate files must be formatted in PEM (Base64 ASCII encoding), with one of these file extensions: .pem, .crt, .cer, or .key **Resolution.** Contact your CA and request certificate files in PEM format. Or find a website that allows you to convert the file formats to PEM.
4. Did you attempt to import a wildcard certificate?	**Explanation.** Wildcard certificates are not currently supported. **Resolution.** Contact your CA and request a certificate in PEM format.
5. Did you break the certificate chain into individual files?	**Explanation.** The CA typically sends you a single, certificate chain file—for example, a `p7b` file. You cannot import this file. Instead, you must use a utility such as Windows Cert Manager to break up the chain into the root, intermediate, and server files. You can then import them individually. **Resolution.** Follow the instructions in Section 0, Step 3: Unpack the certificate chain. If the root certificate was successfully imported, but not the others, contact Technical Support or see this KB article to break up the files and reimport them: E-Series Invalid Certificate File on System Manager.
6. Do the certificate files for the controllers have unique names?	**Explanation.** Each controller must have a certificate file with a unique name. If the names are identical, the import fails. **Resolution.** Rename the server certificate files for Controller A and Controller B—for example, ContrACert and ContrBCert.

Checklist question	Explanation and resolution
7. Did you include all certificates—root, intermediate, and server—during the import?	**Explanation.** When importing certificates, you must include each file in the chain: root, intermediate, and server. Without one of these files, the system cannot validate the chain and the import fails. **Resolution.** Check that both the root and intermediate certificates are included in the upper portion of the dialog box, and that the server certificates are included in the lower portion.  Import CA Certificates ✖ Select the array management certificates from your computer... Root/Intermediate CA Certificates Select root/intermediate CA certificates Browse... Filename Size NetApp_CA_Root.cer <0.01 MiB ✖ NetApp_Intermediate.cer <0.01 MiB ✖ Controller A Management Server Certificates Select Controller A certificate Browse... Filename Size EF570_Cont_A_ICTM0904C1-A.cer <0.01 MiB ✖ Select private key file (Optional) ? Browse... Controller B Management Server Certificates Select Controller B certificate Browse... Filename Size EF570_Cont_B_ICTM0904C1-B.cer <0.01 MiB ✖ Select private key file (Optional) ? Browse... **Note:** After the import is complete, your browser will refresh. Import Cancel

Where to find additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- NetApp SANtricity Management Security
  TR-4712 - NetApp SANtricity Management Security
- NetApp Product Documentation
  https://docs.netapp.com

Version history

Version	Date	Document version history
Version 1.0	January 2020	Initial release.
Version 2	October 2020	Updated for SANtricity System Manager version 11.7 and Unified Manager version 5.0.
Version 3	March 2022	Refreshed dates, updated dialogs used to import signed certificates.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Trademark Information

TR-4813-0322

NetApp