MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS 2025 R1

Certificates guide

milestone

Contents

Copyright, trademarks, and disclaimer ... **3**

About this guide ... **4**

Introduction to certificates ... **5**

Overview of the scenarios and procedures used with certificates ... **8**

Which clients need certificates? ... 11

Server Configurator (explained) ... **13**

PowerShell scripts ... **16**

Creating and distributing certificates manually ... **17**

Create CA certificate ... 17

Install certificates on the clients ... 19

Create SSL certificate ... 27

Import SSL certificate ... 29

Create SSL certificate for the failover management server ... **38**

Install certificates for communication with the mobile server ... **40**

Install third-party or commercial CA certificates for communication with the Management Server or Recording Server ... **57**

Install Active Directory Certificate Services ... **74**

Install certificates in a domain for communication with the Management Server or Recording Server **86**

Install certificates in a Workgroup environment for communication with the Management Server or Recording Server ... **107**

Install certificates for communication with the Event Server ... **129**

Import client certificates ... **132**

View encryption status to clients ... **138**

View encryption status on a failover recording server ... **139**

Appendix A Create CA Certificate script ... **140**

Appendix B Create Server SSL Certificate script ... **141**

Appendix C Create Failover Management Server Certificate script ... **142**

Copyright, trademarks, and disclaimer

Copyright © 2025 Milestone Systems A/S

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This text is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserves the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third-party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file `3rd_party_software_terms_and_conditions.txt` located in your Milestone system installation folder.

About this guide

This guide gives you an introduction to encryption and certificates, together with step by step procedures on how to install certificates in a Windows Workgroup environment.

Milestone recommends that you establish a Public Key Infrastructure (PKI) for creating and distributing certificates. A PKI is a set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. In a Windows domain, it's recommended to establish a PKI using the Active Directory Certificate Services (AD CS).
If you are unable to build a PKI, either due to having different domains without trust between them or due to not using domains at all, it's possible to manually create and distribute certificates.
WARNING: Creating and distributing certificates manually isn't recommended as a secure way of distributing certificates. If you choose manual distribution, you are responsible for always keeping the private certificates secure. When you keep the private certificates secure, the client computers that trust the certificates are less vulnerable to attacks.

When do you need to install certificates?

First, decide whether your system actually needs encrypted communication.

Don't use certificates with recording server encryption if you are using one or more integrations that don't support HTTPS communication. This is, for example, third-part MIP SDK integrations that don't support HTTPS.

Unless your installation is made in a physically isolated network, it's recommended that you secure the communication by using certificates.

This document describes when to use certificates:

- If your XProtect VMS system is set up in a Windows Workgroup environment
- Before you install or upgrade to XProtect VMS 2019 R1 or newer, if you want to enable encryption during the installation
- Before you enable encryption, if you installed XProtect VMS 2019 R1 or newer without encryption
- When you renew or replace certificates due to expiry

Introduction to certificates

Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP) for secure communication over a computer network. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS), or its predecessor, Secure Sockets Layer (SSL).

In XProtect VMS, secure communication is obtained by using TLS/SSL with asymmetric encryption (RSA).

TLS/SSL uses a pair of keys—one private, one public—to authenticate, secure, and manage secure connections.

A certificate authority (CA) is anyone who can issue root certificates. This can be an internet service that issues root certificates, or anyone who manually generates and distributes a certificate. A CA can issue certificates to web services, that is to any software using https communication. This certificate contains two keys, a private key and a public key. The public key is installed on the clients of a web service (service clients) by installing a public certificate. The private key is used for signing server certificates that must be installed on the server. Whenever a service client calls the web service, the web service sends the server certificate, including the public key, to the client. The service client can validate the server certificate using the already installed public CA certificate. The client and the server can now use the public and private server certificates to exchange a secret key and thereby establish a secure TLS/SSL connection.

For manually distributed certificates, certificates must be installed before the client can make such a verification.

See Transport Layer Security for more information about TLS.

In XProtect VMS, the following locations are where you can enable TLS/SSL encryption:

- In the communication between the management server and the recording servers, event servers, and mobile servers
- On the recording server in the communication with clients, servers, and integrations that retrieve data streams from the recording server
- In the communication between clients and the mobile server

In this guide, the following are referred to as clients:

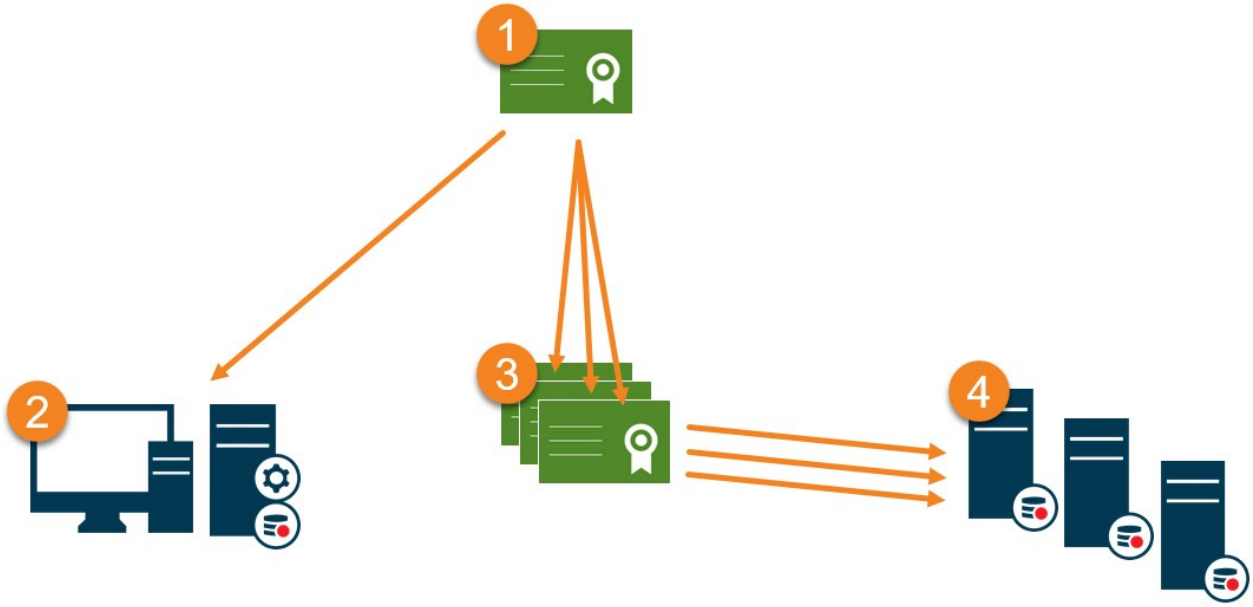
- XProtect Smart Client
- Management Client
- Management Server (for System Monitor and for images and AVI video clips in email notifications)
- XProtect Mobile Server
- XProtect Event Server
- XProtect LPR
- Milestone Open Network Bridge
- XProtect DLNA Server
- Sites that retrieve data streams from the recording server through Milestone Interconnect
- Third-party MIP SDK integrations that support HTTPS

For solutions built with MIP SDK 2018 R3 or earlier that access recording servers:

- If the integrations are made using MIP SDK libraries, they need to be rebuilt with MIP SDK 2019 R1
- If the integrations communicate directly with the Recording Server APIs without using MIP SDK libraries, the integrators must add HTTPS support themselves
- If in doubt, ask your vendor who supplied the integration

Certificate distribution

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS.



1 A certificate authority (CA) is anyone who can issue root certificates. A CA certificate acts as a trusted third-party, trusted by both the subject/owner (server) and by the party that verifies the certificate (clients) (see Create CA certificate on page 17).

2 The public certificate must be trusted on all client computers. In this way the clients can verify the validity of the certificates issued by the CA (see Install certificates on the clients on page 19).

3 The CA certificate is used to issue private server authentication certificates to the servers (see Create SSL certificate on page 27).

4 The created private SSL certificates must be imported to the Windows Certificate Store on all servers (see Import SSL certificate on page 29).

Requirements for the private SSL certificate:

- Issued to the server so that the server's host name is included in the certificate, either as subject (owner) or in the list of DNS names that the certificate is issued to
- Trusted on all computers running services or applications that communicate with the service on the servers, by trusting the CA certificate that was used to issue the SSL certificate
- The service account that runs the server must have access to the private key of the certificate on the server.

Certificates have an expiry date. You will not receive a warning when a certificate is about to expire. If a certificate expires, the clients will no longer trust the server with the expired certificate and thus cannot communicate with it.
To renew the certificates, follow the steps in this guide as you did when you created certificates.

Overview of the scenarios and procedures used with certificates

The procedures for configuring secure communication in an XProtect VMS environment are different, depending on which type of servers require secure communication.

The procedures are also different in a WORKGROUP network compared to a DOMAIN network.

The types of XProtect VMS client applications that are used in the system also determine some of the required procedures for secure communications.

> Using certificates for the server communication can usually be ignored on a single server installation, except for serving as an extra safeguard when communicating with the management server.

This list shows the different scenarios:

- XProtect Mobile Server

  In XProtect VMS, encryption is enabled or disabled per Mobile Server. You enable or disable encryption either during installation of the XProtect VMS product or by using the Server Configurator. When you enable encryption on a Mobile Server, you then use encrypted communication with all clients, services, and integrations that retrieve data streams.

  The Mobile Server connects to the XProtect Mobile client and XProtect Web Client. Browsers, operating systems, and mobile devices that host these clients maintain a list of trusted CA root certificates. Only the authority knows its private key, but everyone knows its public key, which is similar to any particular certificate.

  These clients, then, already have certificate keys installed and work with most any third-party certificate that is available to install on the Mobile Server itself.

  Since each third-party CA has their own requirements for requesting a certificate, it is best to investigate the individual requirements directly with the CA.

  This document describes how to create a certificate request on the Mobile Server and install the certificate once it has been issued from the CA.

  See:

  Install certificates for communication with the mobile server on page 40

- Milestone XProtect Management Server and Recording Server

  You can encrypt the two-way connection between the Management Server and the Recording Server. When you enable encryption on the Management Server, it applies to connections from all the Recording Servers that connect to the Management Server. If you enable encryption on the Management Server, you must also enable encryption on all of the Recording Servers. Before you enable encryption, you must install security certificates on the Management Server and all Recording Servers, including Failover Recording Servers.

  - Third-party or commercial CA certificate

    The process for requesting certificates from third-party CAs for use with Management Servers and Recording Servers is the same as with the Mobile Server. The only difference is the configuration with the Server Configurator.

    See:

    Install third-party or commercial CA certificates for communication with the Management Server or Recording Server on page 57

  - Domain

    When client and server endpoints are all operating within a Domain environment with its own certificate authority infrastructure, there is no requirement to distribute CA certificates to client workstations. As long as you have a Group Policy within the Domain, that will handle the automatic distribution of all trusted CA certificates to all users and computers in the Domain.

    The process for requesting a certificate and installing a server certificate is the same as in a Workgroup.

    See:

    Install certificates in a domain for communication with the Management Server or Recording Server on page 86

  - Workgroup

    When operating in a Workgroup environment, it is assumed that there is no certificate authority infrastructure. To distribute certificates, it is required to create a certificate authority infrastructure. There is also a requirement to distribute the certificate keys to client workstations. Except for these requirements, the process of requesting and installing a certificate on a server is similar to both the Domain and third-party scenarios.

    See:

    Install certificates in a Workgroup environment for communication with the Management Server or Recording Server on page 107

- XProtect Event Server

  You can encrypt the two-way connection between the Event Server and the components that communicate with the Event Server, including the LPR Server. When you enable encryption on the Event Server, it applies to connections from all the components that connect to the Event Server. Before you enable encryption, you must install security certificates on the Event Server and all connecting components.

  See:

  Install certificates for communication with the Event Server on page 129

- Client

  In the Third-party/commercial and Domain scenarios, clients do not need certificate keys installed. You only need to install client certificate keys in a Workgroup environment.

  When you enable encryption on a Recording Server, communication to all clients, servers, and integrations that retrieve data streams from the Recording Server are encrypted.

  In this document these are referred to as 'clients' to the Recording Server:

  - XProtect Smart Client
  - Management Client
  - Management Server (for System Monitor and for images and AVI video clips in email notifications)
  - XProtect Mobile Server
  - XProtect Event Server
  - XProtect LPR
  - Milestone Open Network Bridge
  - XProtect DLNA Server
  - Sites that retrieve data streams from the recording server through Milestone Interconnect
  - Some third-party MIP SDK integrations

-

  For solutions built with MIP SDK 2018 R3 or earlier that accesses recording servers: If the integrations are made using MIP SDK libraries, they need to be rebuilt with MIP SDK 2019 R1; if the integrations communicate directly with the Recording Server APIs without using MIP SDK libraries, the integrators must add HTTPS support themselves.

  See:

  Which clients need certificates? on page 11

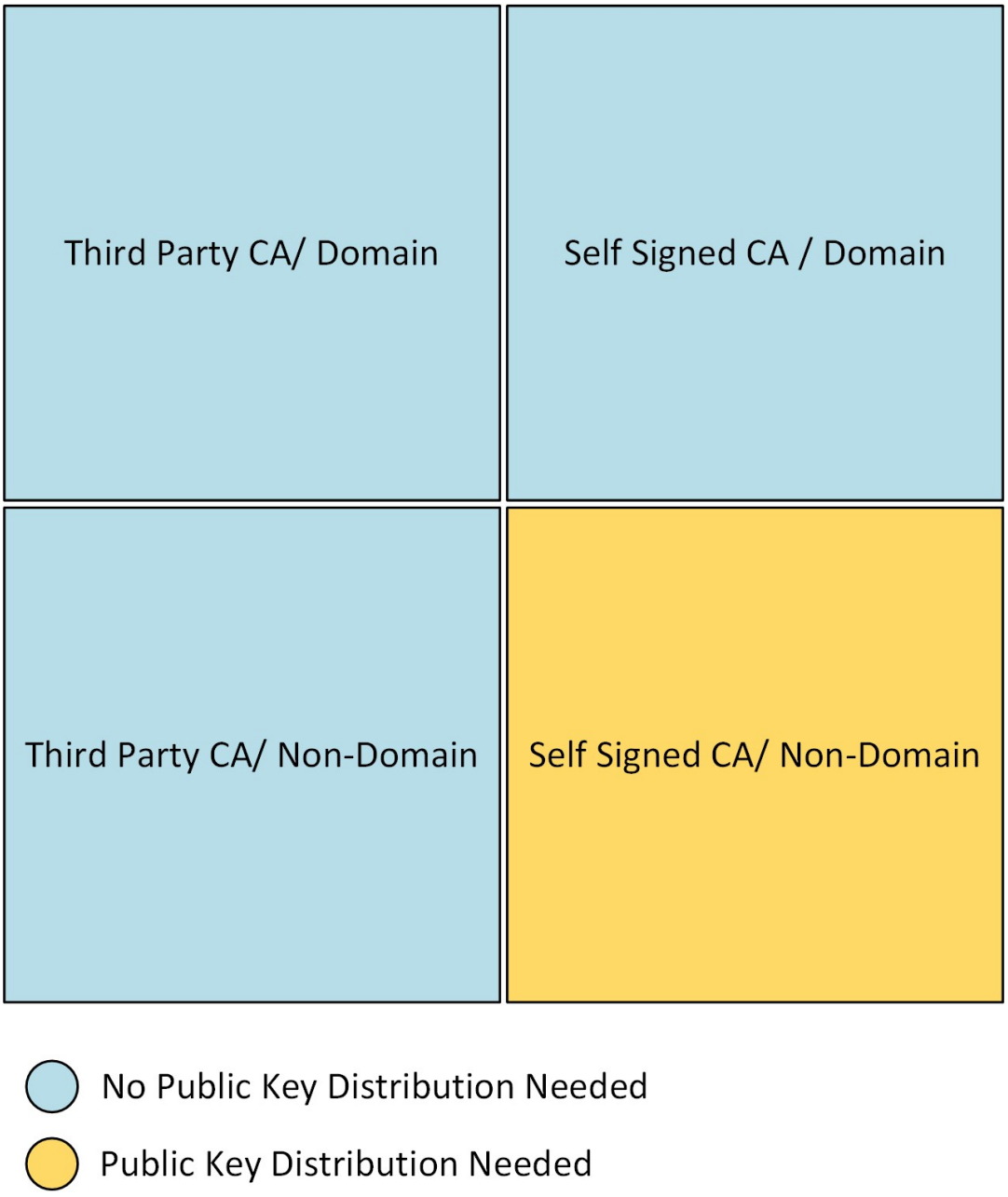
  Import client certificates on page 132

Which clients need certificates?

Which clients need certificates installed? How do we plan for this? What can we do to prepare?

Web-browser-based clients and clients that are distributed via a public third-party application distribution service or store, for example Google Play or Apple AppStore, should not require you to install a certificate. XProtect Mobile will not use installed certificates. XProtect Mobile can only use trusted third-party certificates.

If the XProtect servers (Management Server and Recording Server) are installed on computers that are joined to the Domain, and the users who are logging into the Smart Client are all Domain users, the Domain will handle all public key distribution and authentication required to establish secure communications.



Only in a scenario where Active Directory Certificate Services (AD CS) is used to create self-signed certificates and the resources (users and computers) are operating in a non-domain environment would there be any need to distribute public keys to client workstations.

See also Install certificates on the clients on page 19 and Import client certificates on page 132.

Server Configurator (explained)

Use the Server Configurator to select certificates on local servers for encrypted communication and register server services to make them qualified to communicate with the servers.

The following types of servers in XProtect VMS need certificates for secure communication:

- Management Servers
- Recording Servers
- Event Servers
- Mobile Servers

These servers work with the Server Configurator to manage secure communications. Use the Server Configurator to set whether or not the XProtect servers use secure encrypted communications and to manage the certificates that the XProtect servers use.

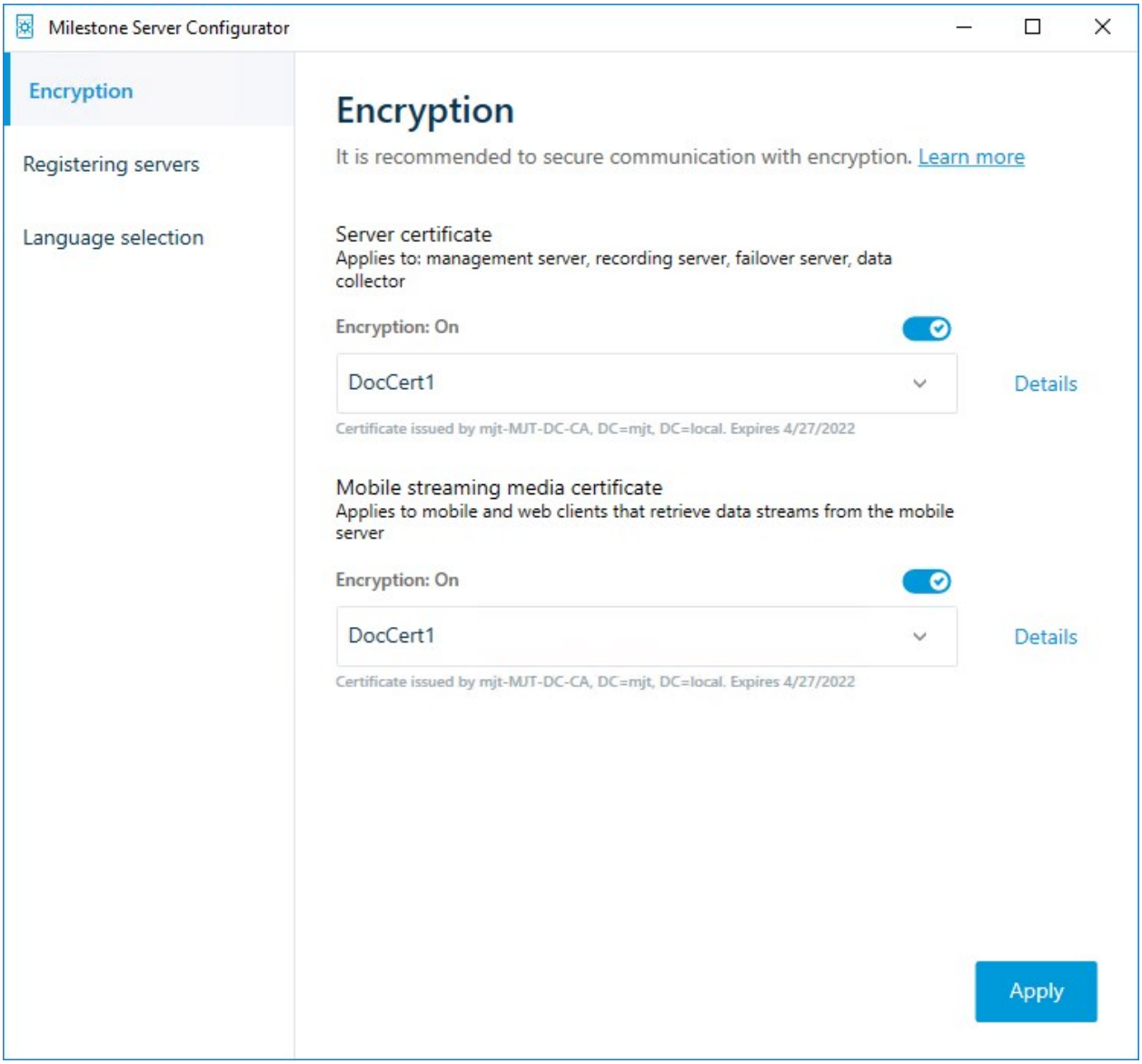
The Server Configurator is installed by default on any computer that hosts an XProtect server.

Open the Server Configurator from:

- The Windows Start menu

  or

- The XProtect server manager by right-clicking the server manager icon on the computer task bar and selecting Server Configurator



Use the Server Configurator to choose the certificates that the XProtect servers use to secure communicates with their client applications, and to verify that encryption settings are configured properly.

In the **Encryption** section of the Server Configurator, set encryption of the following types:

- **Server certificate**

  Select the certificate to be used to encrypt the two-way connection between the management server and the following servers:

  - Recording Server
  - Event Server
  - Log Server
  - LPR Server
  - Mobile Server

- **Event server and add-ons**

  Select the certificate to be used to encrypt the two-way connection between the event server and the components that communicate with the event server, including the LPR Server.

- **Streaming media certificate**

  Select the certificate to be used to encrypt communication between the recording servers and all clients, servers, and integrations that retrieve data streams from the recording servers.

- **Mobile streaming media certificate**

  Select the certificate to be used to encrypt communication between the mobile server and the mobile and web clients that retrieve data streams from the mobile server.

In the **Registering servers** section of the Server Configurator, register the servers that are running on the computer with the designated management server.

To register the servers, verify the address of the management server and select **Register**.

PowerShell scripts

You can use PowerShell and the Milestone PSTools Module to install, integrate, simplify, monitor and automate the ongoing maintenance and required configuration processes of large, complex, and technically advanced XProtect VMS systems.

Nonetheless, Milestone recommends that administrators, installers and technicians know how to configure their customer's XProtect VMS environment manually. You will learn with experience when to use PowerShell scripts in place of manual configurations. You can find PowerShell scripts in these locations:

- PowerShell Process/Video for Mobile Server & Lets Encrypt
- Github repository for Milestone PSTools information, documentation and scripts.

Creating and distributing certificates manually

Important to know:

> Creating and distributing certificates manually is not recommended as a secure way of distributing certificates. If you choose manual distribution, you are responsible for keeping the private certificates secure at all times. When you keep the private certificates secure, the client computers that trust the certificates are less vulnerable to attacks.

In some situations, Windows Update may periodically remove certificates that are not from a "trusted third-party certificate authority."

To make sure that your certificates are not removed by Windows Update, you must enable the **Turn off Automatic Root Certificates Update**. Before making this change, you should make sure that the change is following your company security policy.

1. Enable this by opening the **Local Group Policy Editor** on the computer (click on the Windows start bar and type **gpedit.msc**).
2. In the Windows **Local Group Policy Editor**, navigate to **Computer Configuration** > **Administrative Templates** > **System** > **Internet Communication Management** > **Internet Communication Settings**.
3. Double-click **Turn off Automatic Root Certificate Update** and select **Enabled**.
4. Click **OK**.

Note that this setting might be controlled by a domain policy. In which case, it must be disabled at that level.

Your certificate will now stay on the computer despite it is not from a "trusted third-party certificate authority," because Windows Update will not contact the Windows Update website to see if Microsoft has added the CA to its list of trusted authorities.

Create CA certificate

On a computer with restricted access and not connected to your XProtect system, run this script once to create a CA certificate.

> The computer that you use for creating certificates must run Window 10 or Windows Server OS 2016 or newer.

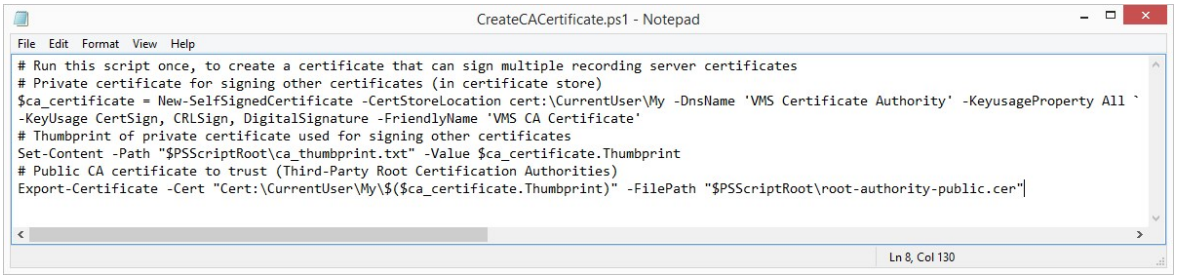
Be aware that when you create certificates in this way, the certificates are related to the computer they are installed on. If the computer name changes, then the VMS will not be able to start until the certificates are created again and re-installed on the computer.

This script creates two certificates:

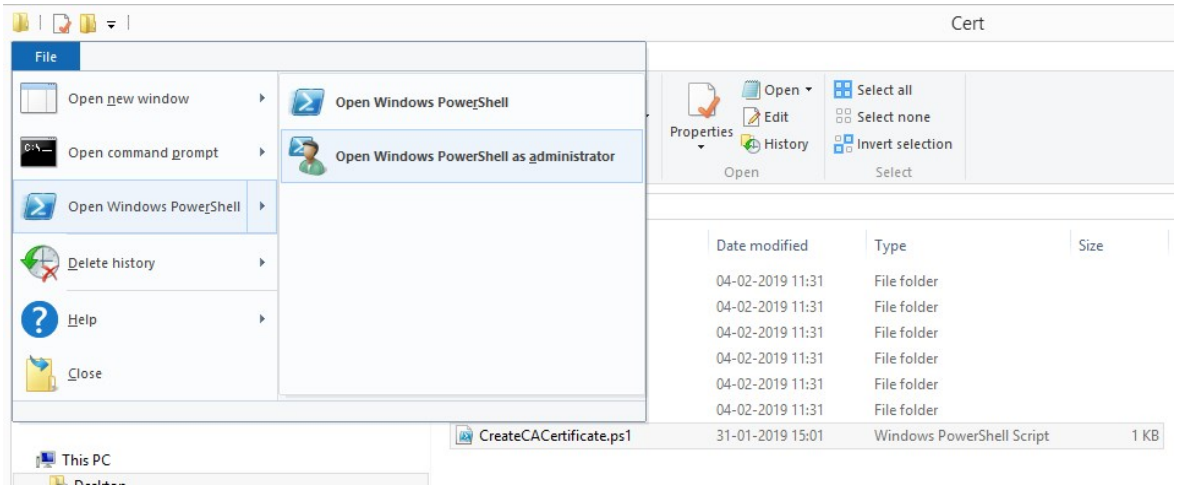
- A private certificate - only exists in the Personal Certificates store for the current user after the script is run. It is recommended that you create a backup kept on a medium (USB) in a safe place, and preferably two backups kept in physically different locations. With the exception of the backups, this certificate should never leave the computer that you created the certificate on
- A public certificate - to be imported as trusted certificate on all client computers

1. In Appendix A, in the back of this guide, you find a script for creating the CA certificate. Copy the content.
2. Open Notepad and paste the content.

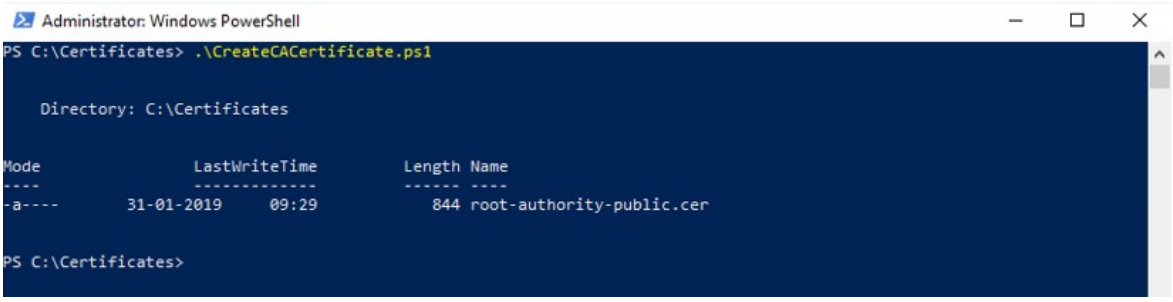
   It is very important that the lines break in the same places as in Appendix A. You can add the line breaks in Notepad or alternatively, reopen this PDF with Google Chrome, copy the content again and paste it into Notepad.



3. In Notepad, click **File** -> **Save as**, name the file **CreateCACertificate.ps1** and save it locally, like this: `C:\Certificates\CreateCACertificate.ps1`.
4. In File Explorer, go to `C:\Certificates` and select the **CreateCACertificate.ps1** file.
5. In the **File** menu, select **Open Windows PowerShell** and then **Open Windows PowerShell as administrator**.



6. In PowerShell at the prompt, enter **.\CreateCACertificate.ps1** and press **Enter**.



7. Check that the **root-authority-public.cer** file appears in the folder where you ran the script.

> Your computer may require that you change the PowerShell execution policy. If yes, enter **Set-ExecutionPolicy RemoteSigned**. Press **Enter** and select **A**.

Install certificates on the clients

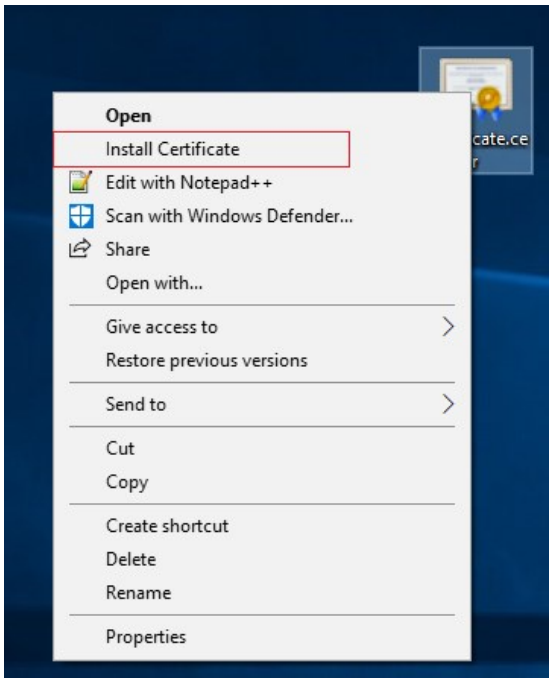
After you created the CA certificate, you trust the public CA certificate by installing it on all the computers that act as clients to the service according to the descriptions in Introduction to certificates on page 5.

> See Import client certificates on page 132 for an alternative procedure to manually installing certificates on clients.

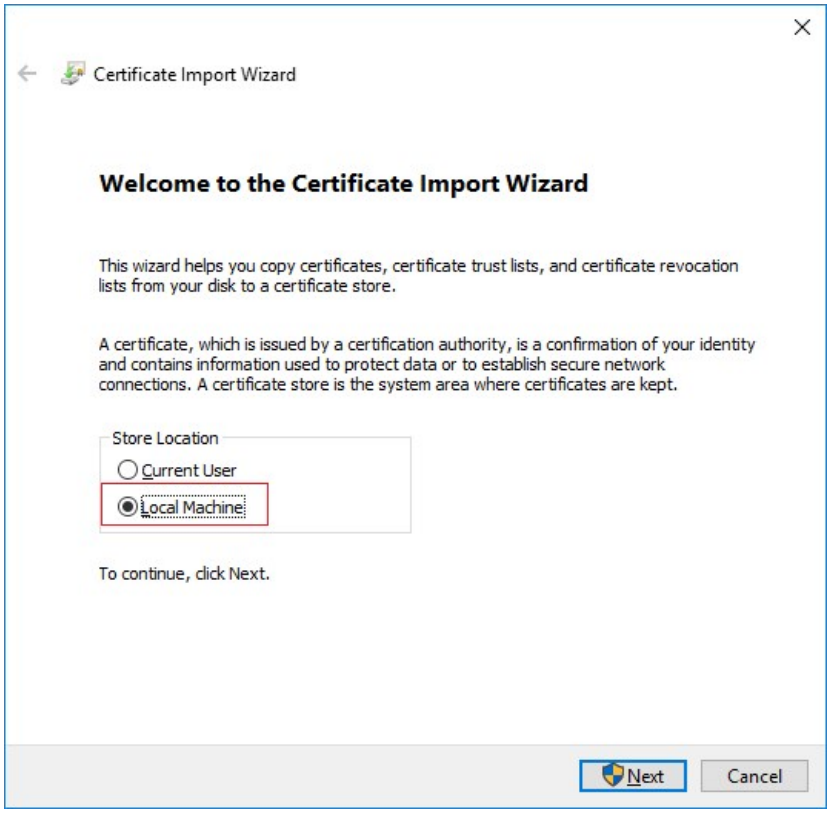
1. Copy the `root-authority-public.cer` file from the computer where you created the CA certificate (`C:\Certificates\root-authority-public.cer`) to the computer where the XProtect client is installed.

For information about which client and server services, and integrations that require the certificate, see Introduction to certificates on page 5.

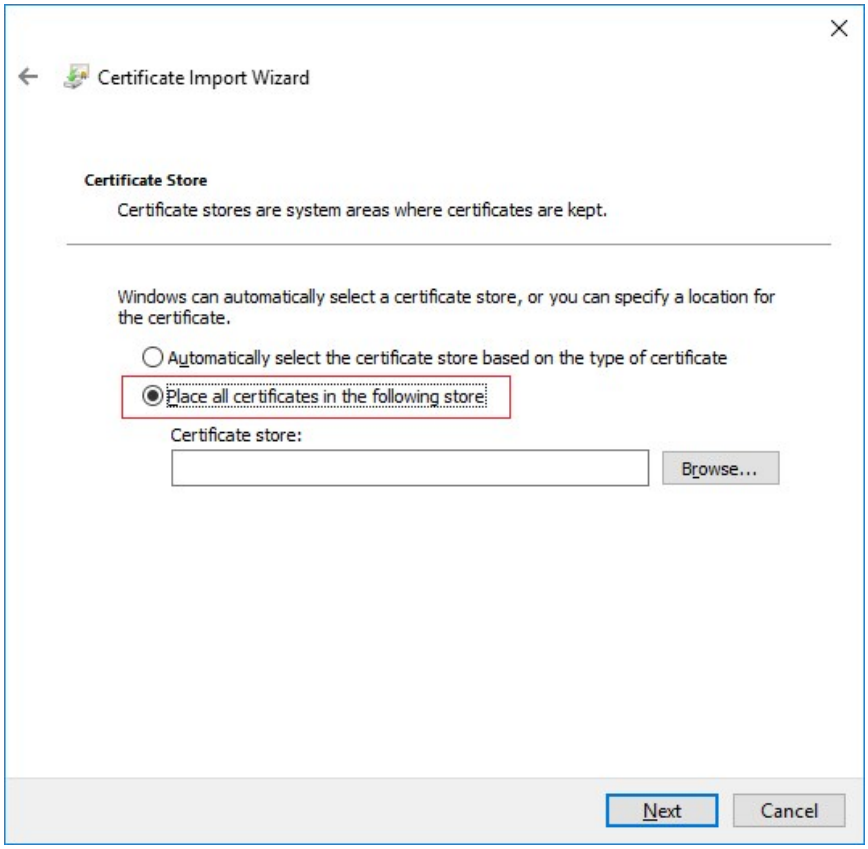
2. Right-click on the certificate and select **Install Certificate**.



3. In the **Certificate Import Wizard**, select to install the certificate in the store of the **Local Machine** and click **Next**.



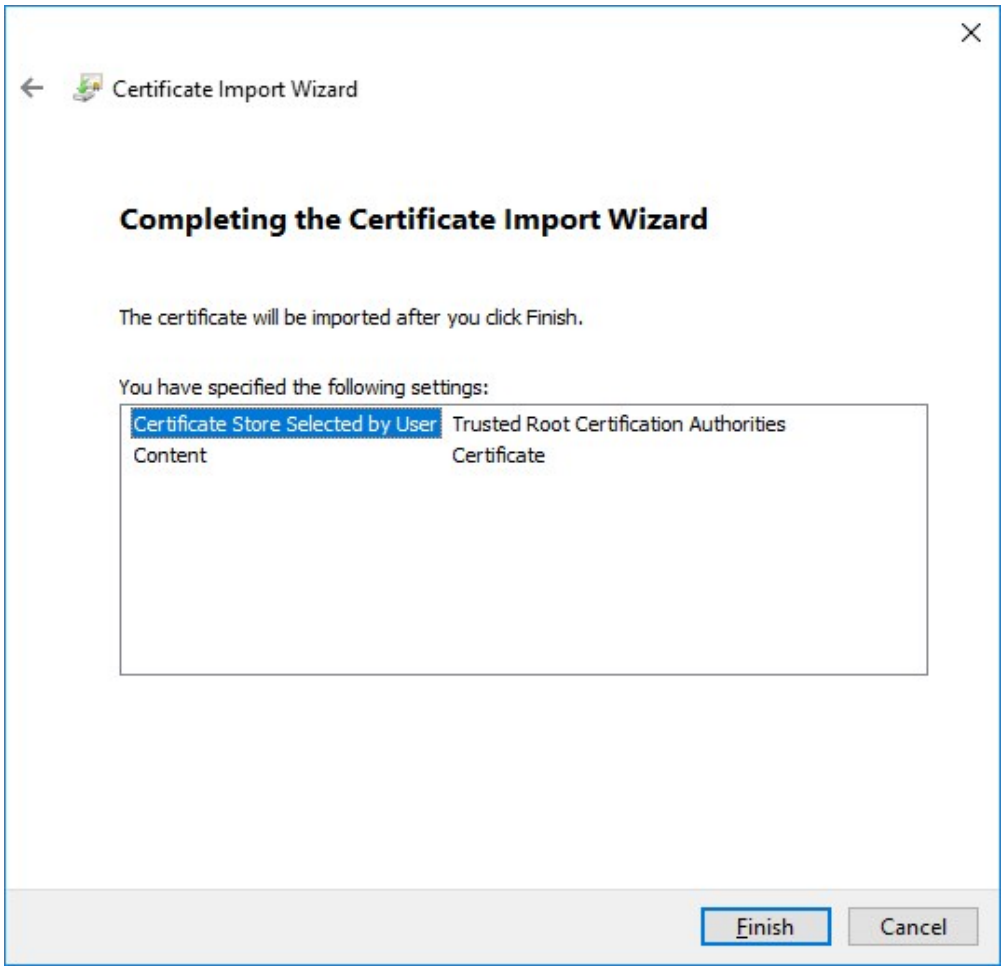
4. Select to manually locate the store in which the certificate will be installed.



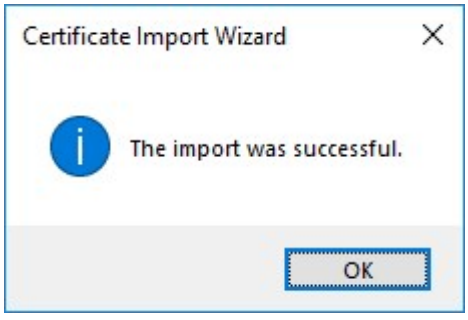
5. Click **Browse**, select **Trusted Root Certification Authorities** and click **OK**. Then click **Next**.

6. On the **Completing the Certificate Import Wizard** dialog, click **Finish**.

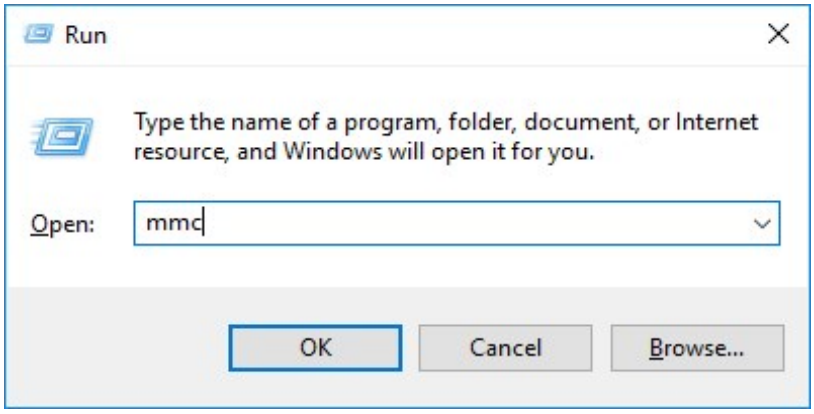
If you receive a security warning that you are about to install a root certificate, click **Yes** to continue.



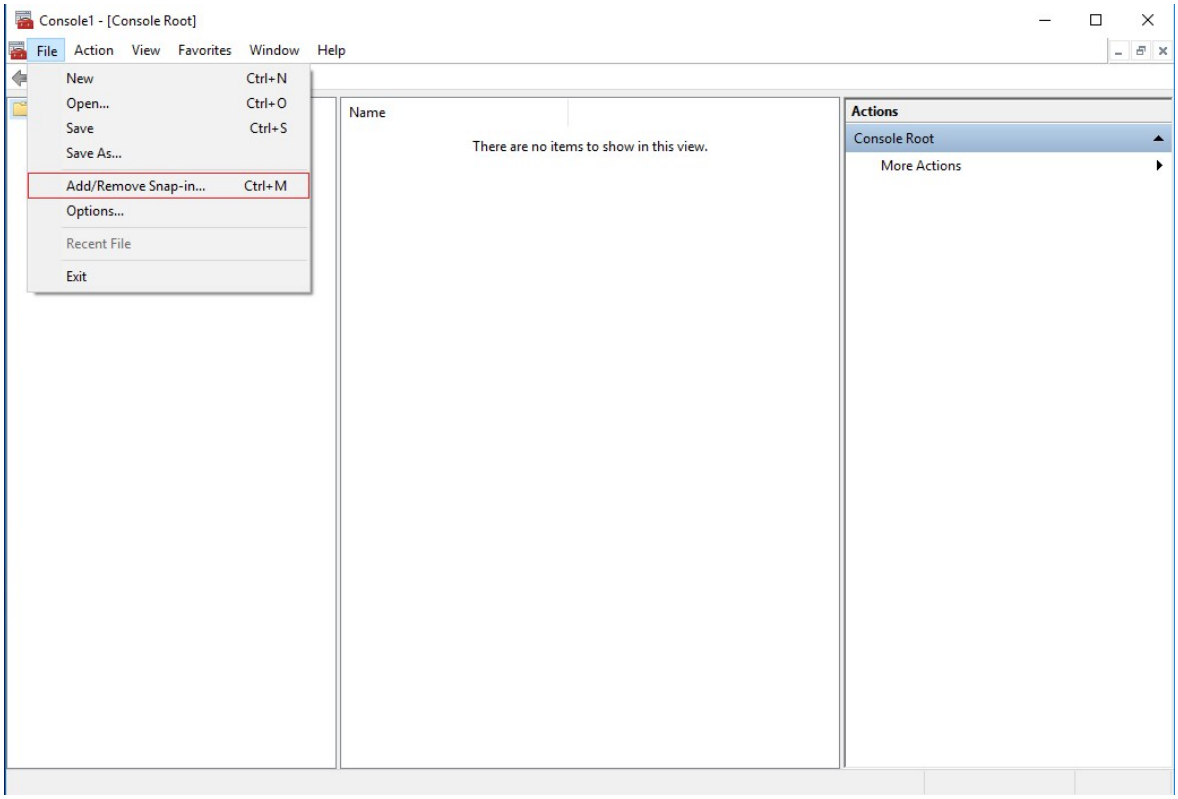
7. You will receive a confirmation dialog of successful import.



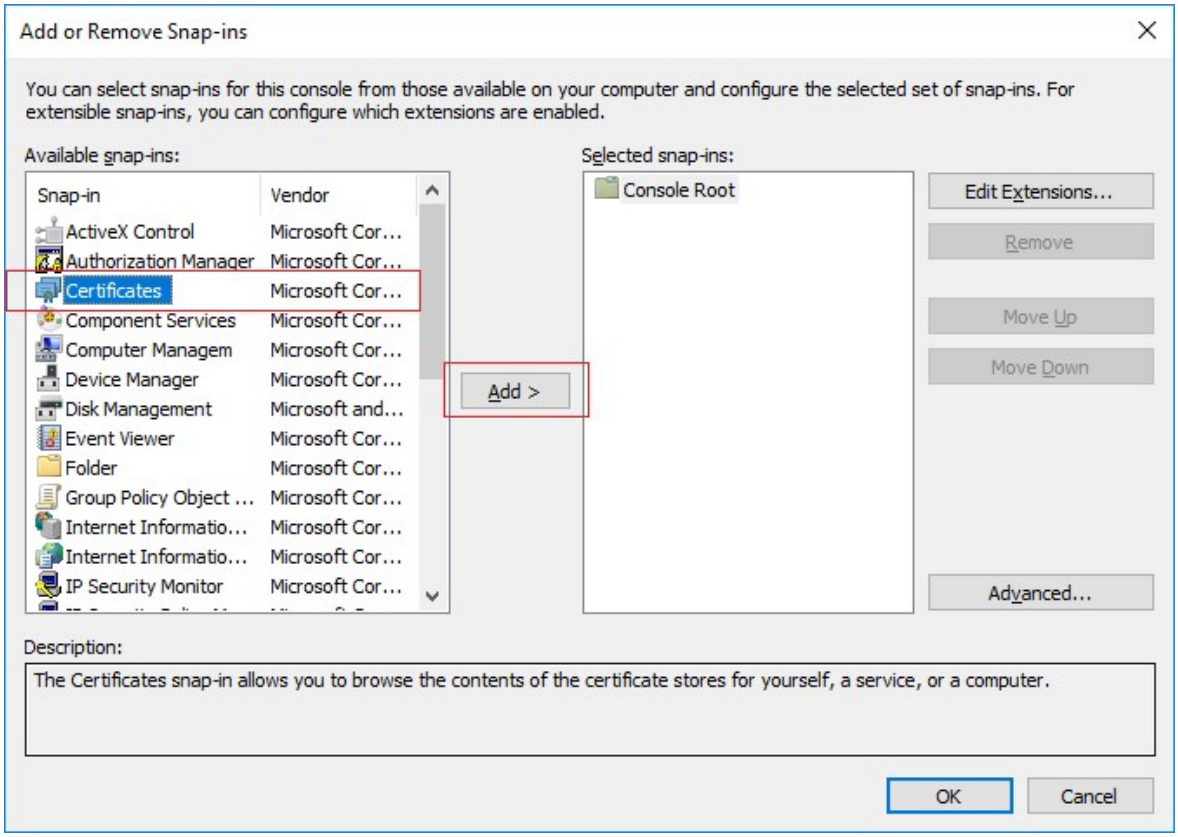
8. To verify that the certificate is imported, start the Microsoft Management Console.



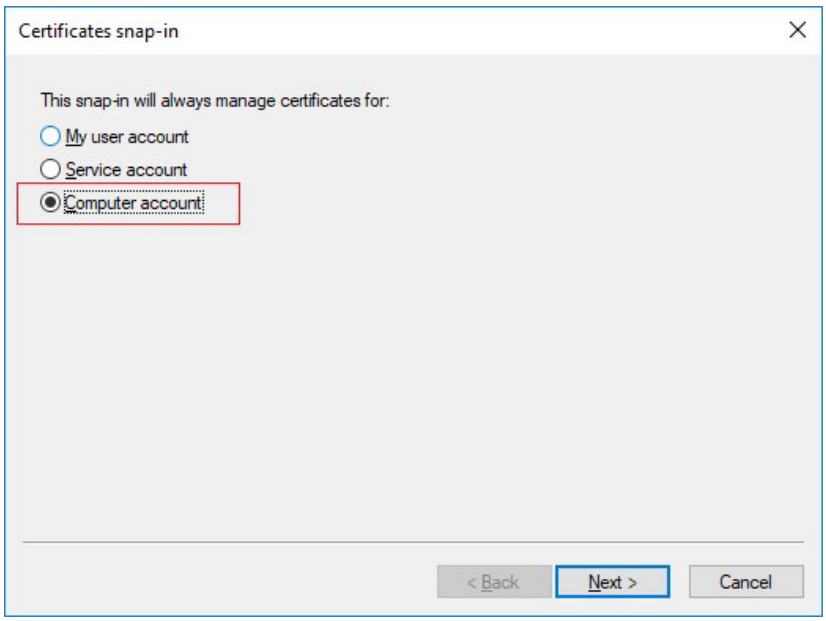
9. In the Microsoft Management Console, from the **File** menu select **Add/Remove Snap-in...**.



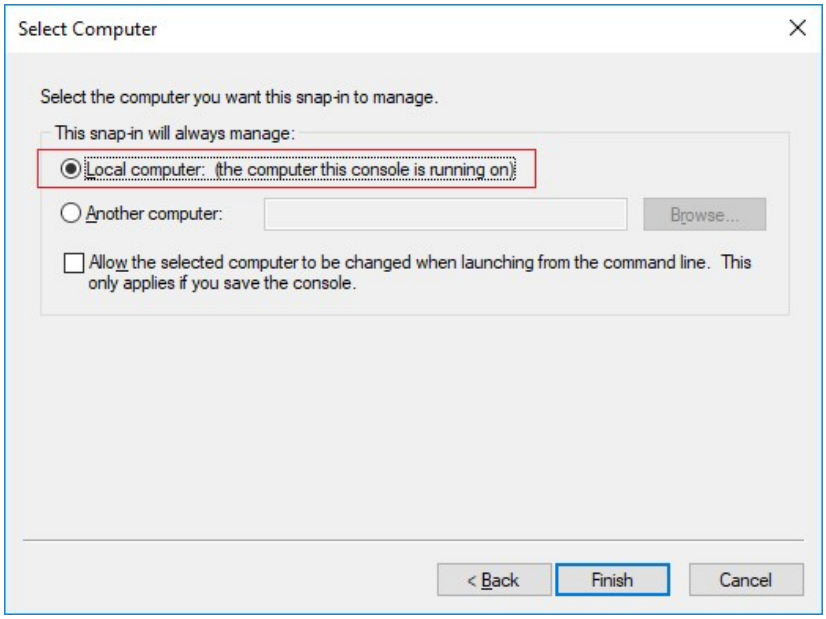
10. Select the **Certificates** snap-in and click **Add**.



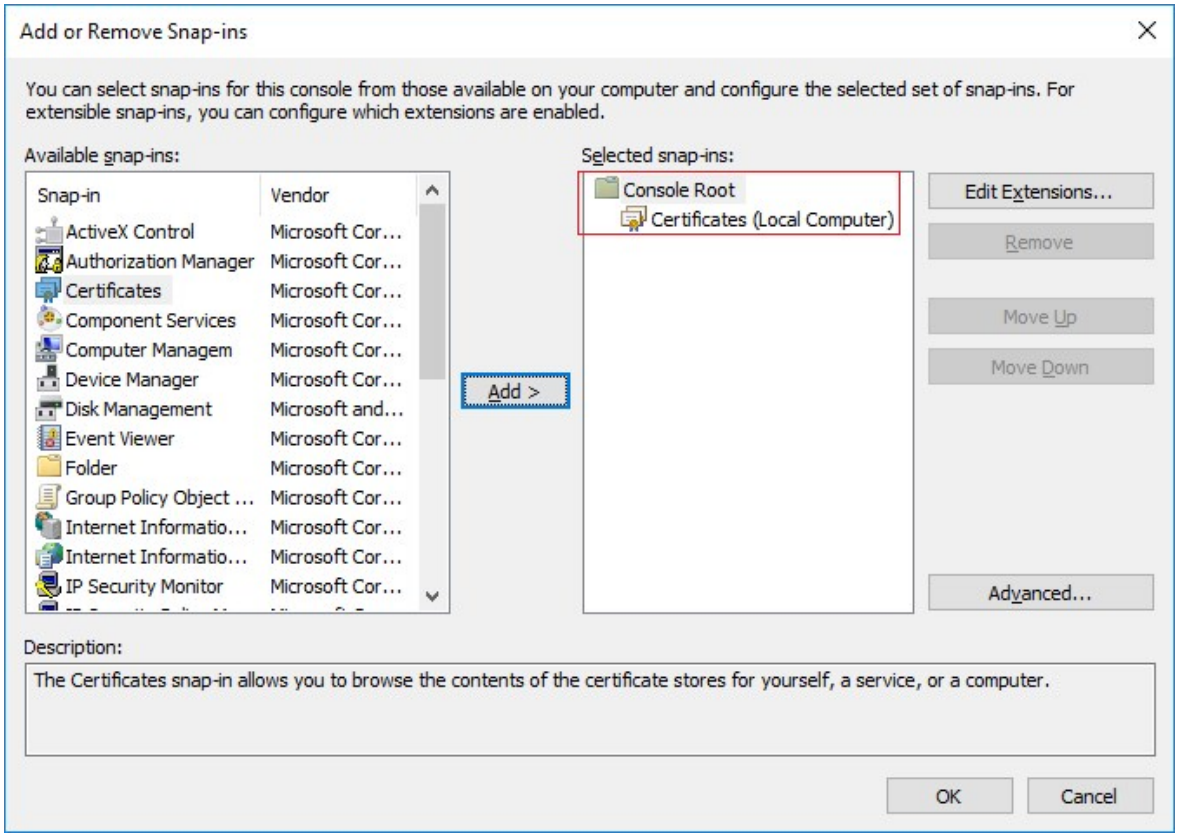
11. Select that the snap-in must manage certificates for the **Computer account**.



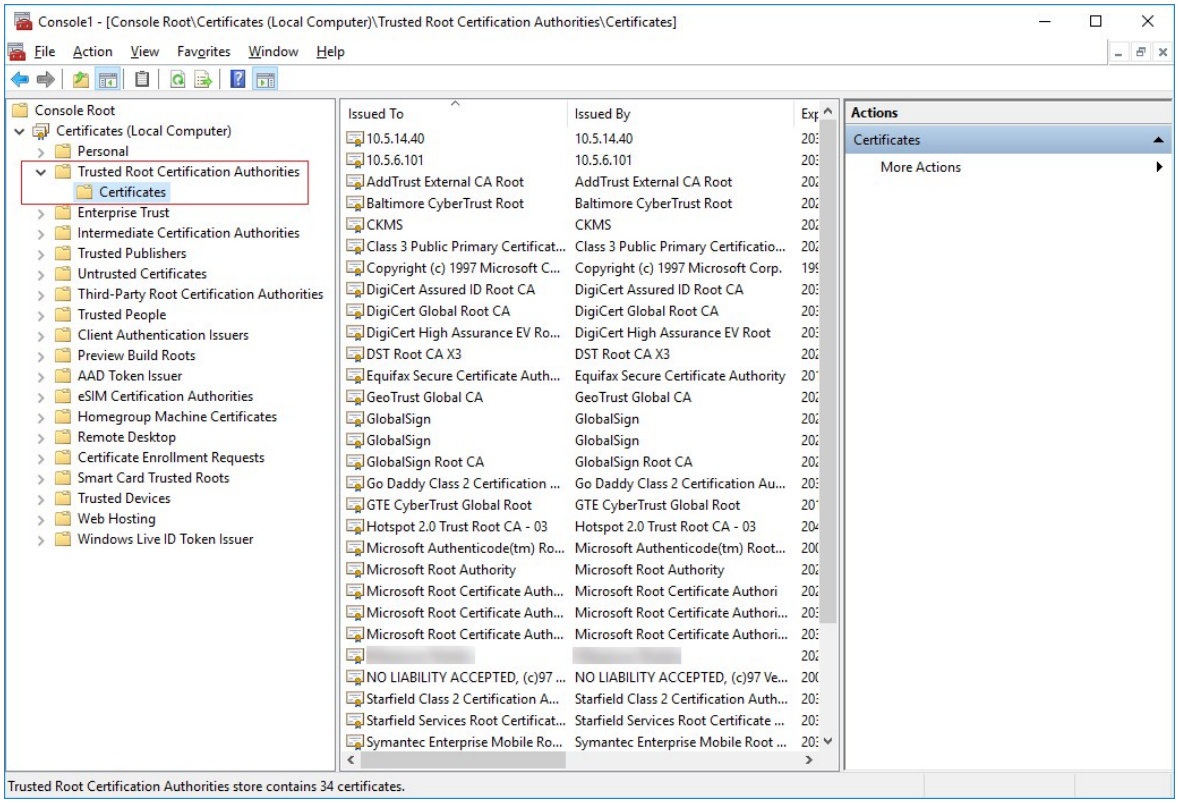
12. Select **Local computer** as the computer that you want the snap-in to manage and click **Finish**.



13. Click **OK** after the snap-in has been added.



14. Verify that the certificate is listed in the center view of the **Trusted Root Certification Authorities** subtree.



15. Repeat the steps on the next computer that runs as a client to the service where encryption is being enabled, until you have installed the certificate on all relevant computers.

Create SSL certificate

After you have installed the CA certificate on all the clients, you are ready to create certificates to be installed on all computers that run servers (recording servers, management servers, mobile servers or failover servers).

If you want to configure a failover management server, you need to create a different SSL certificate. For more information, see Create SSL certificate for the failover management server on page 38.

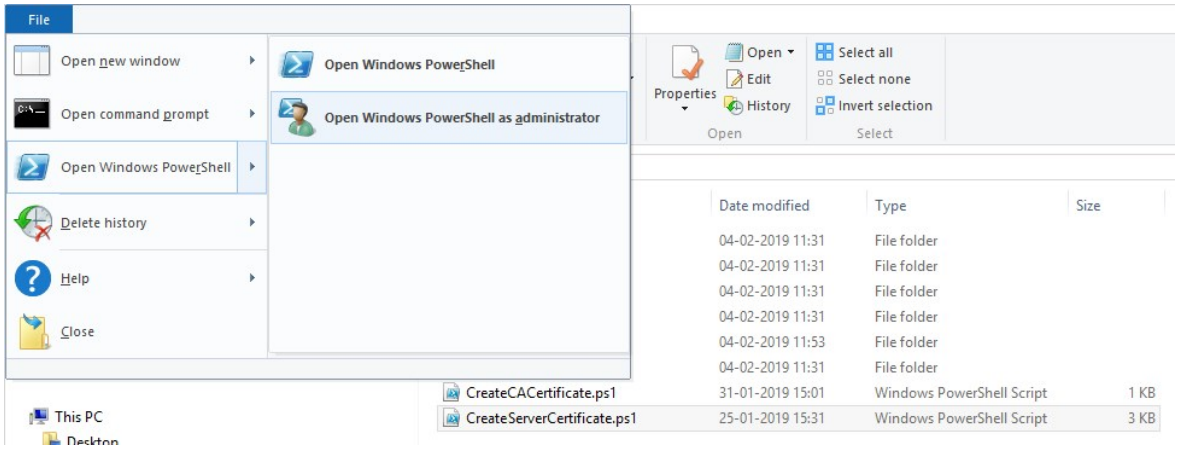
On the computer where you created the CA certificate, from the folder where you placed the CA certificate, run the **Server certificate** script to create SSL certificates for all servers.

The computer that you use for creating certificates must run Window 10 or Windows Server 2016 or newer.

1. In Appendix B in the back of this guide, you find a script for creating server certificates.
2. Open Notepad and paste the contents.

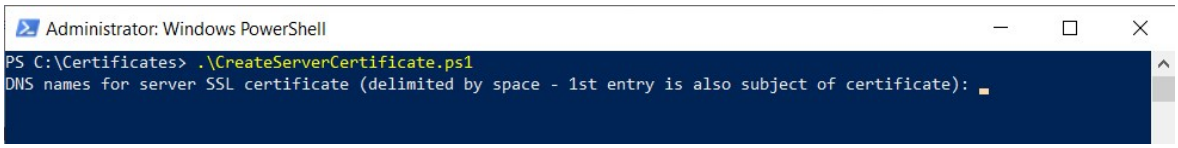
   > It is very important that the lines break in the same places as in Appendix B. You can add the line breaks in Notepad or alternatively, reopen this PDF with Google Chrome, copy the contents again and paste it into Notepad.

3. In Notepad, click **File** -> **Save as**, name the file **CreateServerCertificate.ps1** and save it locally in the same folder as the CA certificate, like this: `C:\Certificates\CreateServerCertificate.ps1`.
4. In File Explorer, go to `C:\Certificates` and select the **CreateServerCertificate.ps1** file.
5. In the **File** menu, select **Open Windows PowerShell** and then **Open Windows PowerShell as administrator**.



6. In PowerShell at the prompt, enter **.\CreateServerCertificate.ps1** and press **Enter**.
7. Enter the DNS name for the server. If the server has multiple names, for example for internal and external use, add them here, separated by a space. Press **Enter**.

   > To find the DNS name, open File explorer on the computer running the Recording Server service. Right-click **This PC** and select **Properties**. Use the **Full computer name**.



8. Enter the IP address of the server. If the server has multiple IP addresses, for example for internal and external use, add them here, separated by a space. Press **Enter**.

   To find the IP address, you can open Command Prompt on the computer running the Recording Server service. Enter **ipconfig /all**. If you have installed the XProtect system, you can open the Management Client, navigate to the server and find the IP address on the **Info** tab.

9. Specify a password for the certificate and press **Enter** to finish the creation.

   You use this password when you import the certificate on the server.

   A `Subjectname.pfx` file appears in the folder where you ran the script.

10. Run the script until you have certificates for all of your servers.

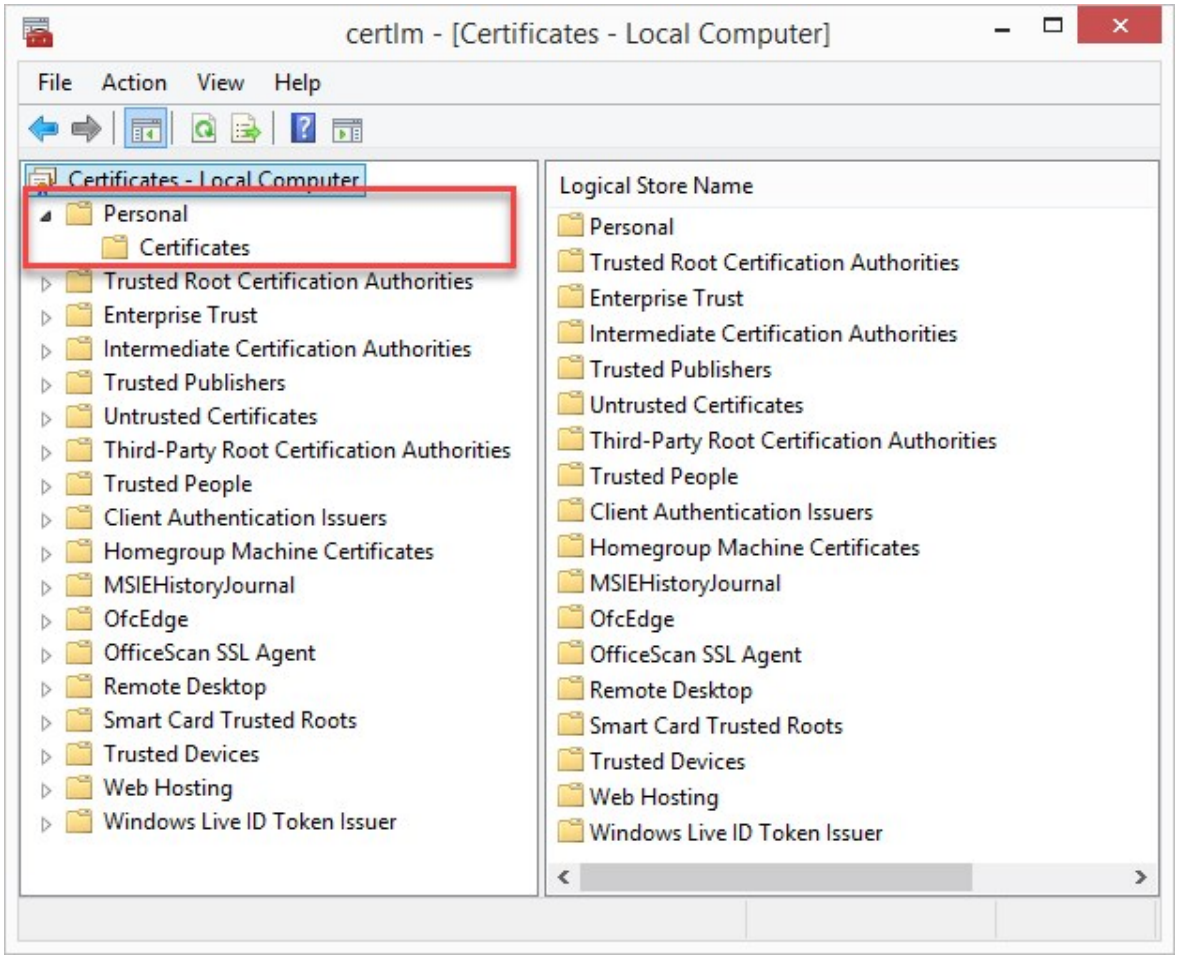
Import SSL certificate

After you created the SSL certificates, install them on the computers that run the server service.

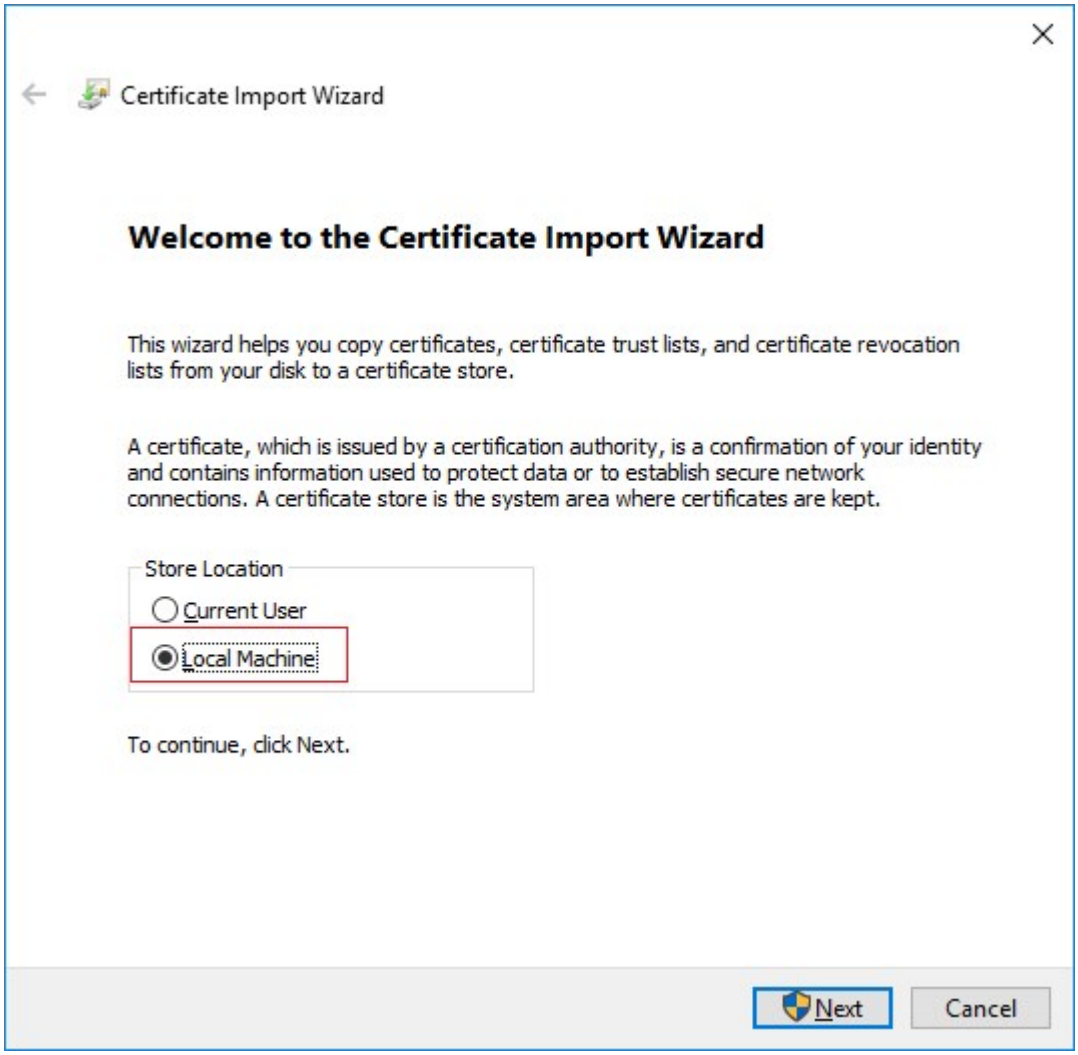
1. Copy the relevant `Subjectname.pfx` file from the computer where you created the certificate to the corresponding server service computer.

   Remember that each certificate is created to a specific server.

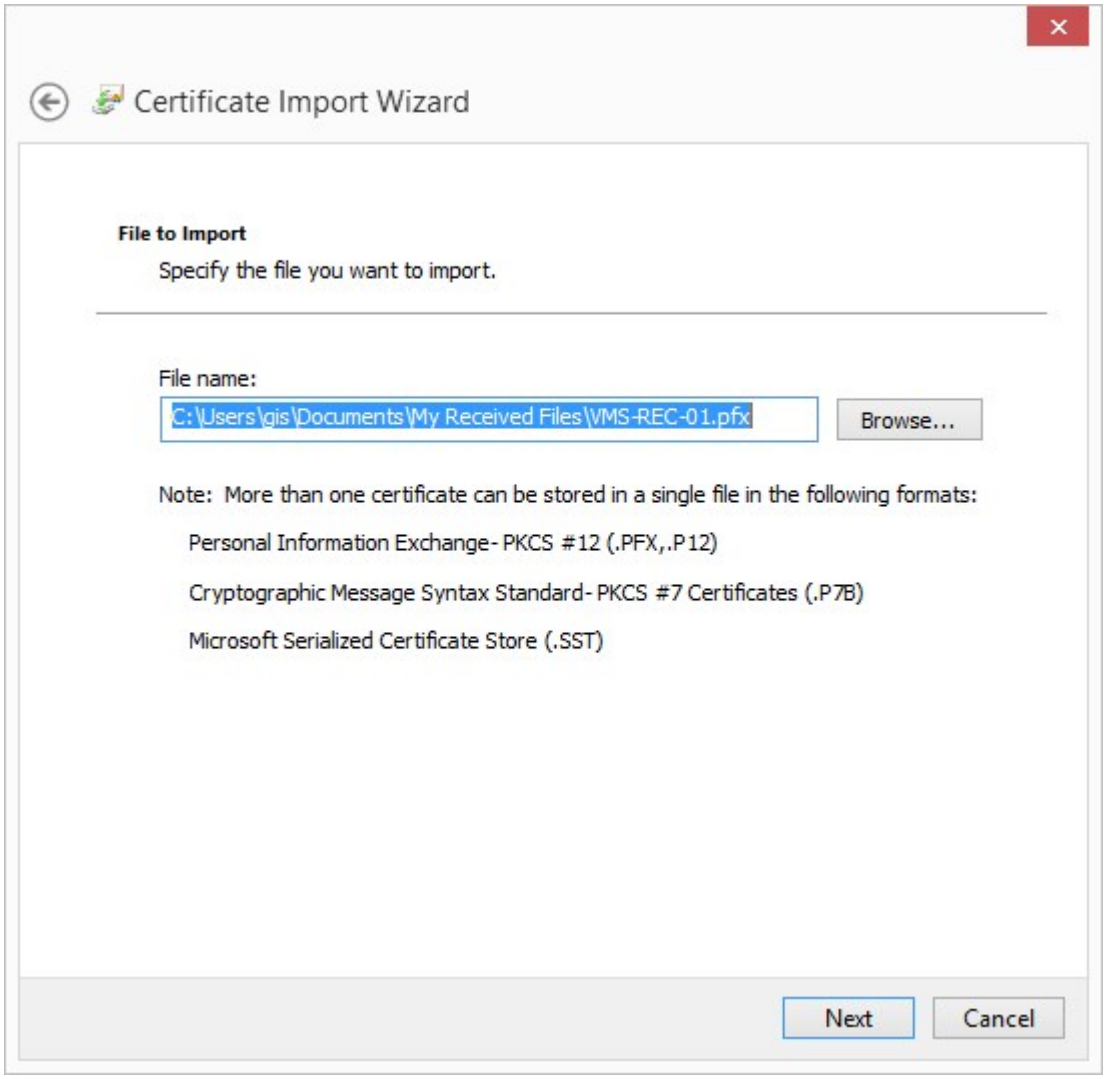
2. On the server service computer, start **Manage computer certificates**.
3. Click on **Personal**, right-click **Certificates** and select **All Tasks** > **Import**.



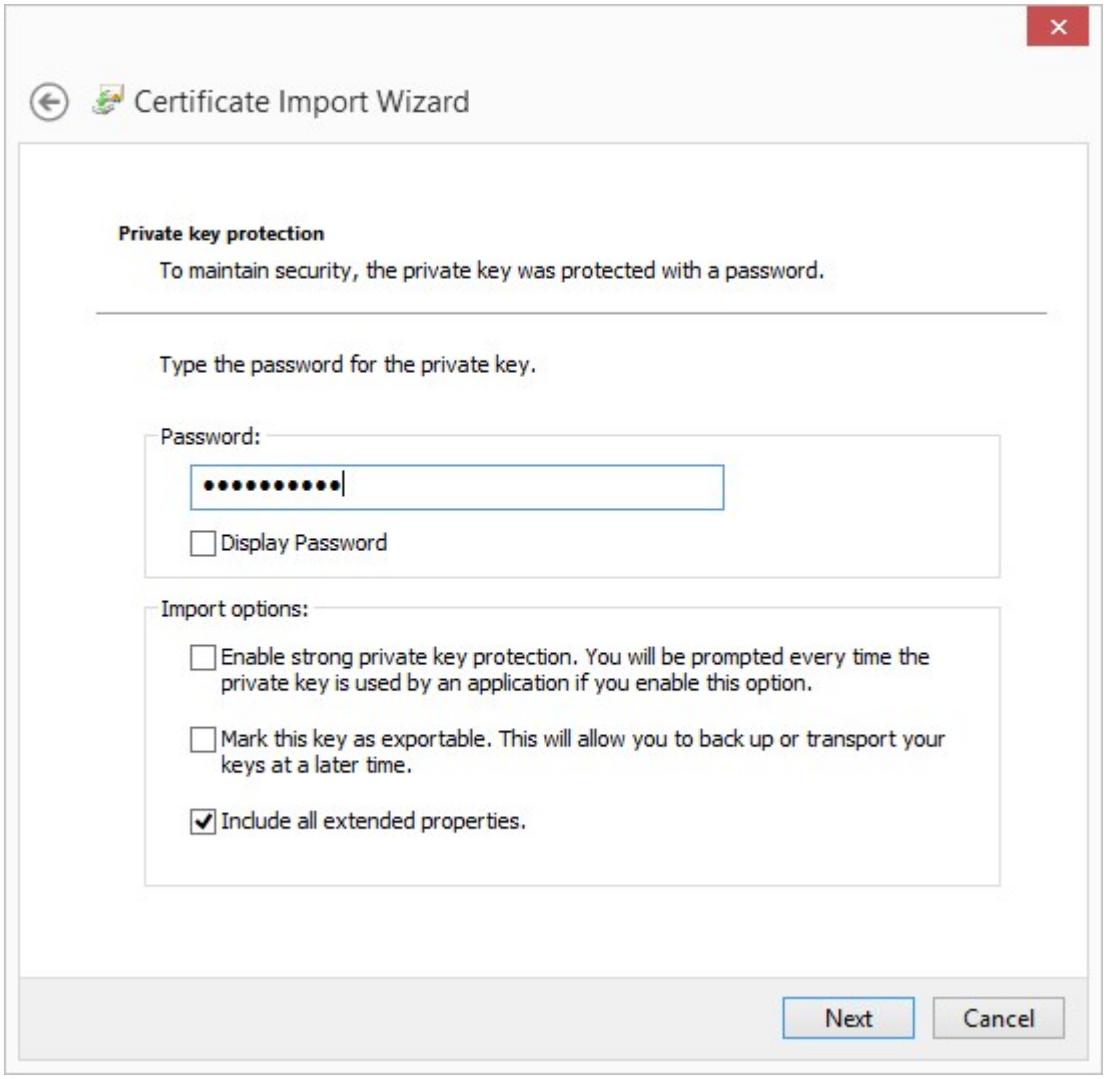
4. Select to import the certificate in the store of the **Local Machine** and click **Next**.



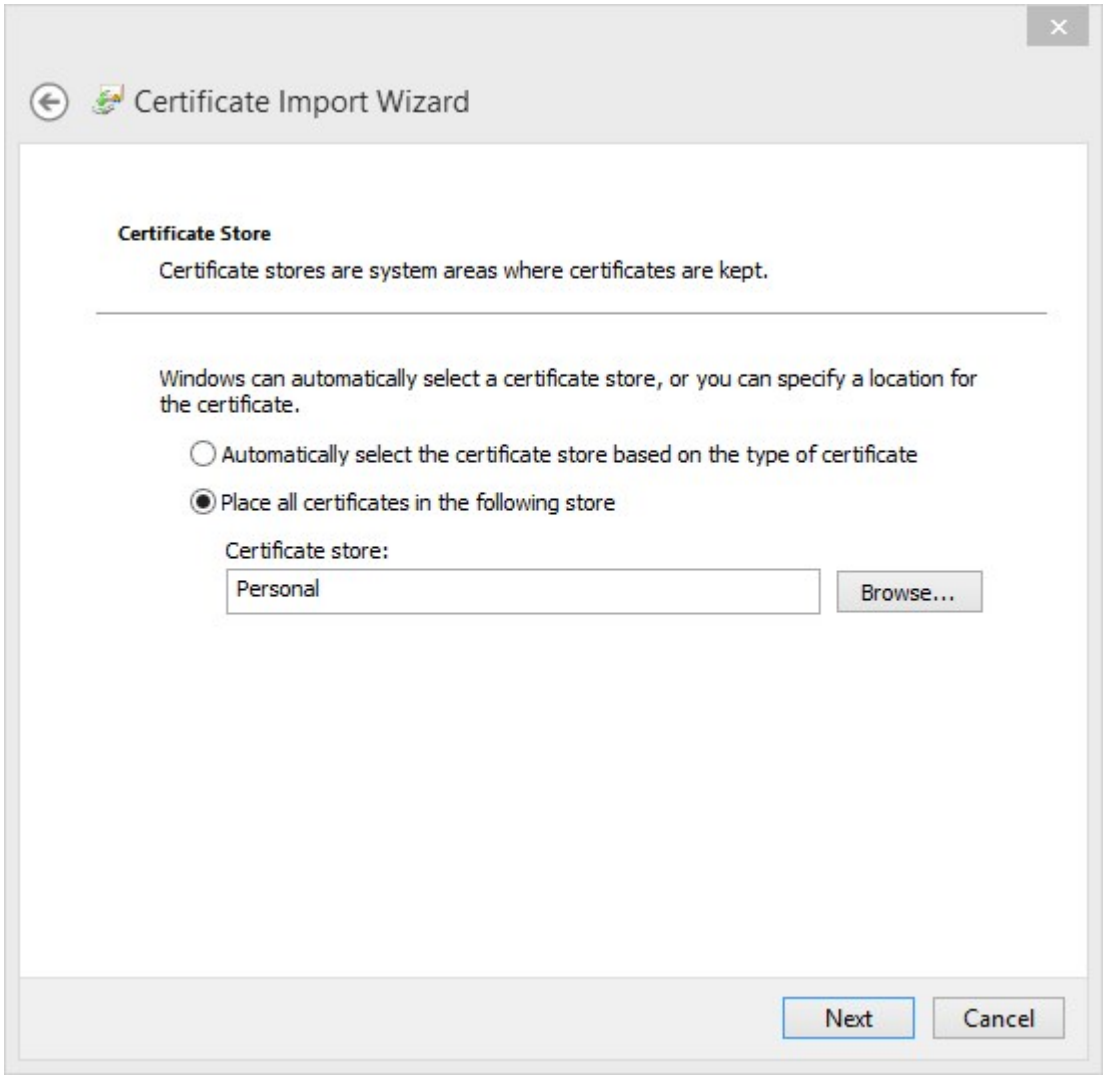
5. Browse to the certificate file and click **Next**.



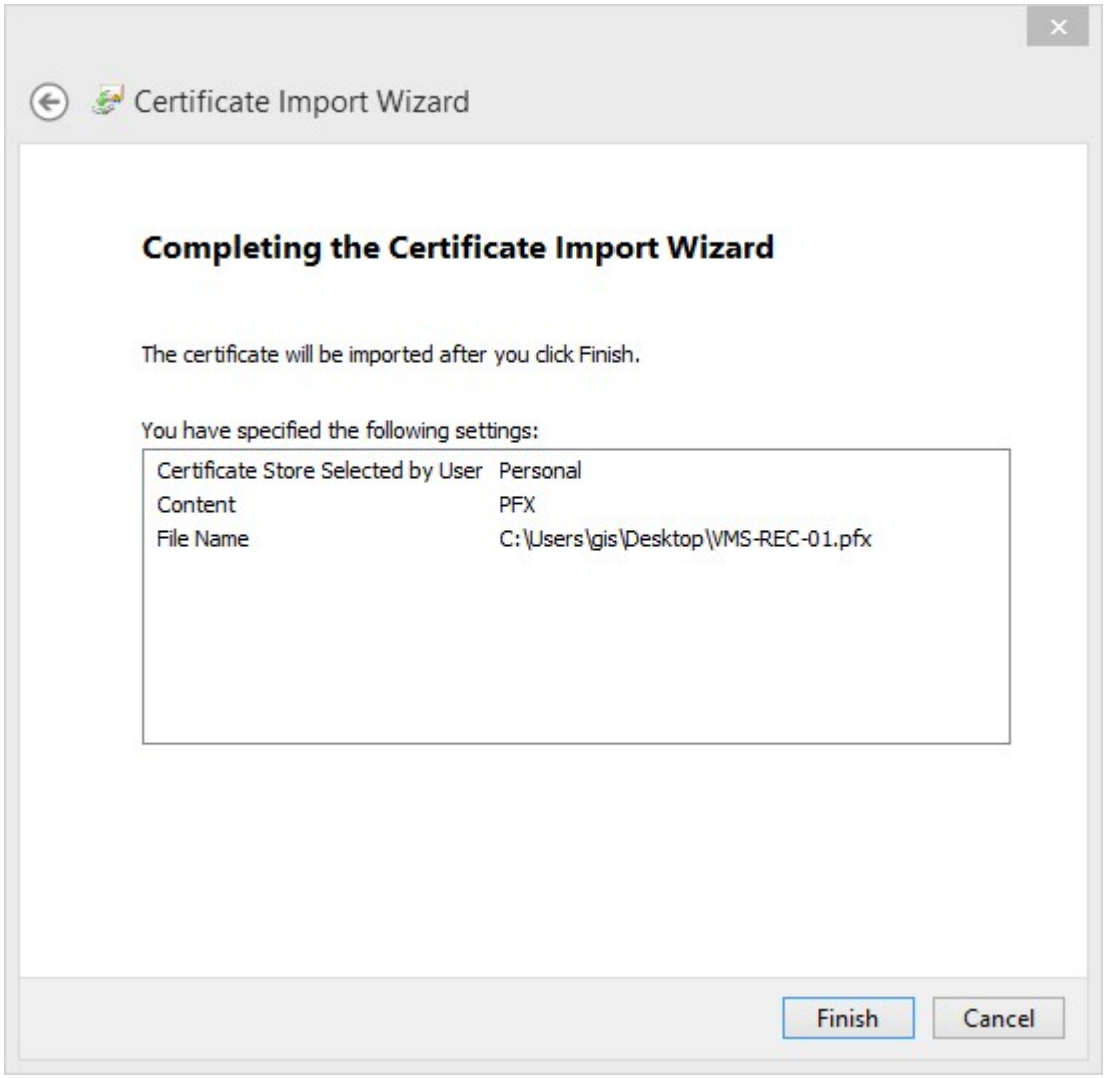
6. Enter the password for the private key that you specified when you created the server certificate, and click **Next**.



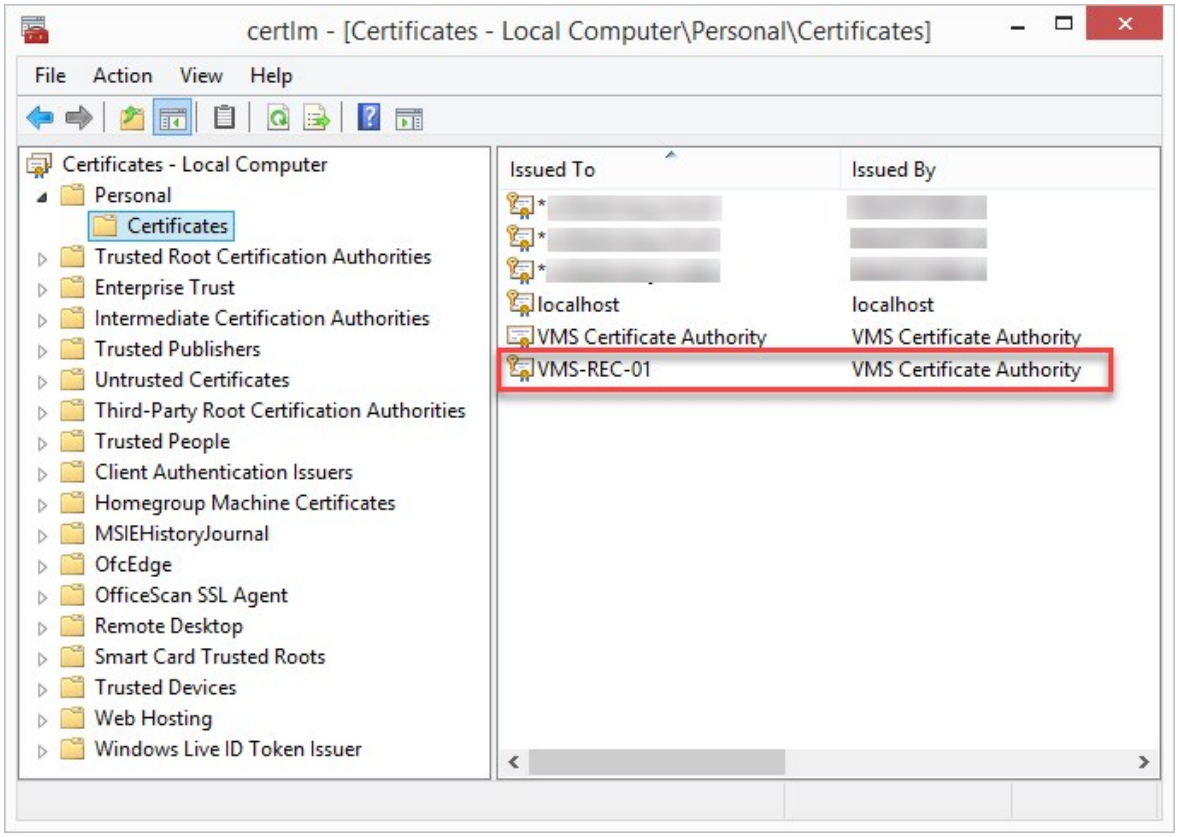
7. Place the file in the **Certificate Store**: **Personal** and click **Next**.



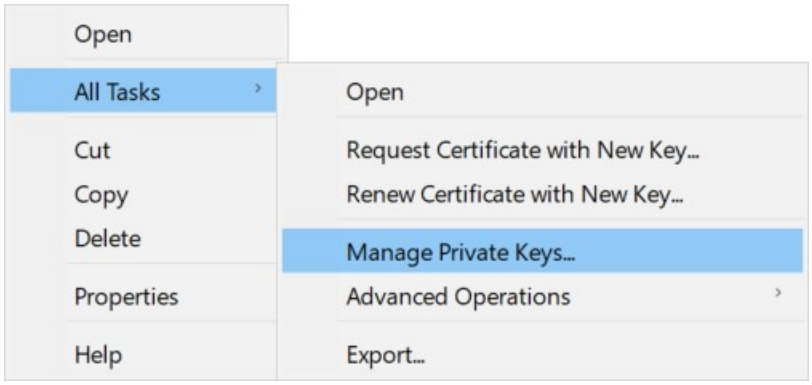
8. Verify the information and click **Finish** to import the certificate.



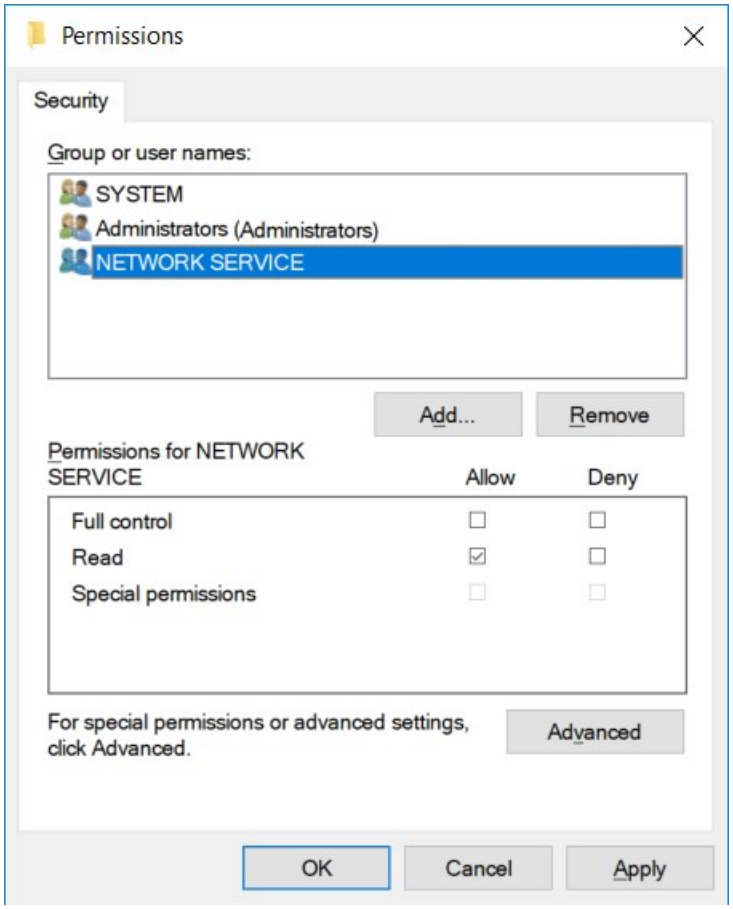
9. The imported certificate appears in the list.



10. To allow a service to use the private key of the certificate, right click the certificate and select **All Tasks** > **Manage Private Keys**.



11. Add read permission for the user running the XProtect VMS services that need to use the server certificate.



12. Continue to the next computer, until you have installed all server certificates.

Create SSL certificate for the failover management server

XProtect Management Server Failover is configured on two computers. To make sure that the clients trust the running management server, install the SSL certificate on the primary and the secondary computer.

To create and install the SSL certificate for the failover cluster, you need to install the CA certificate first.

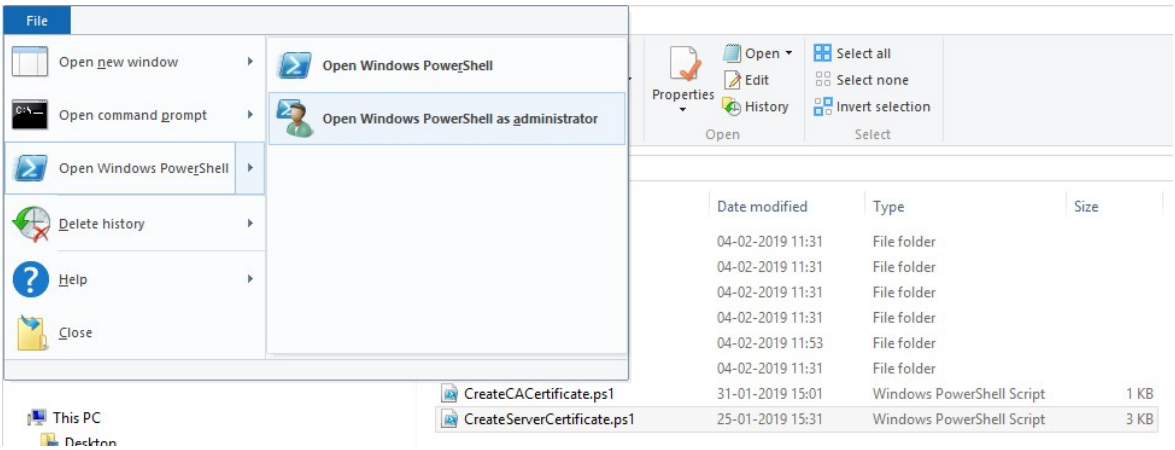
On the computer where you created the CA certificate, from the folder where you placed the CA certificate, run the **Failover management server certificate** script to create an SSL certificate for the primary and the secondary computer.

> The computer that you use for creating certificates must run Window 10 or Windows Server 2016 or newer.

1. In Appendix C of this guide, copy the script for creating failover management server certificates.
2. Open Notepad and paste the script.

   > It is very important that the lines break in the same places as shown in Appendix C. You can add the line breaks in Notepad or alternatively, reopen this PDF with Google Chrome, copy the contents again and paste it into Notepad.

3. In Notepad, select **File** -> **Save as**, name the file **CreateFailoverCertificate.ps1** and save it locally in the same folder as the CA certificate:
   Example: `C:\Certificates\CreateFailoverCertificate.ps1`.
4. In File Explorer, go to `C:\Certificates` and select the **CreateFailoverCertificate.ps1** file.
5. In the **File** menu, select **Open Windows Powershell** and then **Open Windows PowerShell as administrator**.



6. In PowerShell, enter **.\CreateFailoverCertificate.ps1** at the prompt and press **Enter**.

7. Specify the FQDNs and the host names for the primary and the secondary computer, separated by a comma.

   Example: pc1host,pc1host.domain,pc2host,pc2host.domain.

   Press **Enter**.

8. Specify the virtual IP address of the failover cluster. Press **Enter**.
9. Specify a password for the certificate and press **Enter** to finish the creation.

   You use this password when you import the certificate on the server.

   The `[virtualIP].pfx` file appears in the folder where you ran the script.

Import the certificate the same way you would import an SSL certificate, see Import SSL certificate on page 29. Import the certificate on the primary and secondary computers.

Install certificates for communication with the mobile server

To use an HTTPS protocol for establishing a secure connection between the mobile server and clients and services, you must apply a valid certificate on the server. The certificate confirms that the certificate holder is authorized to establish secure connections.

Encryption is enabled or disabled per mobile server. You enable or disable encryption either during installation of the XProtect VMS product or by using the Server Configurator. When you enable encryption on a mobile server, you then use encrypted communication with all clients, services, and integrations that retrieve data streams.

When you configure encryption for a server group, it must either be enabled with a certificate belonging to the same CA certificate or, if the encryption is disabled, then it must be disabled on all computers in the server group.

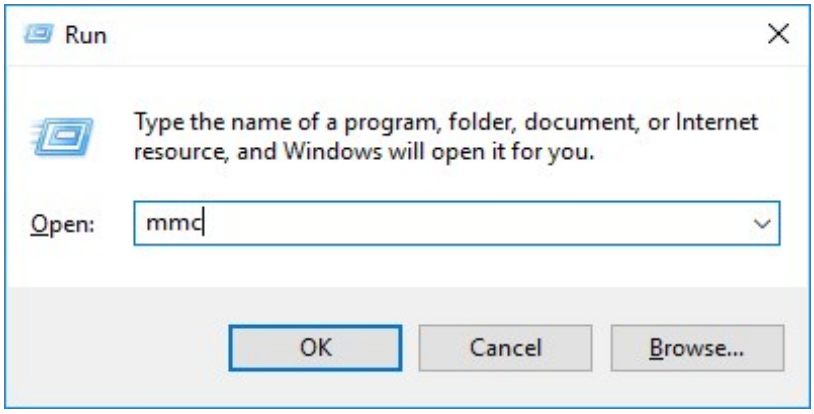
Certificates issued by CA (Certificate Authority) have a chain of certificates and on the root of that chain is the CA root certificate. When a device or browser sees this certificate, it compares its root certificate with pre-installed ones on the OS (Android, iOS, Windows, etc.). If the root certificate is listed in the pre-installed certificates list, then the OS ensures the user that the connection to the server is secure enough. These certificates are issued for a domain name and are not free of charge.

Add a CA certificate to the server

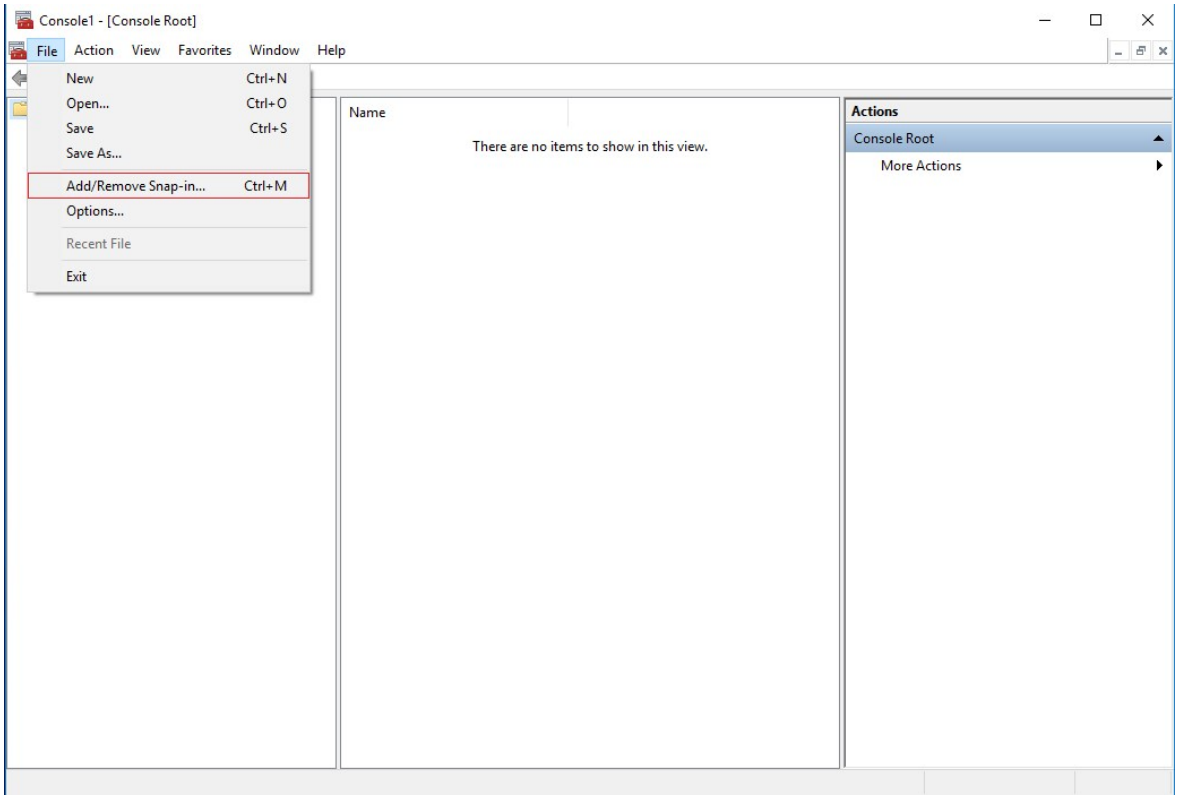
Add the CA certificate to the Mobile Server by doing the following.

Specific parameters depend on the CA. Refer to the documentation of your CA before proceeding.

1. On the computer that hosts the Mobile Server, open the Microsoft Management Console.

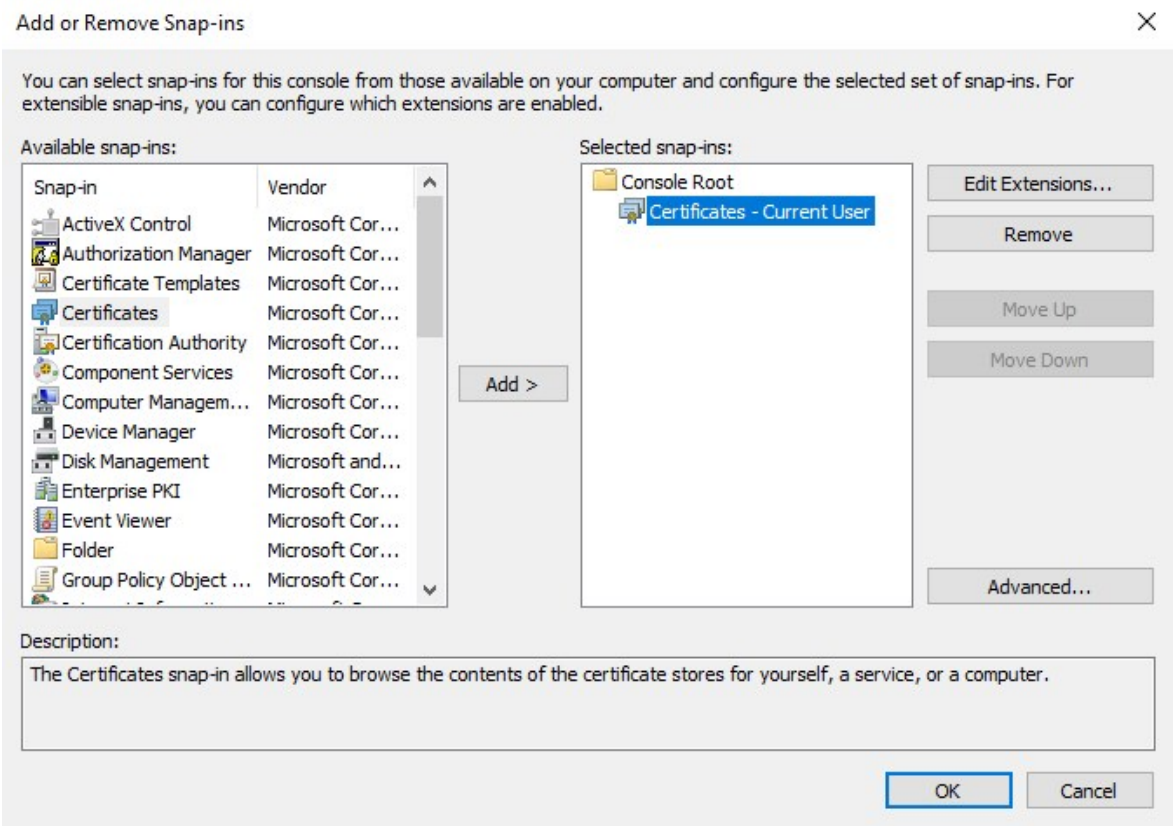


2. In the Microsoft Management Console, from the **File** menu select **Add/Remove Snap-in...**.

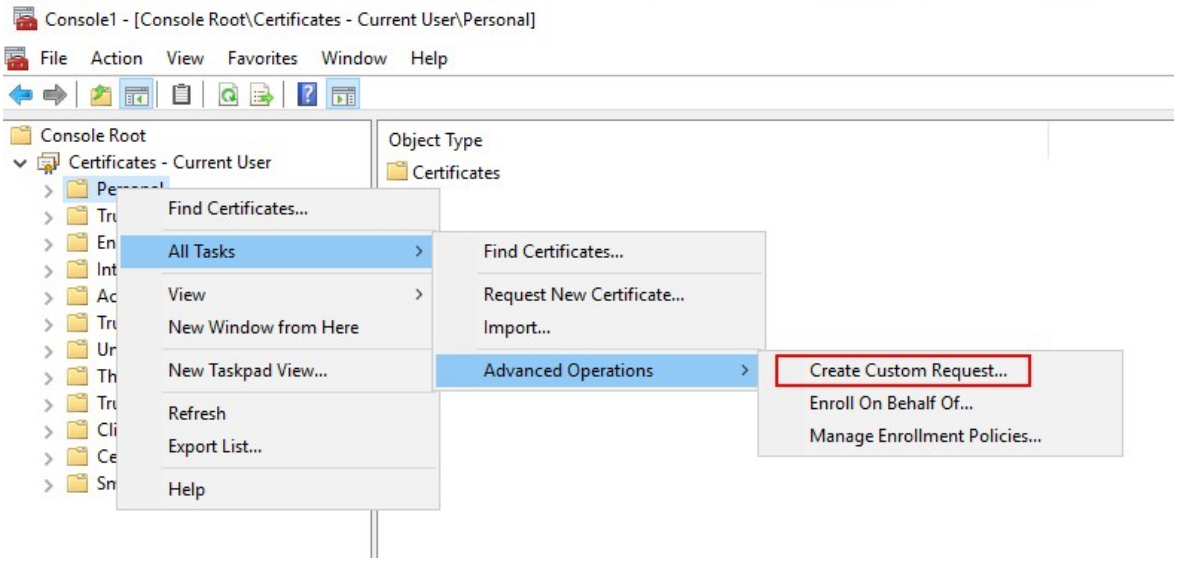


3. Select the **Certificates** snap-in and click **Add**.

   Click **OK**.

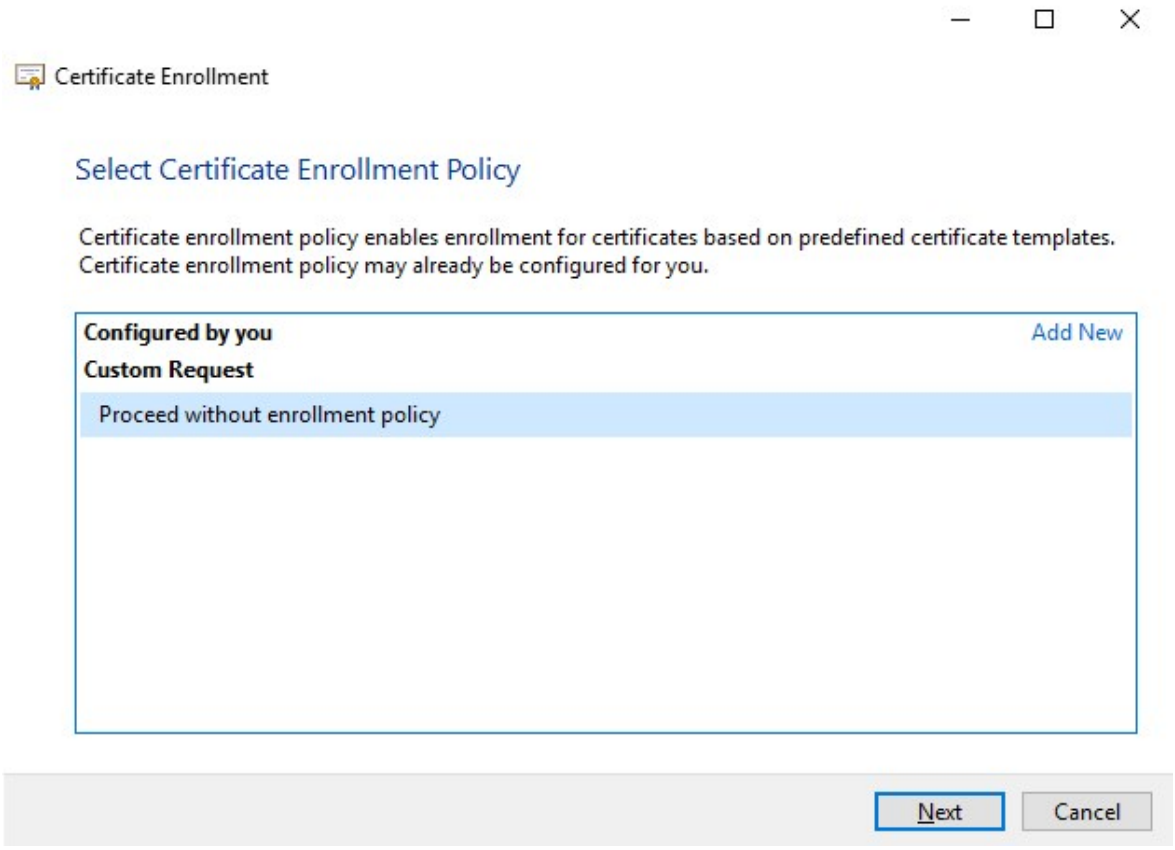


4. Expand the Certificates object. Right-click on the **Personal** folder and select **All Tasks** > **Advanced Operations** > **Create Custom Request**.

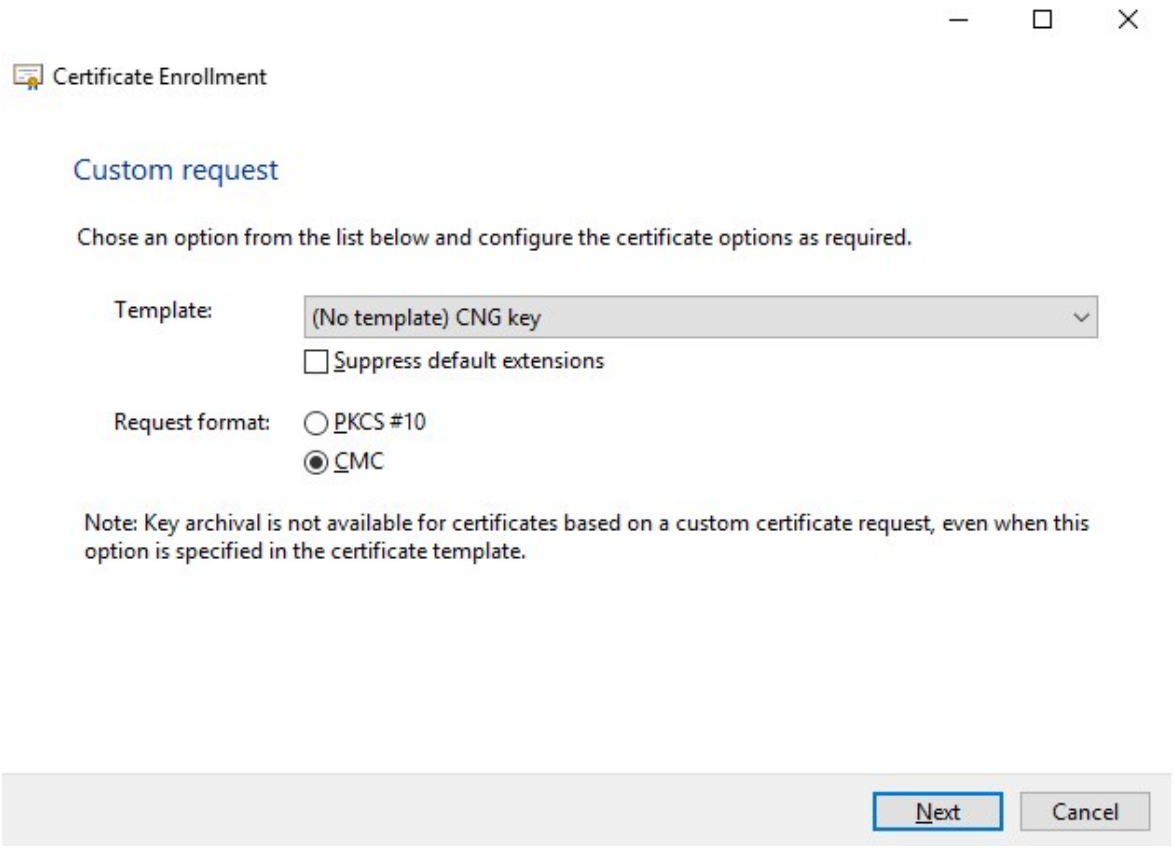


5. Click **Next** in the **Certificate Enrollment** wizard and select **Proceed without enrollment policy**.

   Click **Next**.



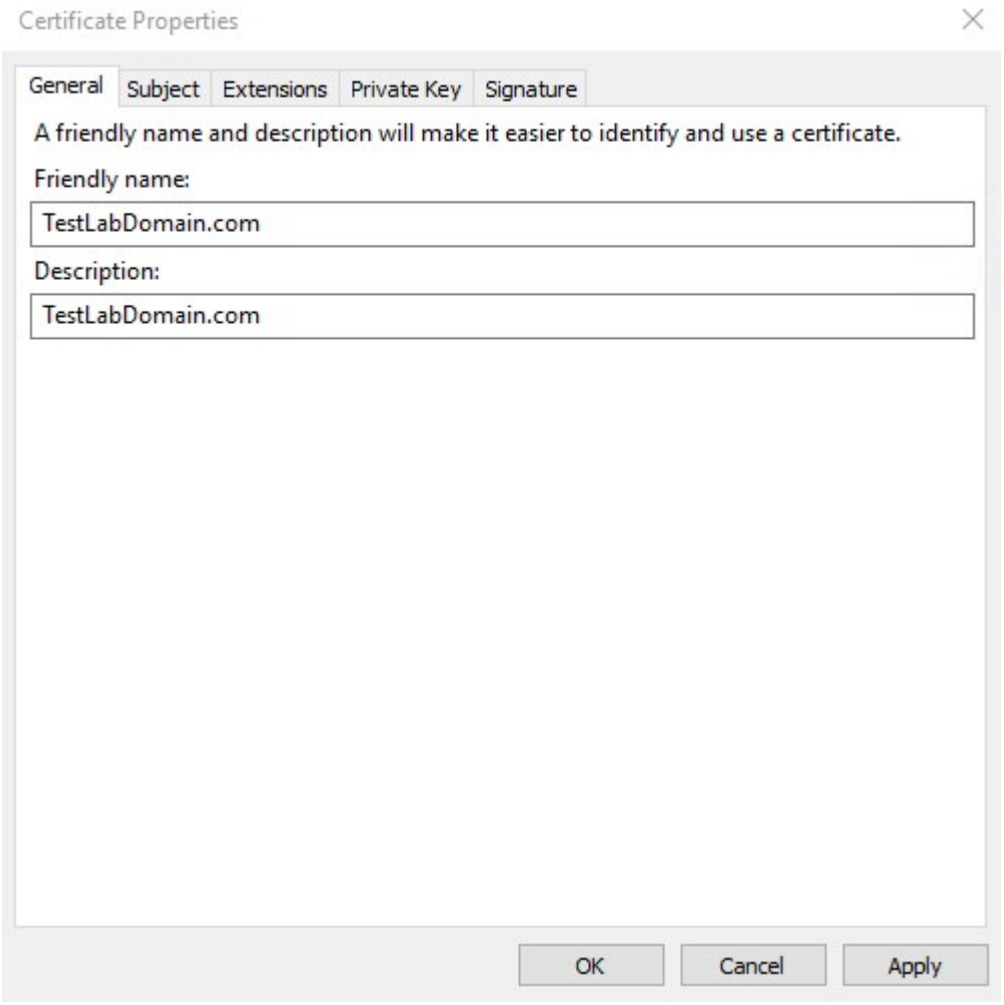
6. Select the **(No template) CNG Key** template and the **CMC** request format, and click **Next**.



The request format depends on the CA. If the wrong format is chosen, the CA will issue an error when the certificate signing request (CSR) is submitted. Check with the CA to make sure you choose properly.

7. Expand to view the **Details** of the custom request, and click **Properties**.

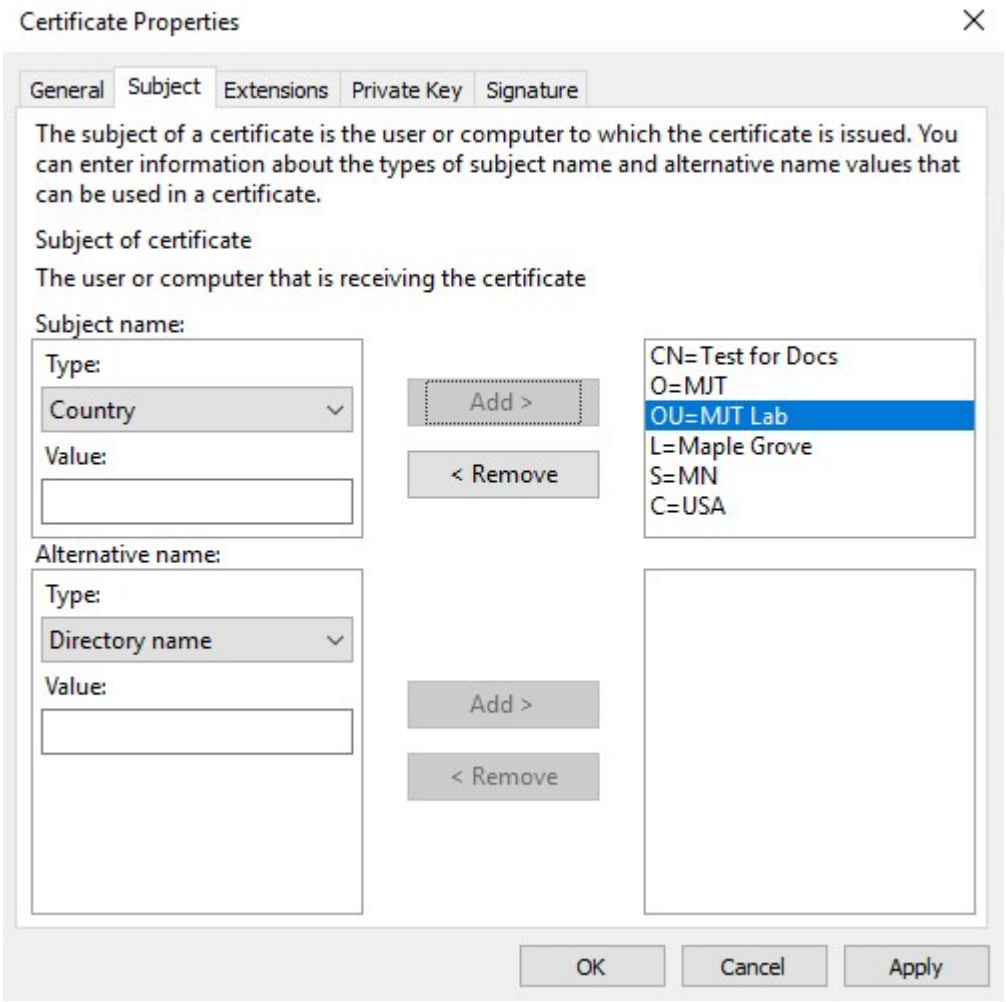
8. On the **General** tab, fill in the **Friendly name** and **Description** fields with the domain name registered with the CA.



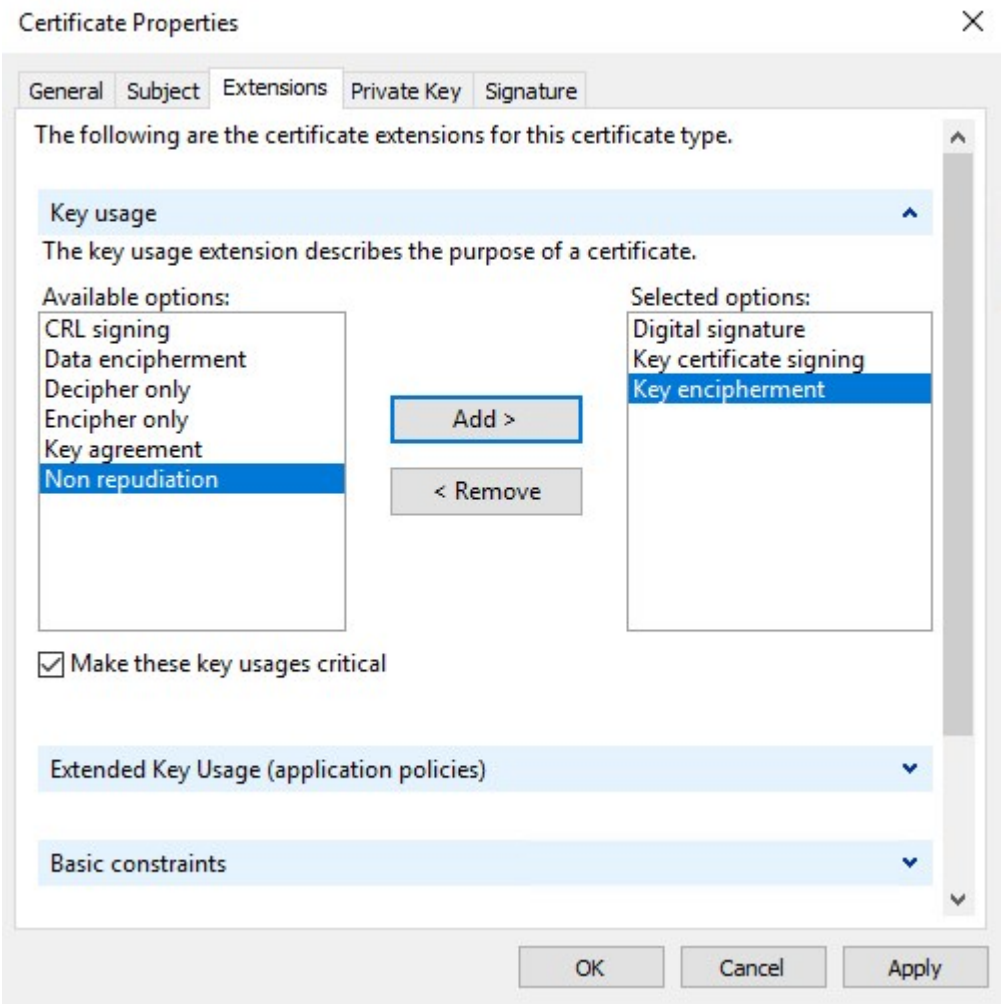
9. On the **Subject** tab, enter the parameters as required by the specific CA.

   For example, the subject name **Type** and **Value** are different for each CA. One example is the following required information:

   - Common Name:
   - Organization:
   - Organizational Unit:
   - City/Locality:
   - State/Province:
   - Country/Region:



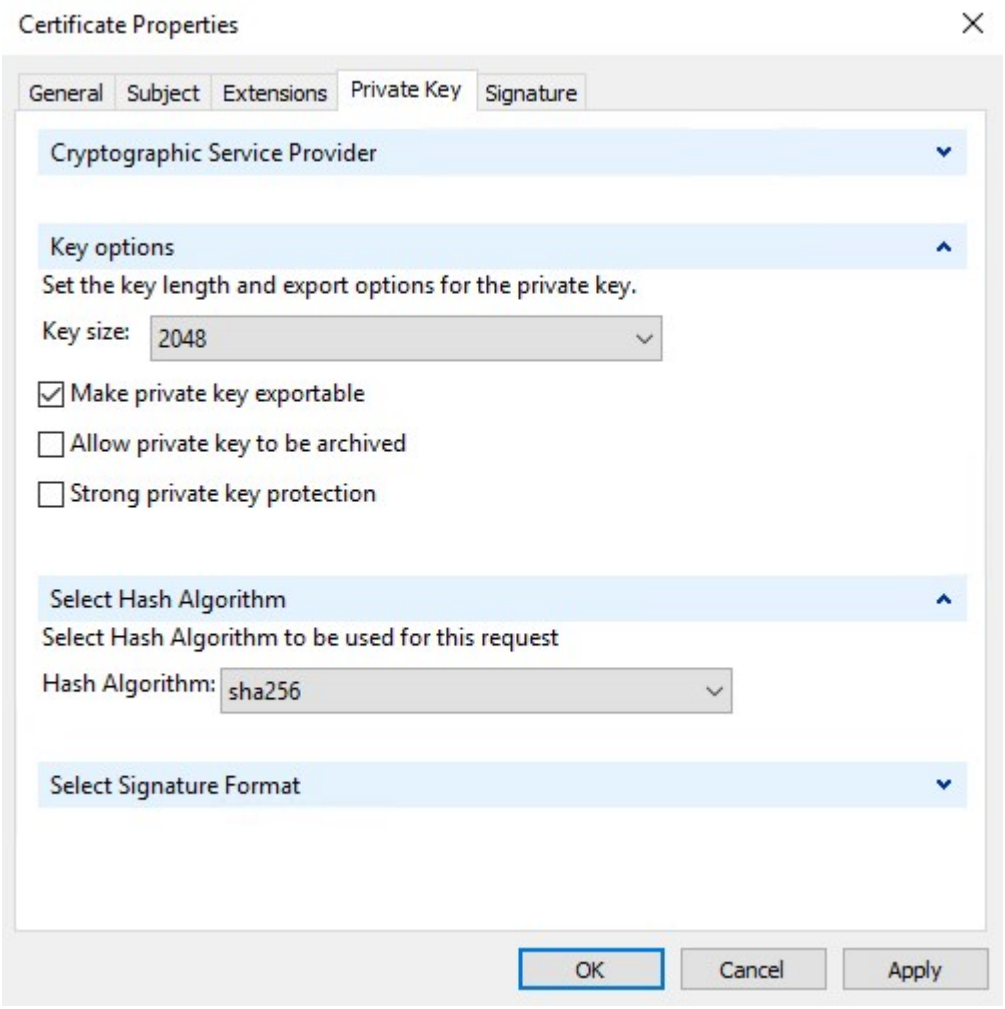
10. Some CAs don't require extensions. However, if required, go to the **Extensions** tab and expand the **Key usage** menu. Add the required options from the list of **Available options** to the **Selected options** list.



11. On the **Private Key** tab, expand the **Key options** menu.

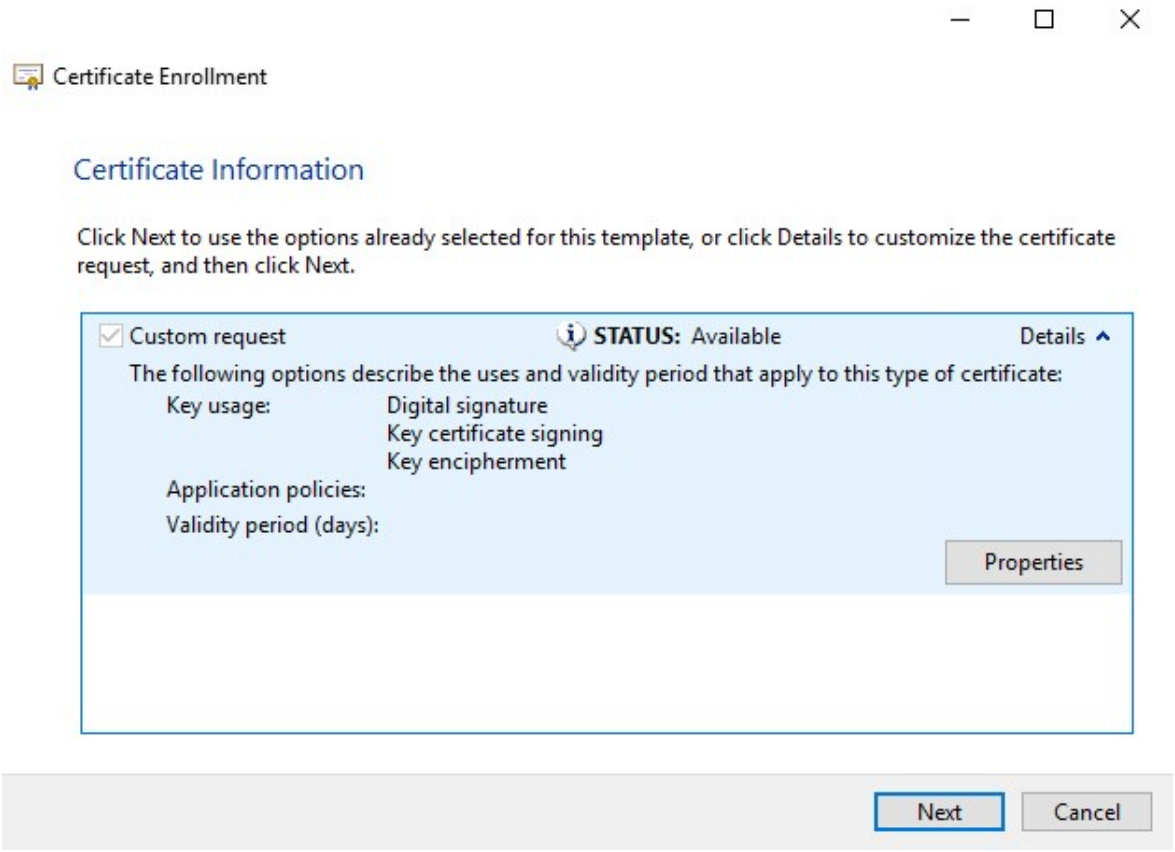
    Set the key size to 2048 and select the option to make the private key exportable.

    > The key size variable is determined by the CA, therefore a higher size key may be required. Other options, such as a specific Hash Algorithm (sha256), may also be required. Adjust all of the options required before proceeding to the next step.



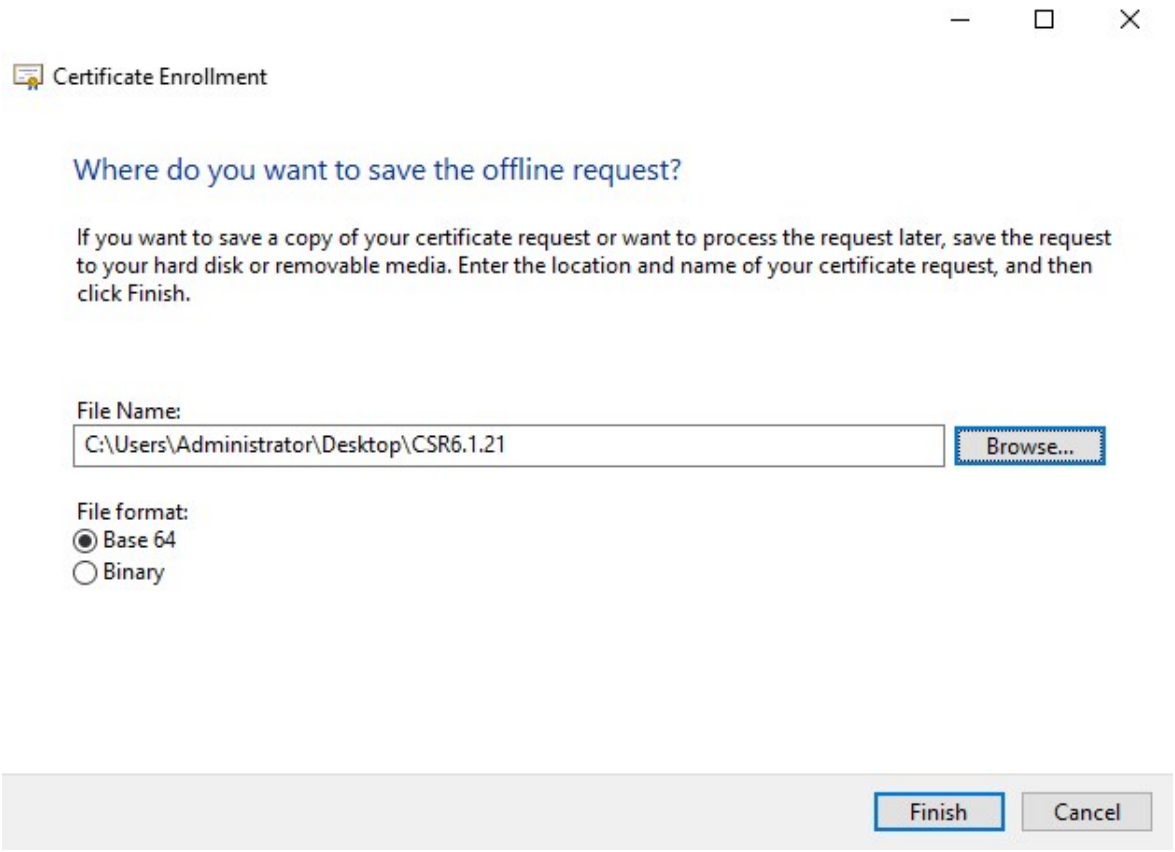
12. Unless the CA requires a signature, the next step is to click **OK**.

13. When all of the certificate properties have been defined, click **Next** on the **Certificate Enrollment** wizard.



14. Select a location to save the certificate request and a format. Browse to that location and specify a name for the .req file. The default format is base 64, however some CAs require the binary format.

15. Click **Finish**.



A .req file is generated, which you must use to request a signed certificate.

Upload the .req file to receive a signed certificate in return

Every CA has a different process for uploading .req files in order to receive a signed certificate in return. Refer to the documentation of your CA for information on retrieving a signed certificate.

When working with the Mobile Server it is recommended to use a third-party CA. In most third-party CA situations, it is required to download a .ZIP file, and extract the contents to the computer that hosts the Mobile Server.

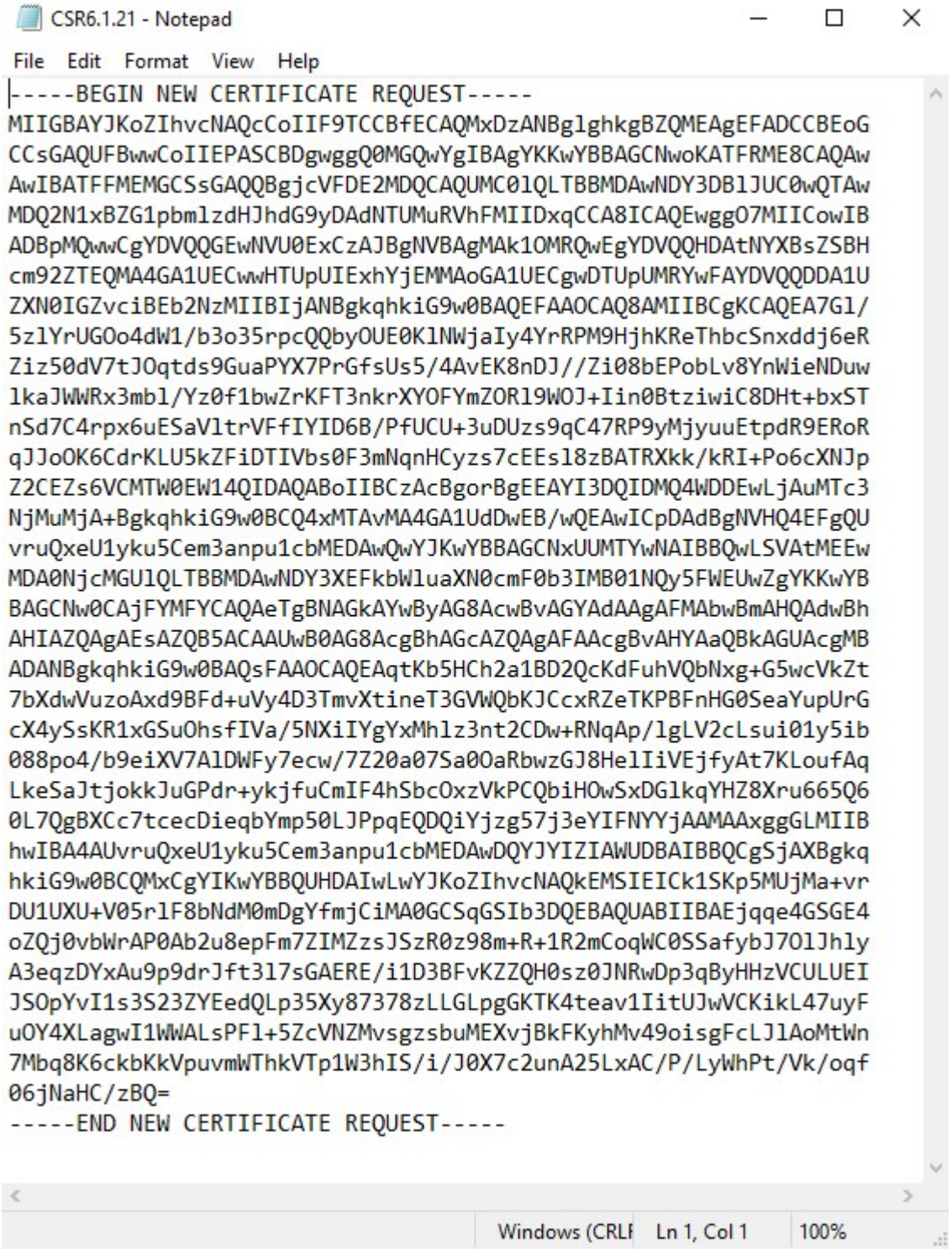
There are several file types that could be included in the extracted .ZIP file contents.

.CER or .CRT files can be installed using a similar process. Right-click the file and choose **Install Certificate** from the shortcut menu.

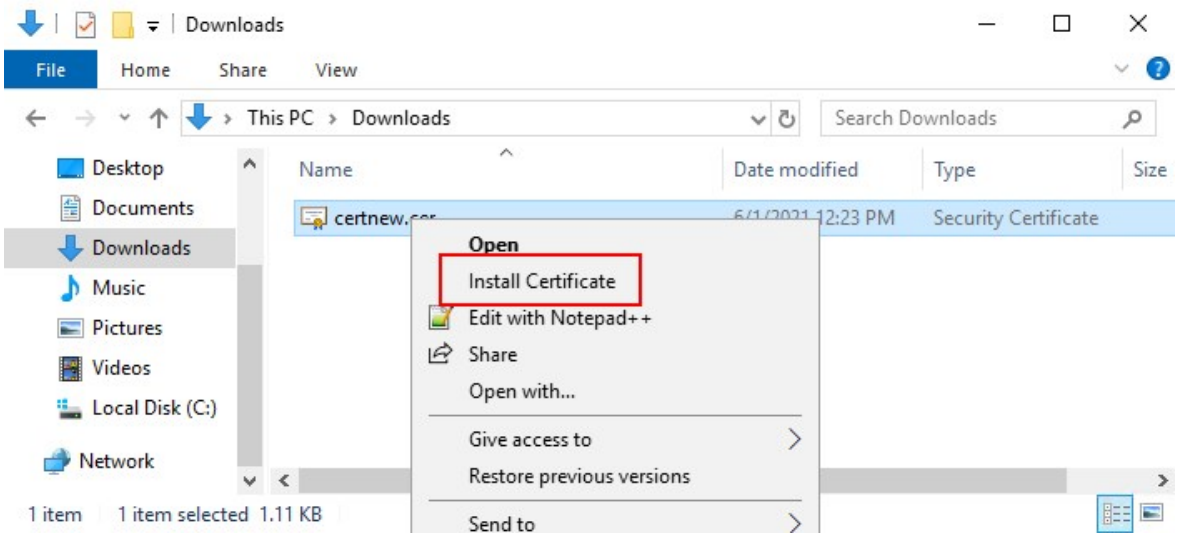
The following steps use a .CER file from an internal CA.

Your CA will need the contents of the .req file. You will be asked to copy the entire text of the .req file, including the begin and end lines, and paste the text into a field made available at a portal managed by the CA.

1. Browse to the location of the .req file and open it in Notepad, and paste the text into a field made available at a portal managed by your CA.

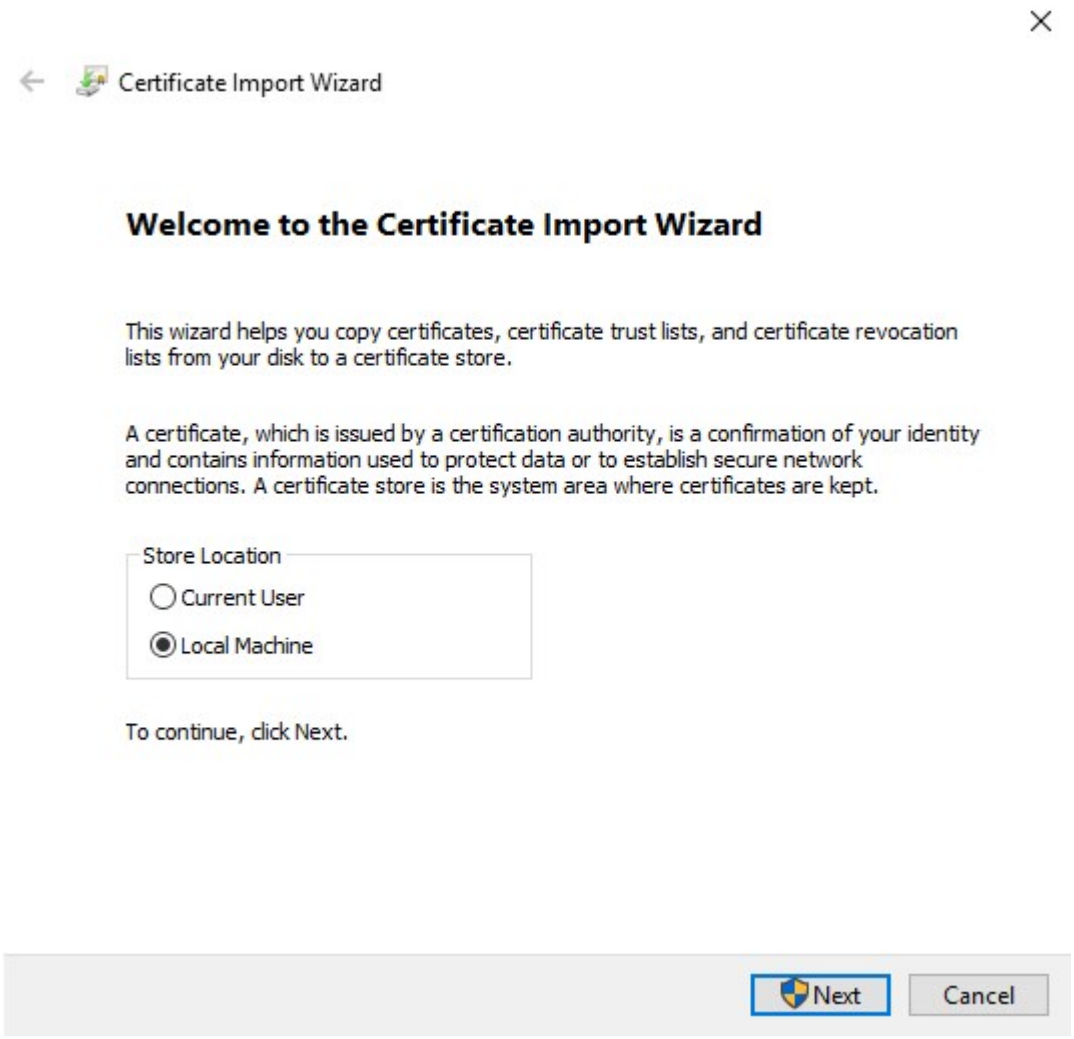


2. When you receive the certificate from your CA, browse to the downloads folder (or wherever you choose to store the folder on the computer), right-click the certificate and select **Install Certificate**.

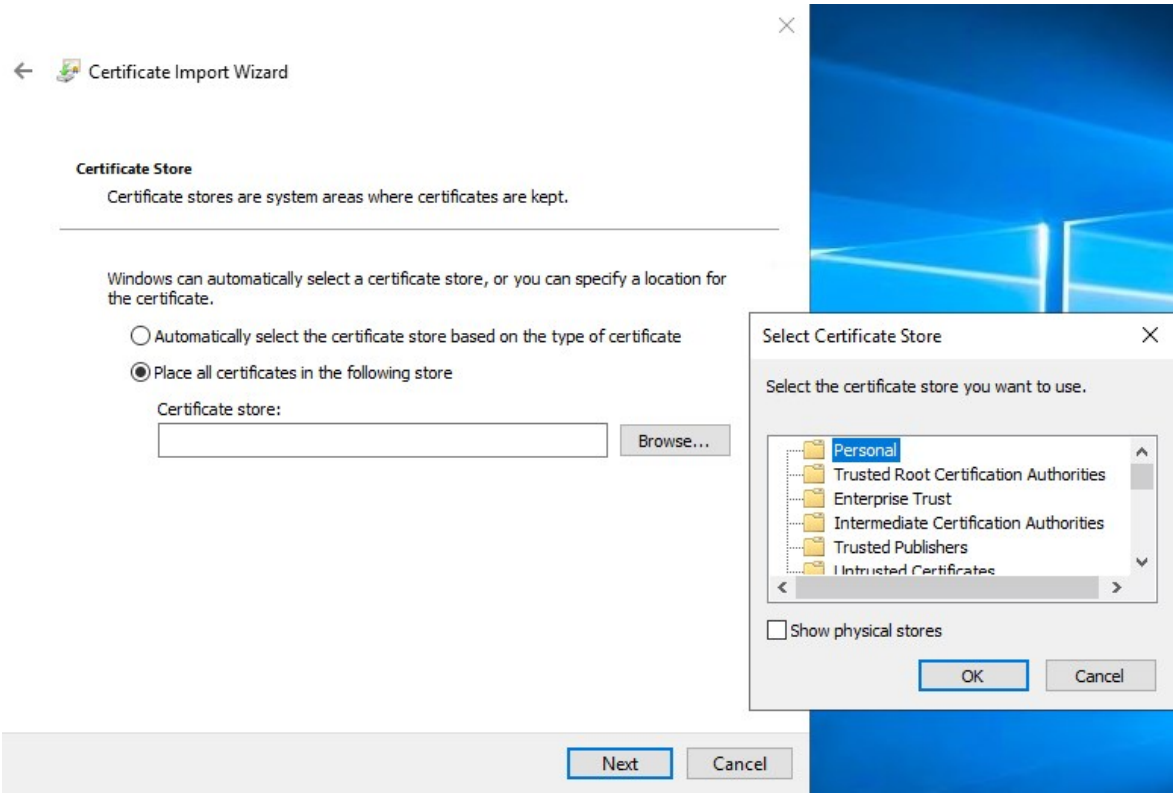


3. Accept the security warning if it appears.

   Select to install the certificate for the local machine and click **Next**.



4. Choose a storage location, and browse to the Personal certificate store, and click **Next**.



5. Finish the **Install Certificate** wizard.

Enable encryption on the Mobile Server

Once the certificate is installed on thecomputer that hosts the Mobile Server, do the following.

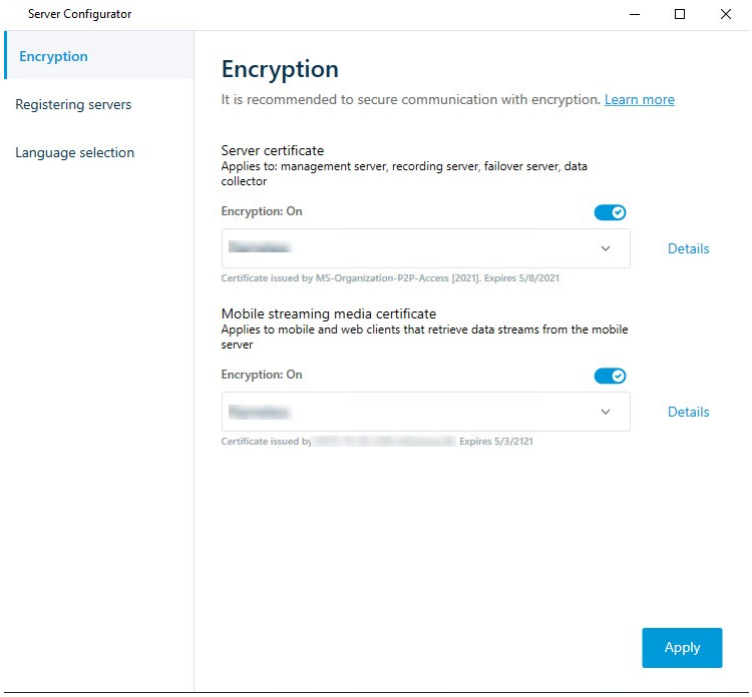
1. On a computer with a Mobile Server installed, open the **Server Configurator** from:
   - The Windows Start menu

   or

   - The Mobile Server Manager by right-clicking the Mobile Server Manager icon on the computer task bar
2. In the **Server Configurator**, under **Mobile streaming media certificate**, turn on **Encryption**.
3. Click **Select certificate** to open a list with unique subject names of certificates that have a private key and that are installed on the local computer in the Windows Certificate Store.
4. Select a certificate to encrypt the communication of XProtect Mobile client and XProtect Web Client with the Mobile Server.

   Select **Details** to view Windows Certificate Store information about the selected certificate.

The Mobile Server service user has been given access to the private key. It is required that this certificate be trusted on all clients.



5. Click **Apply**.

When you apply certificates, the Mobile Server service restarts.

For more information, you may want to see:

Powershell Process Video.

Whitepaper on certificates with the Mobile Server.

Milestone XProtect Knowledgebase Document that outlines the following process using GoDaddy CA.

Install third-party or commercial CA certificates for communication with the Management Server or Recording Server

Management Servers and Recording Servers do not require trusted third-party or commercial CA certificates for encryption, but you can choose to use these certificates if it is part of your security policy, and they will be automatically trusted by client workstations and servers.

The process is identical to the Mobile Server certificate installation.

When you configure encryption for a server group, it must either be enabled with a certificate belonging to the same CA certificate or, if the encryption is disabled, then it must be disabled on all computers in the server group.

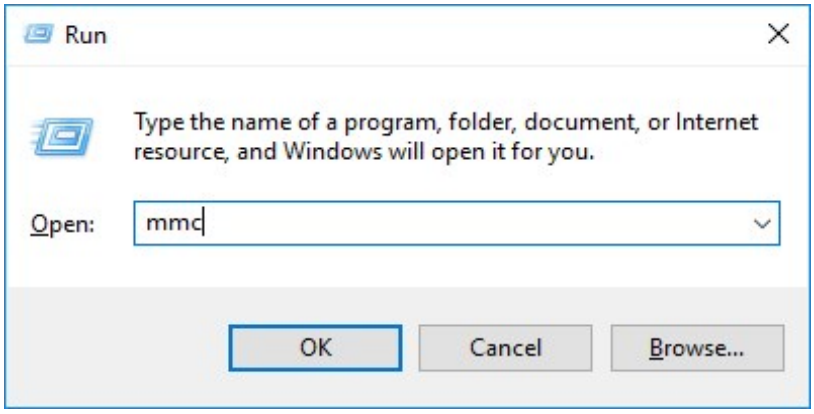
Certificates issued by CA (Certificate Authority) have a chain of certificates and on the root of that chain is the CA root certificate. When a device or browser sees this certificate, it compares its root certificate with pre-installed ones on the OS (Android, iOS, Windows, etc.). If the root certificate is listed in the pre-installed certificates list, then the OS ensures the user that the connection to the server is secure enough. These certificates are issued for a domain name and are not free of charge.

Add a CA certificate to the server

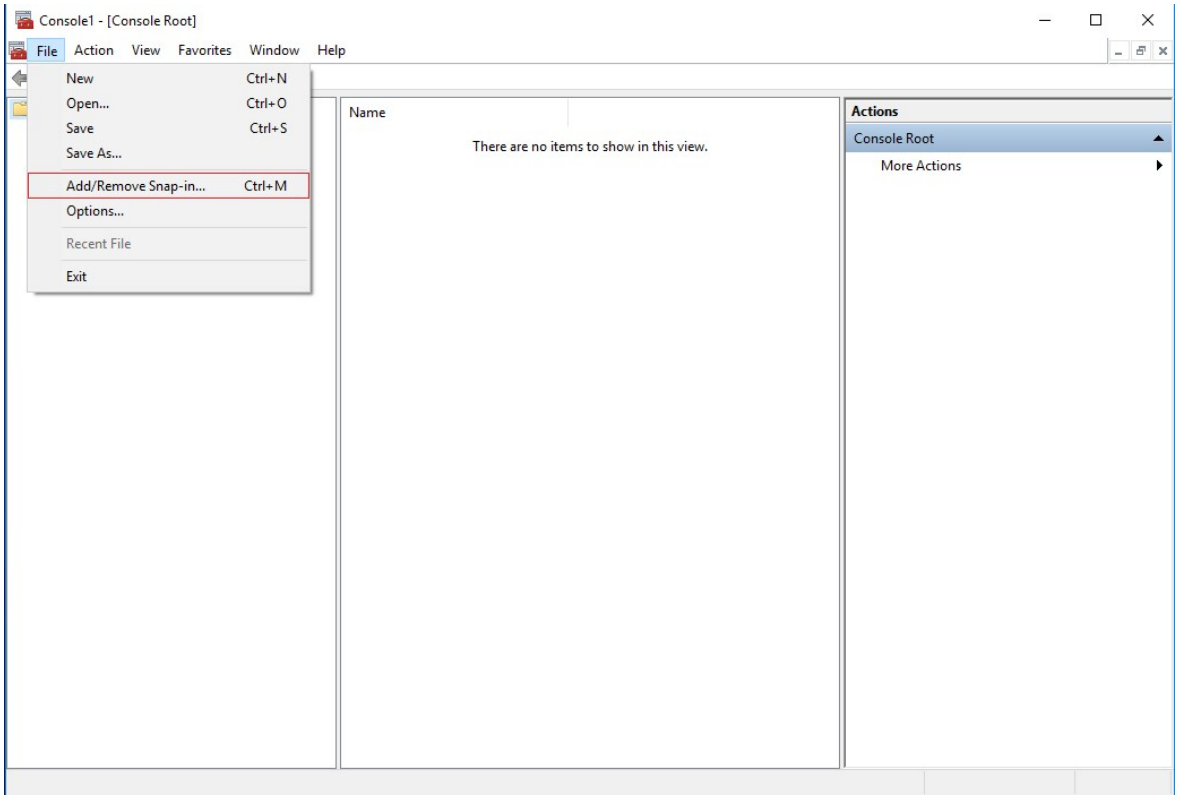
Add the CA certificate to the server by doing the following.

Specific parameters depend on the CA. Refer to the documentation of your CA before proceeding.

1. On the computer that hosts the XProtect server, open the Microsoft Management Console.

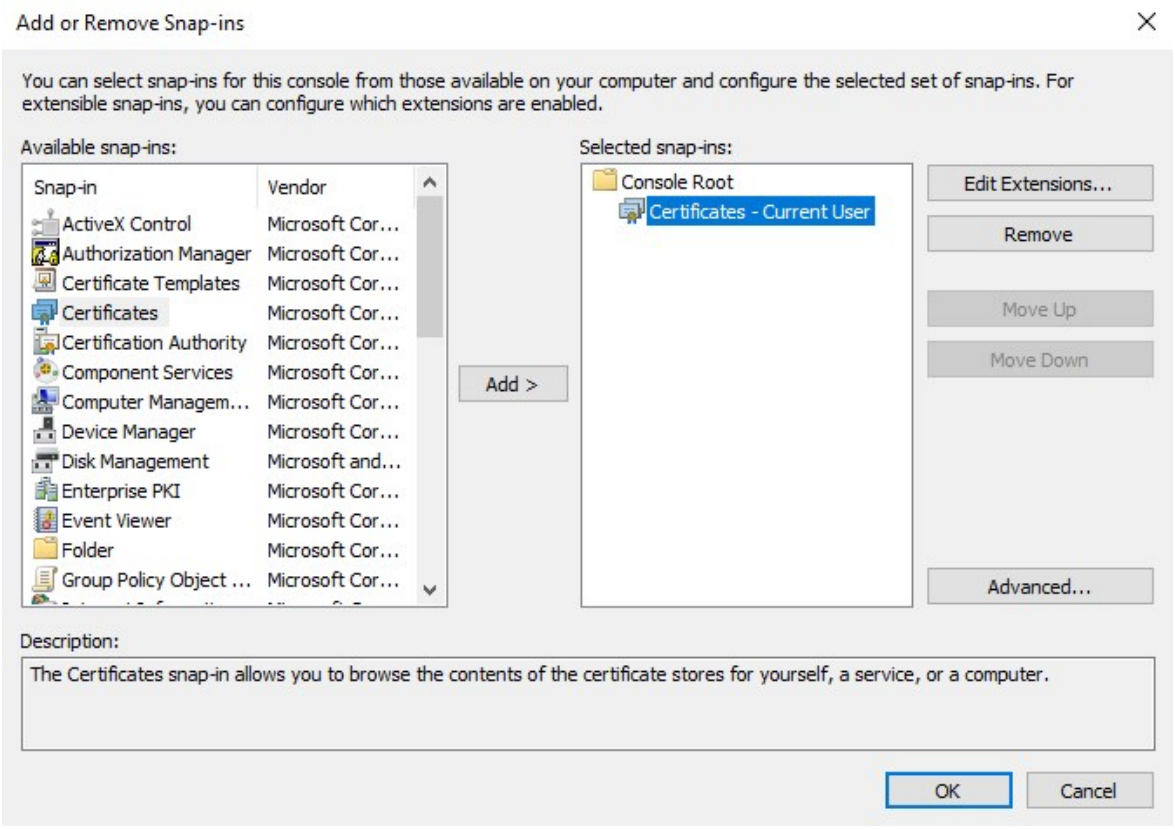


2. In the Microsoft Management Console, from the **File** menu select **Add/Remove Snap-in...**.

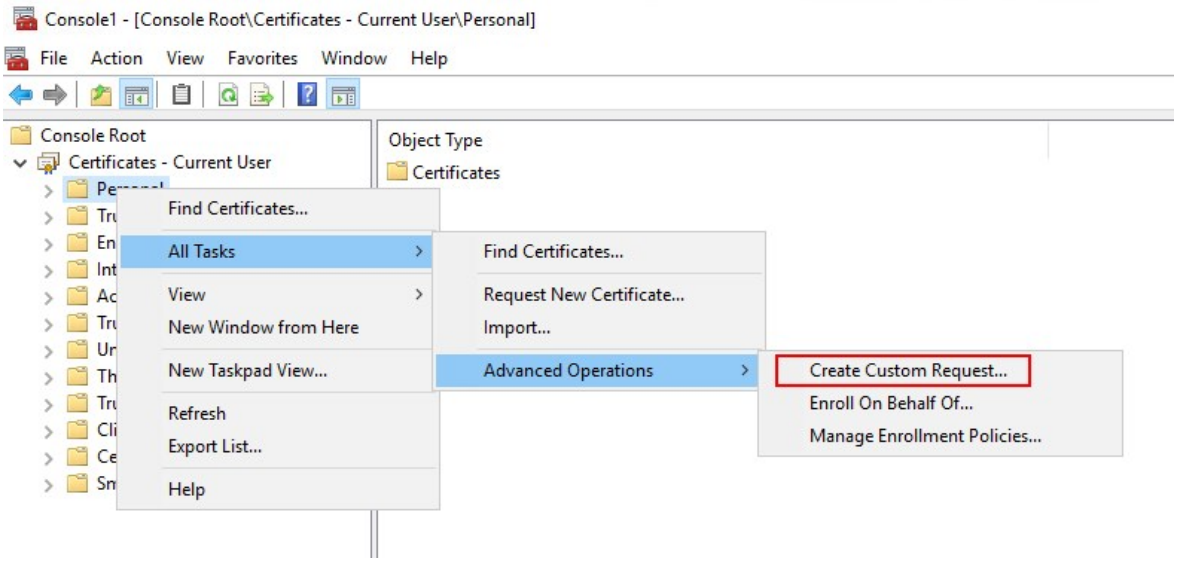


3. Select the **Certificates** snap-in and click **Add**.

   Click **OK**.

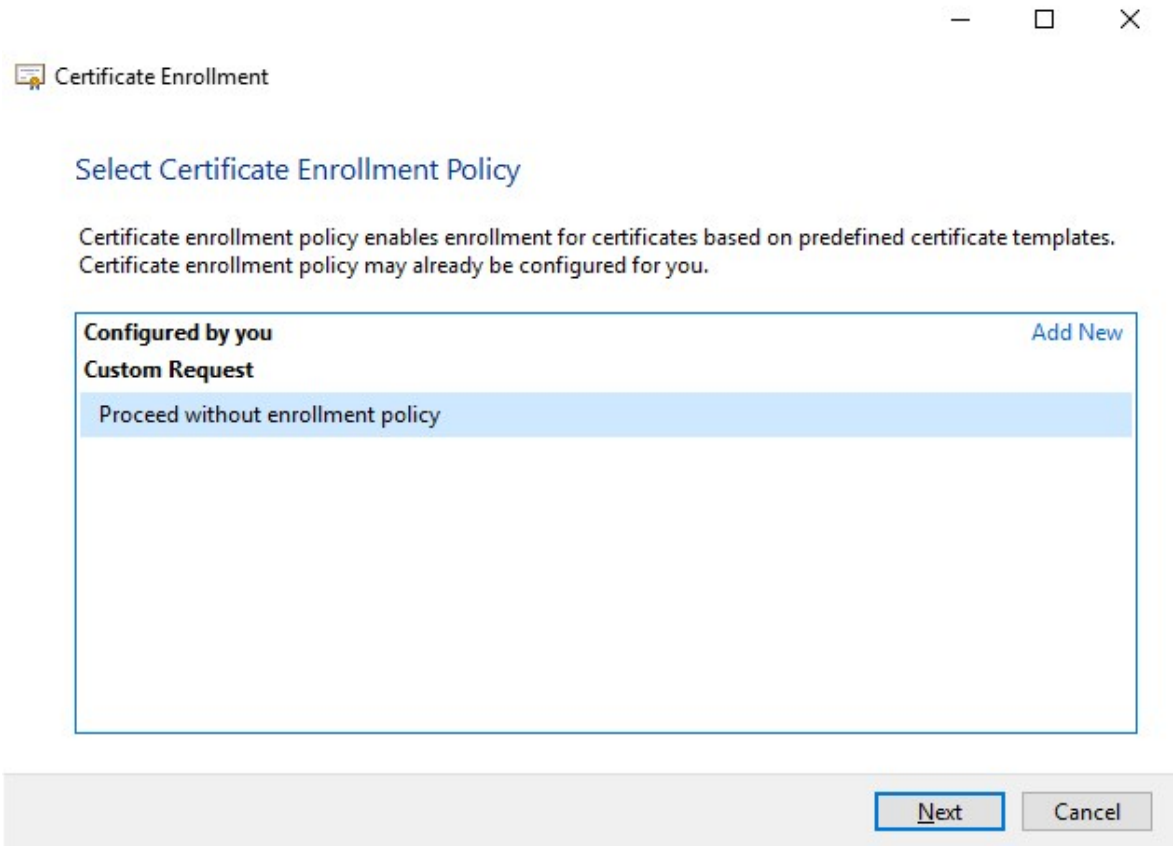


4. Expand the Certificates object. Right-click on the **Personal** folder and select **All Tasks** > **Advanced Operations** > **Create Custom Request**.

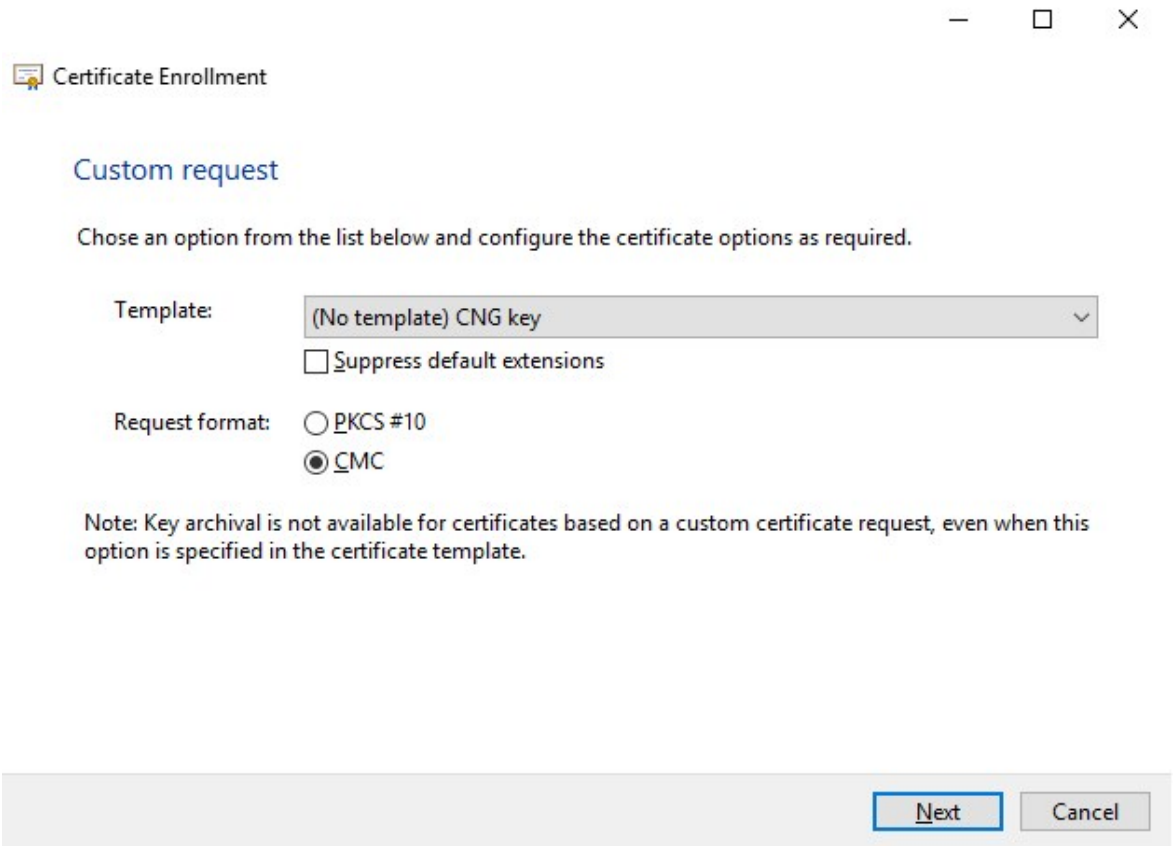


5. Click **Next** in the **Certificate Enrollment** wizard and select **Proceed without enrollment policy**.

   Click **Next**.



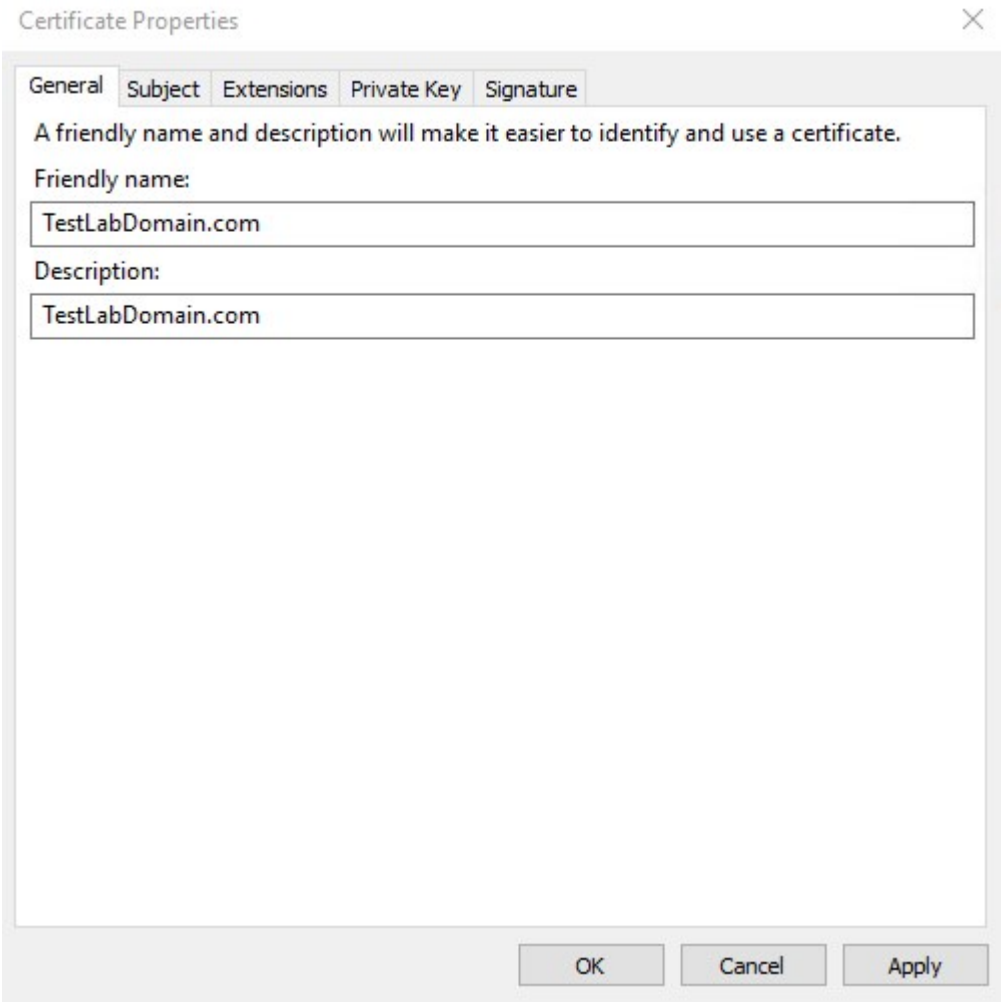
6. Select the **(No template) CNG Key** template and the **CMC** request format, and click **Next**.



The request format depends on the CA. If the wrong format is chosen, the CA will issue an error when the certificate signing request (CSR) is submitted. Check with the CA to make sure you choose properly.

7. Expand to view the **Details** of the custom request, and click **Properties**.

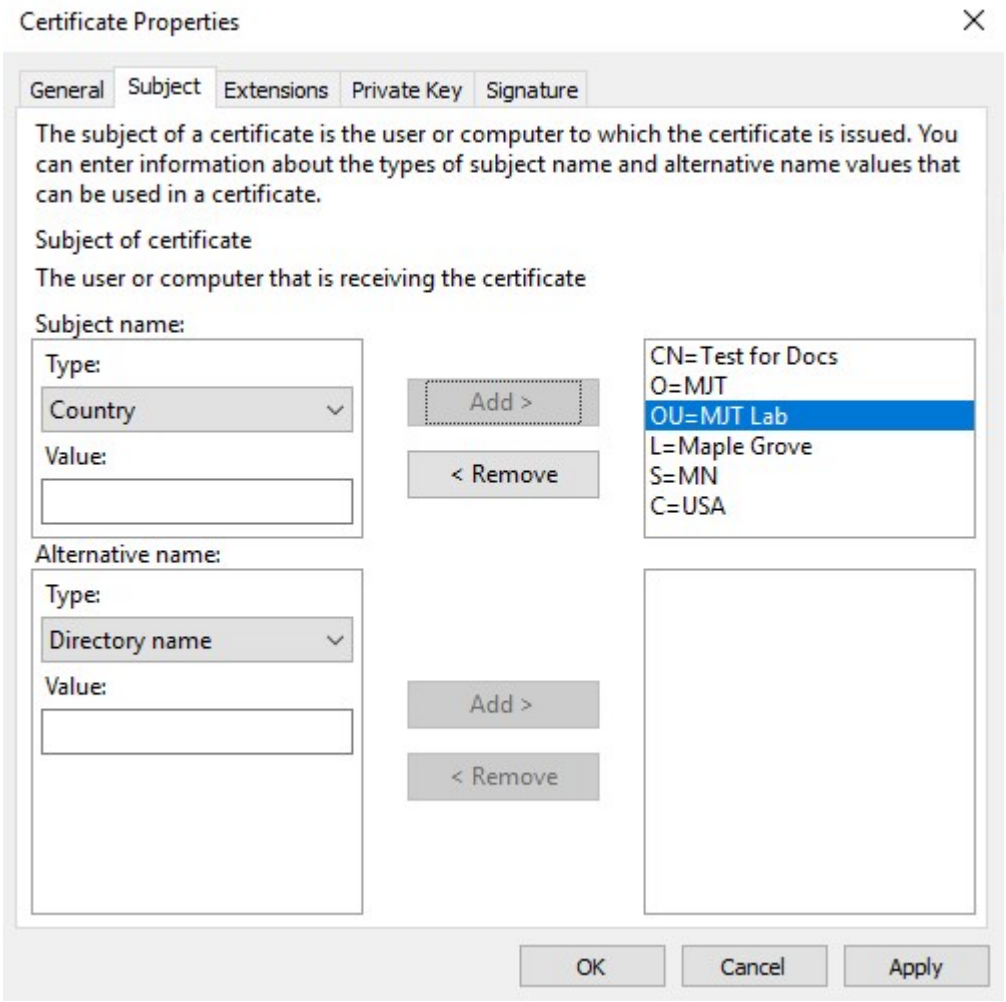
8. On the **General** tab, fill in the **Friendly name** and **Description** fields with the domain name registered with the CA.



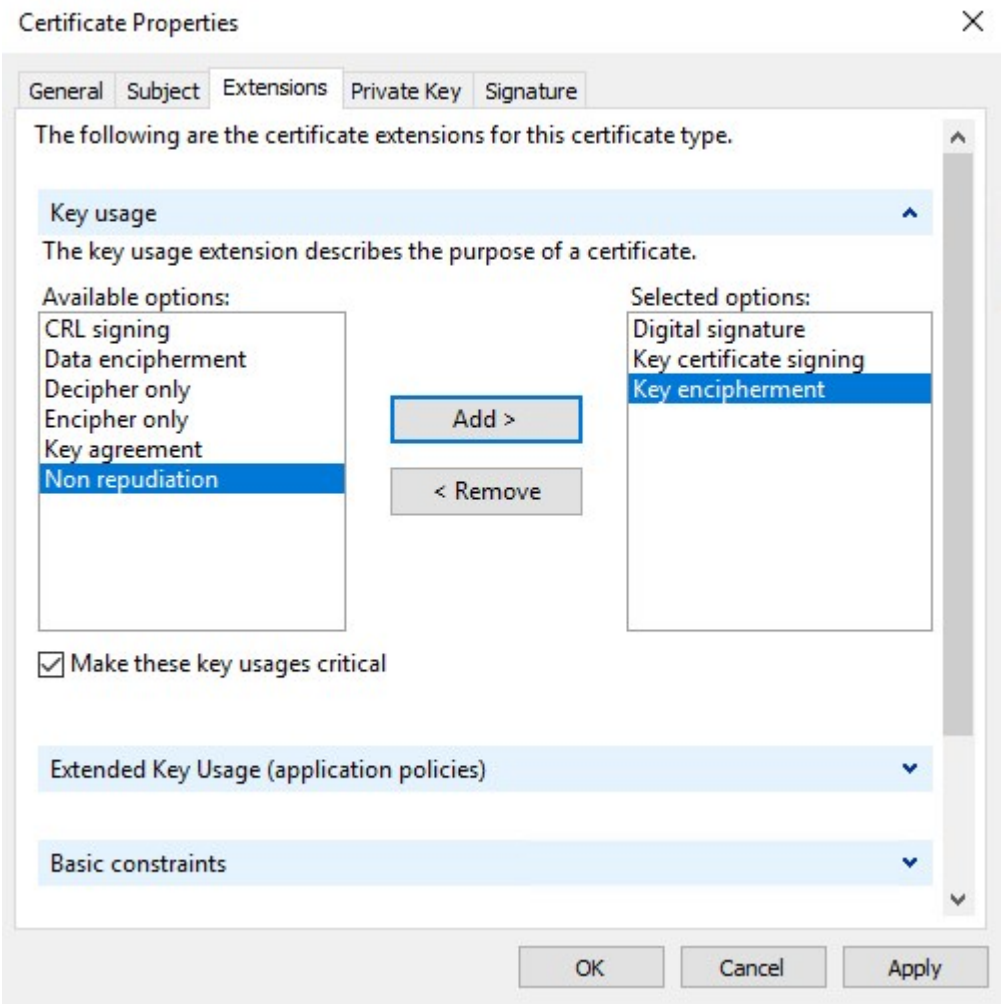
9. On the **Subject** tab, enter the parameters as required by the specific CA.

   For example, the subject name **Type** and **Value** are different for each CA. One example is the following required information:

   - Common Name:
   - Organization:
   - Organizational Unit:
   - City/Locality:
   - State/Province:
   - Country/Region:



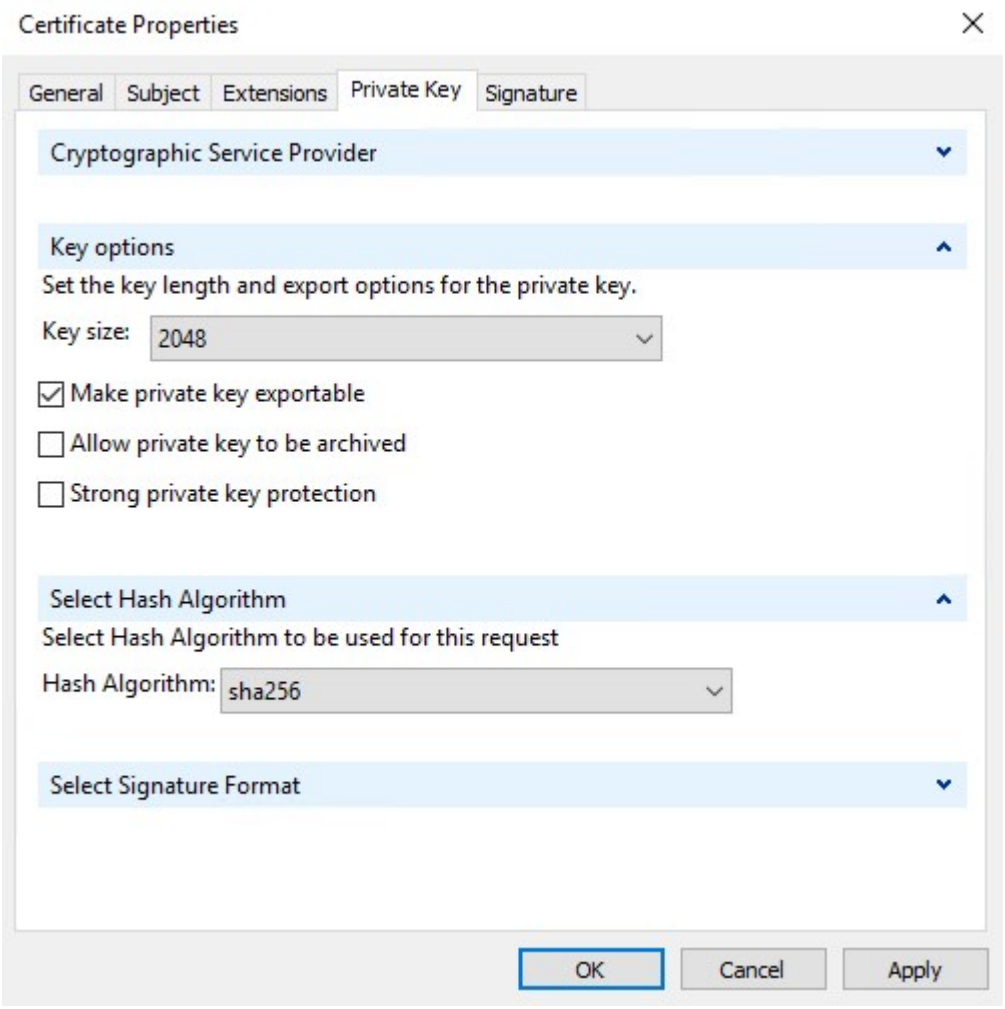
10. Some CAs don't require extensions. However, if required, go to the **Extensions** tab and expand the **Key usage** menu. Add the required options from the list of **Available options** to the **Selected options** list.



11. On the **Private Key** tab, expand the **Key options** menu.

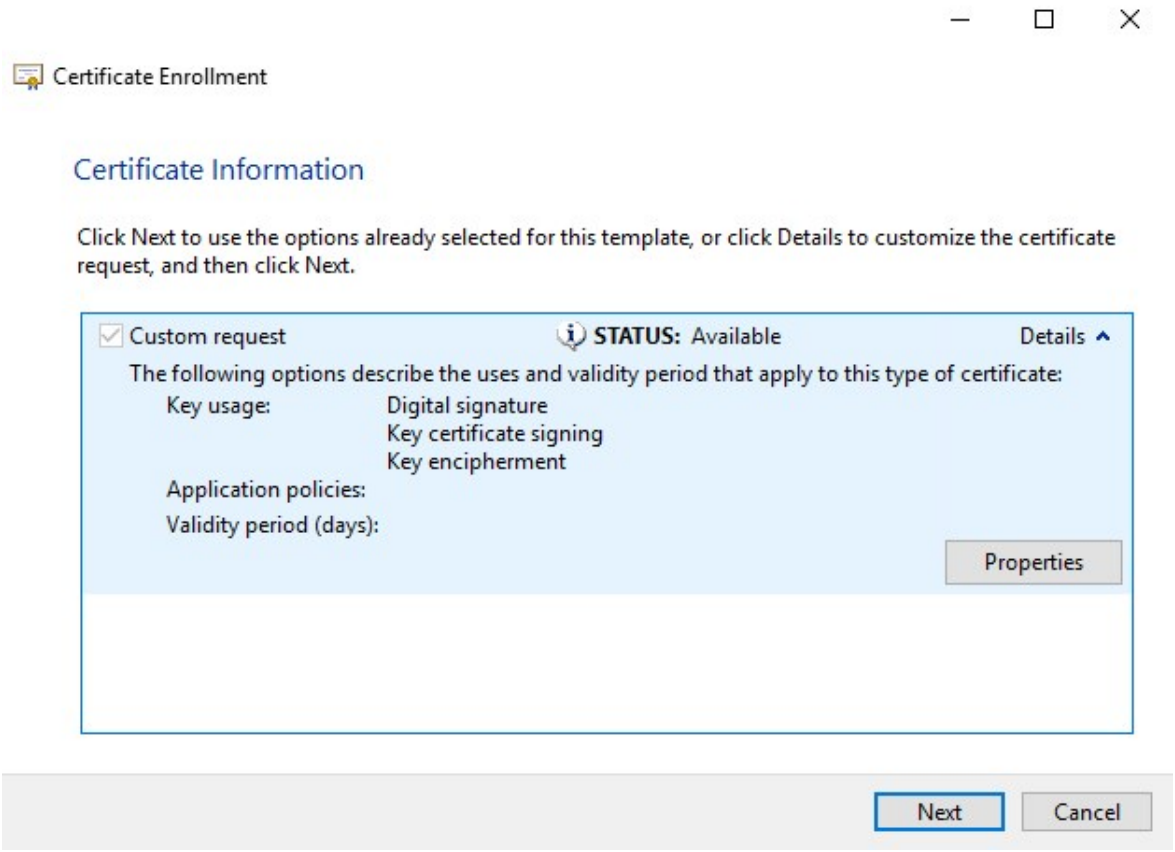
    Set the key size to 2048 and select the option to make the private key exportable.

    > The key size variable is determined by the CA, therefore a higher size key may be required. Other options, such as a specific Hash Algorithm (sha256), may also be required. Adjust all of the options required before proceeding to the next step.



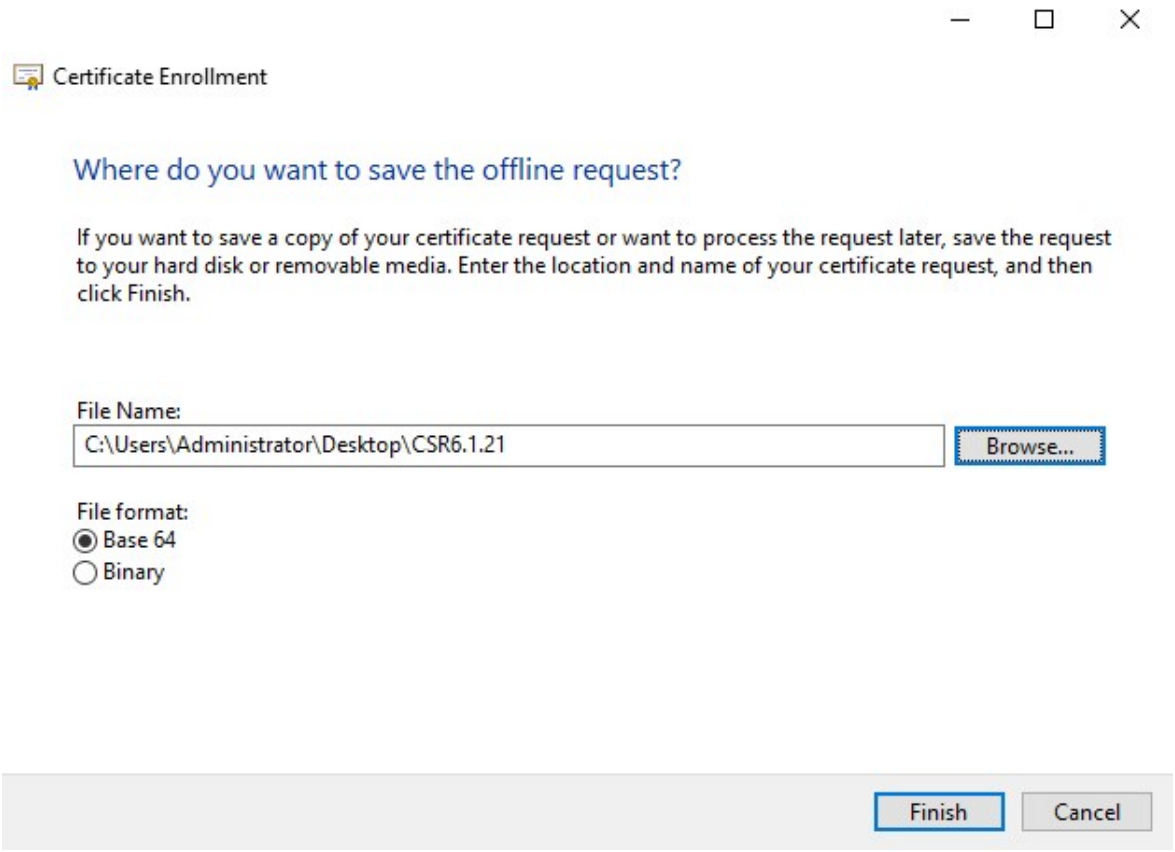
12. Unless the CA requires a signature, the next step is to click **OK**.

13. When all of the certificate properties have been defined, click **Next** on the **Certificate Enrollment** wizard.



14. Select a location to save the certificate request and a format. Browse to that location and specify a name for the .req file. The default format is base 64, however some CAs require the binary format.

15. Click **Finish**.



A .req file is generated, which you must use to request a signed certificate.

Upload the .req file to receive a signed certificate in return

> Every CA has a different process for uploading .req files in order to receive a signed certificate in return. Refer to the documentation of your CA for information on retrieving a signed certificate.

In most third-party CA situations, it is required to download a .ZIP file, and extract the contents to the computer that hosts the XProtect server.

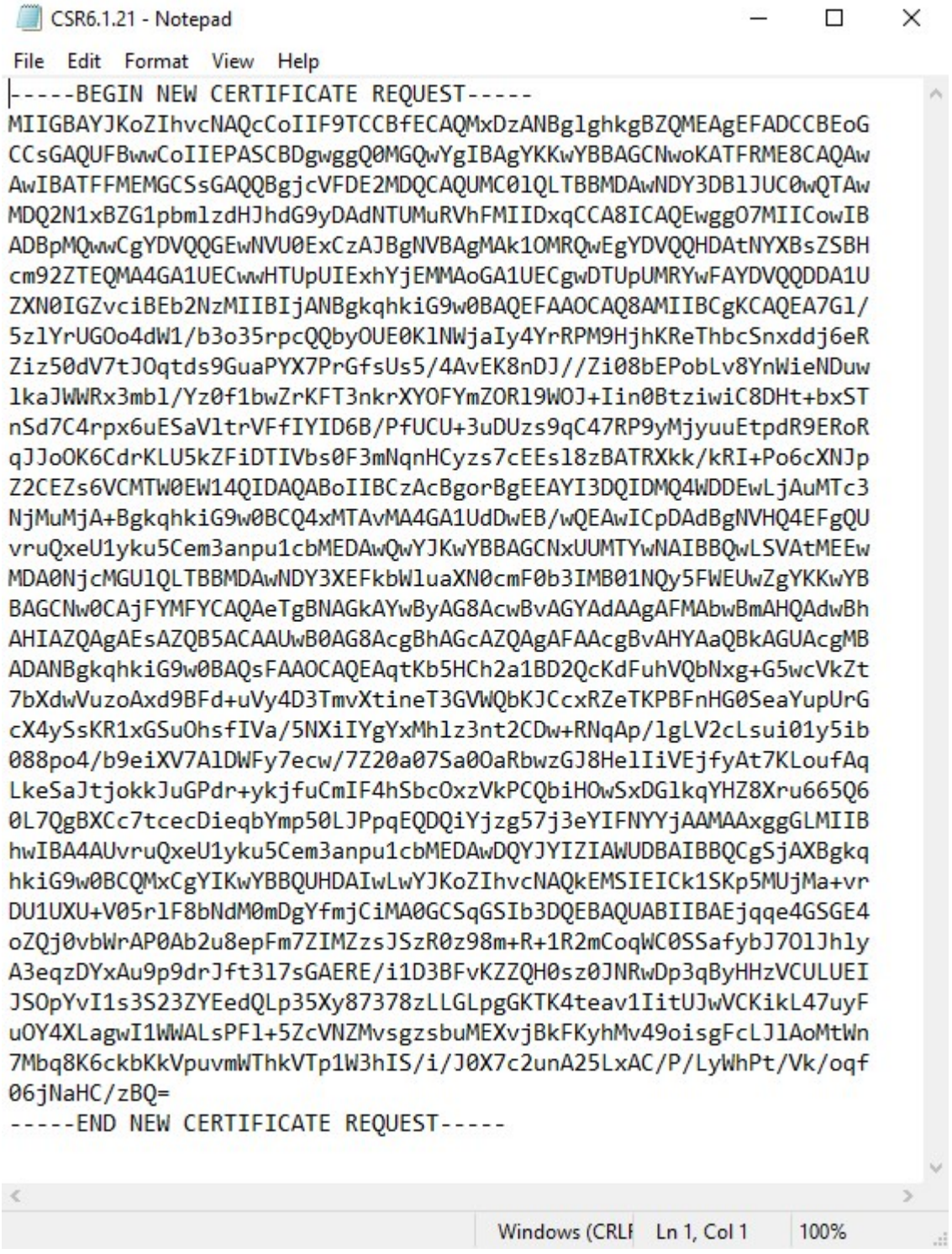
There are several file types that could be included in the extracted .ZIP file contents.

.CER or .CRT files can be installed using a similar process. Right-click the file and choose **Install Certificate** from the shortcut menu.

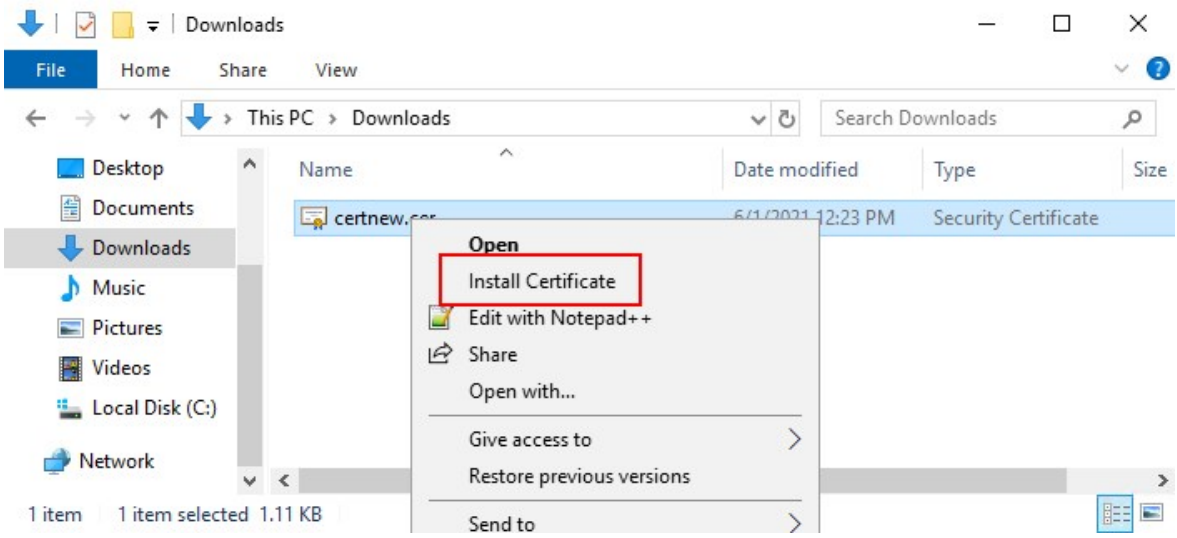
The following steps use a .CER file from an internal CA.

Your CA will need the contents of the .req file. You will be asked to copy the entire text of the .req file, including the begin and end lines, and paste the text into a field made available at a portal managed by the CA.

1. Browse to the location of the .req file and open it in Notepad, and paste the text into a field made available at a portal managed by your CA.

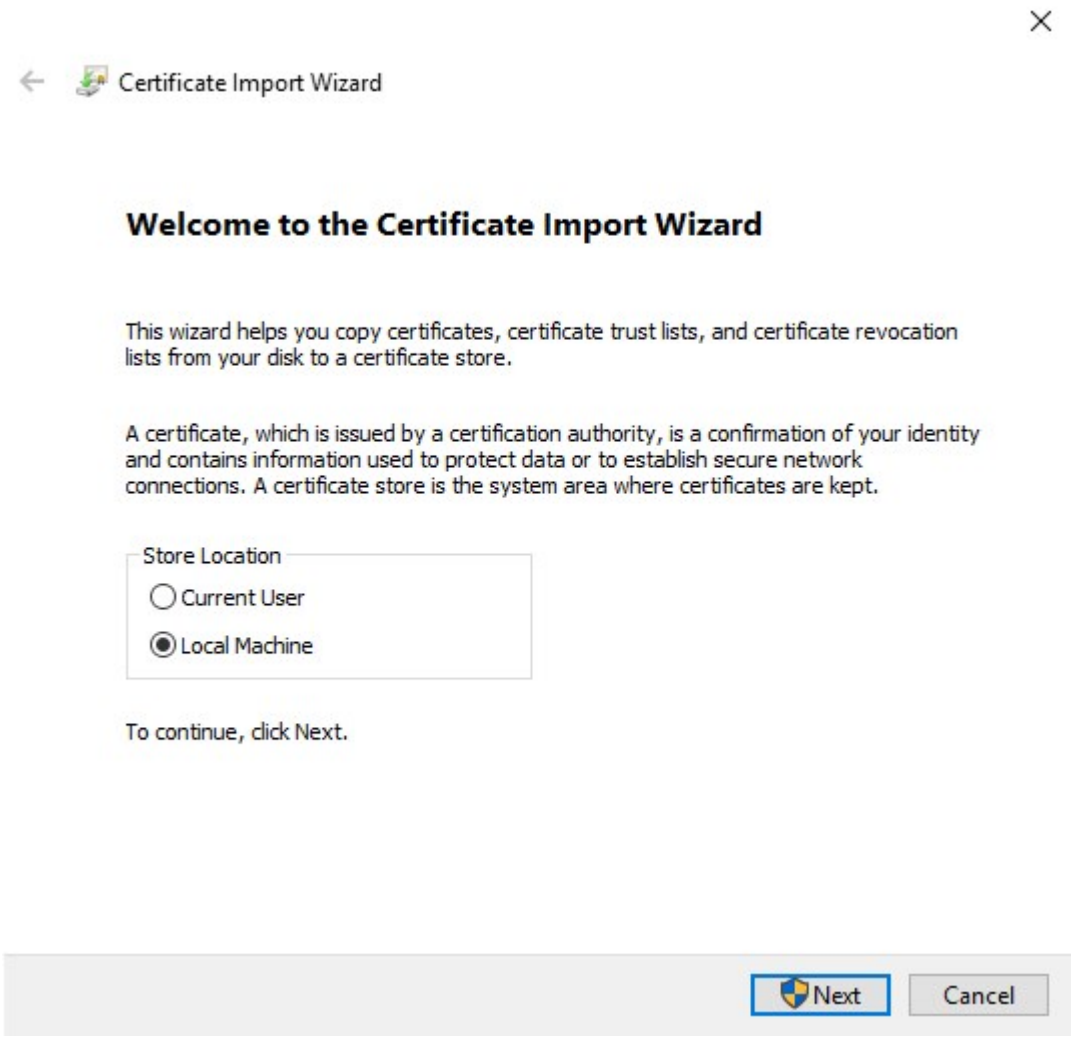


2. When you receive the certificate from your CA, browse to the downloads folder (or wherever you choose to store the folder on the computer), right-click the certificate and select **Install Certificate**.

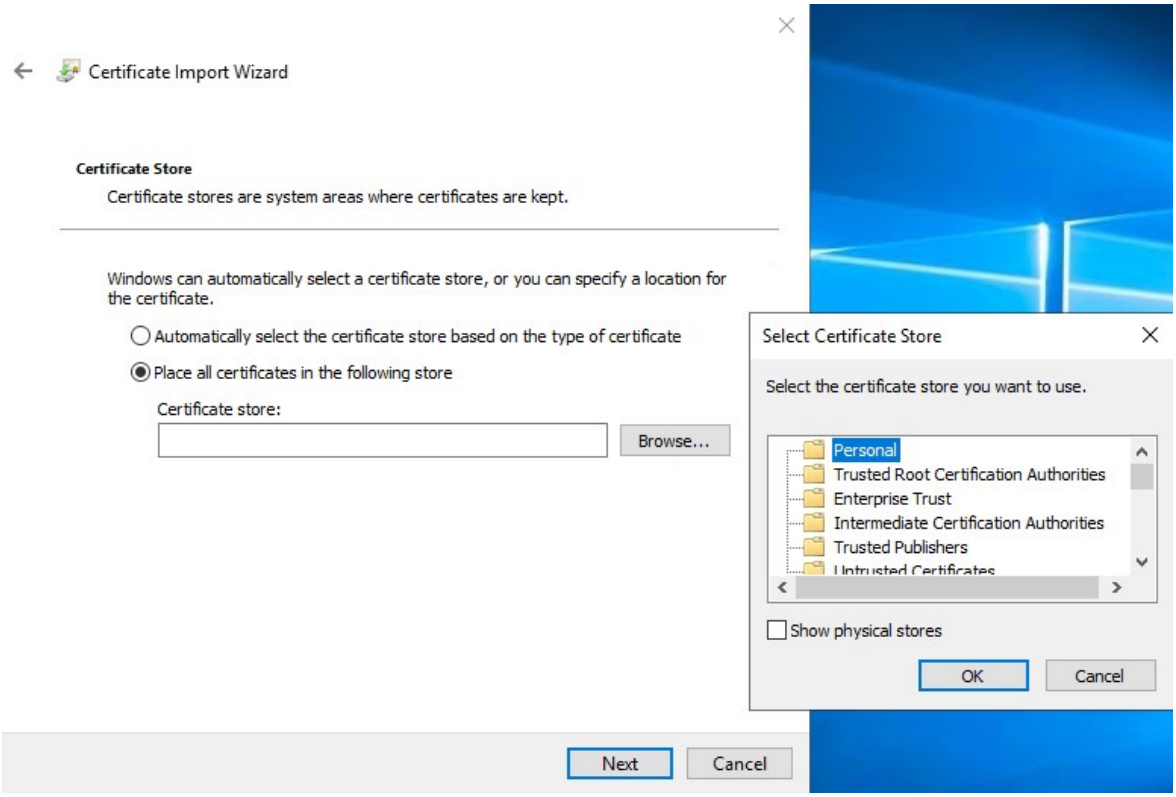


3. Accept the security warning if it appears.

   Select to install the certificate for the local machine and click **Next**.



4. Choose a storage location, and browse to the Personal certificate store, and click **Next**.



5. Finish the **Install Certificate** wizard.

Enable encryption to and from the Management Server

You can encrypt the two-way connection between the management server and the Data Collector affiliated when you have a remote server of the following type:

- Recording Server
- Event Server
- Log Server
- LPR Server
- Mobile Server

If your system contains multiple recording servers or remote servers, you must enable encryption on all of them.

> When you configure encryption for a server group, it must either be enabled with a certificate belonging to the same CA certificate or, if the encryption is disabled, then it must be disabled on all computers in the server group.

Prerequisites:

- A server authentication certificate is trusted on the computer that hosts the management server

First, enable encryption on the management server.

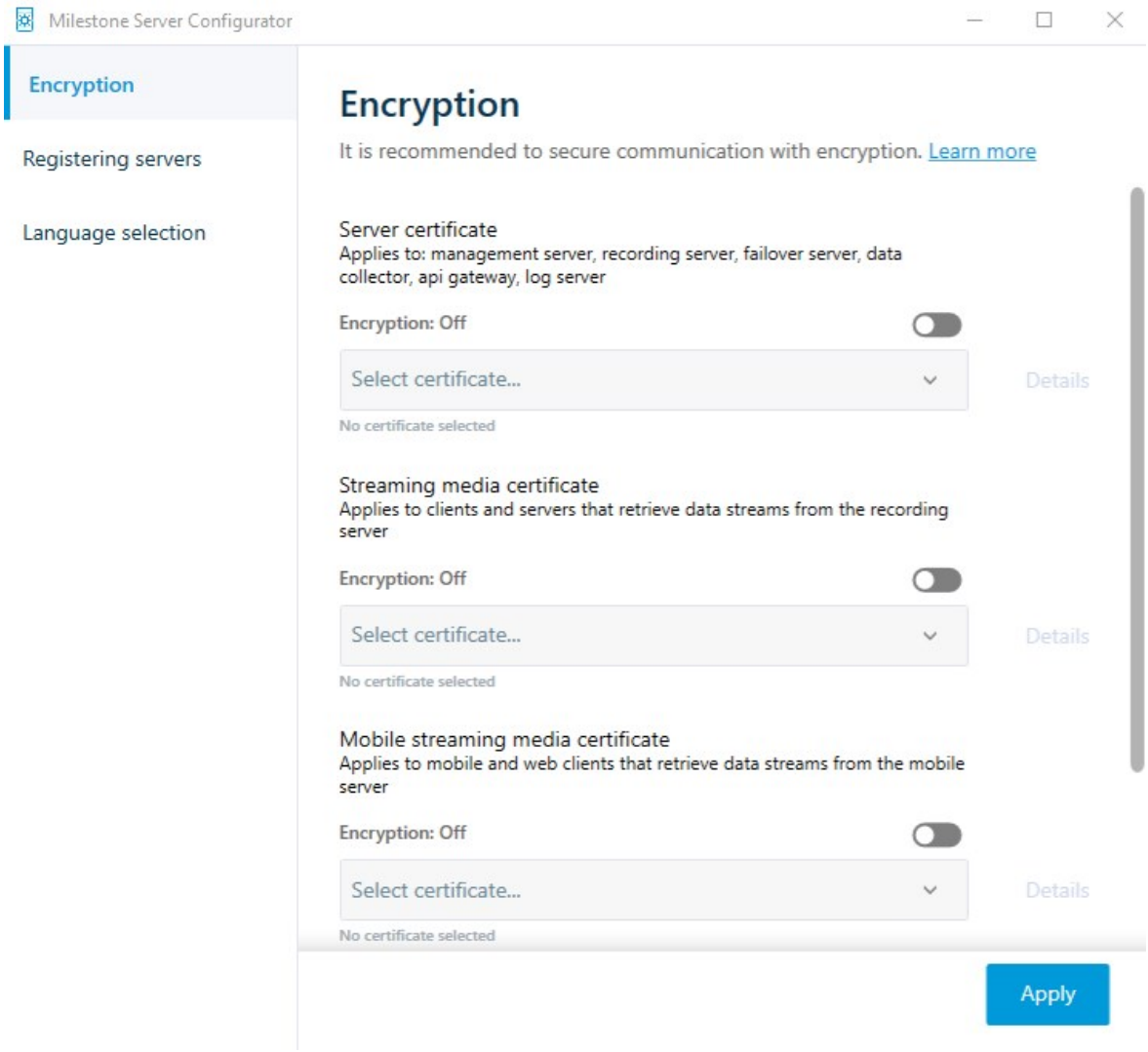
Steps:

1. On a computer with a management server installed, open the **Server Configurator** from:
   - The Windows Start menu

   or

   - The Management Server Manager by right-clicking the Management Server Manager icon on the computer task bar
2. In the **Server Configurator**, under **Server certificate**, turn on **Encryption**.
3. Click **Select certificate** to open a list with unique subject names of certificates that have a private key and that are installed on the local computer in the Windows Certificate Store.
4. Select a certificate to encrypt communication between the recording server, management server, failover server, and Data Collector server.

Select **Details** to view Windows Certificate Store information about the selected certificate.



5. Click **Apply**.

To complete the enabling of encryption, the next step is to update the encryption settings on each recording server and each server that has a Data Collector (Event Server, Log Server, LPR Server, and Mobile Server).

Install Active Directory Certificate Services

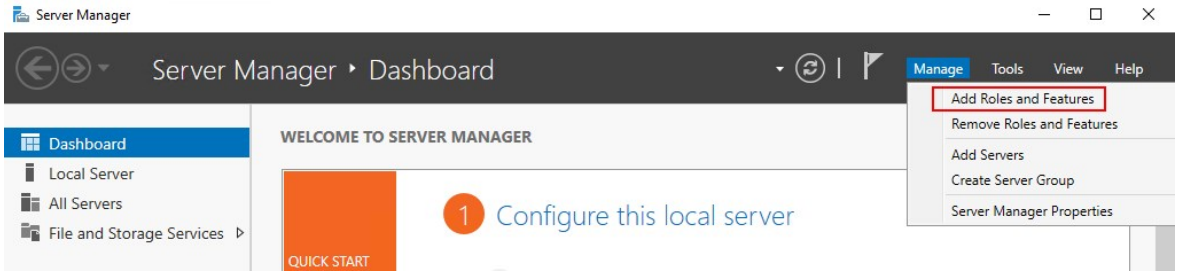
Active Directory Certificate Services (AD CS) is a Microsoft product that performs public key infrastructure (PKI) functionality. It acts as a Server Role that enables you to construct public key infrastructure (PKI) and give open key cryptography, computerized authentication, and advanced mark abilities for your association.

In this document, AD CS is used when installing certificates:

- In a domain environment (see Install certificates in a domain for communication with the Management Server or Recording Server on page 86)
- In a Workgroup environment (see Install certificates in a Workgroup environment for communication with the Management Server or Recording Server on page 107)

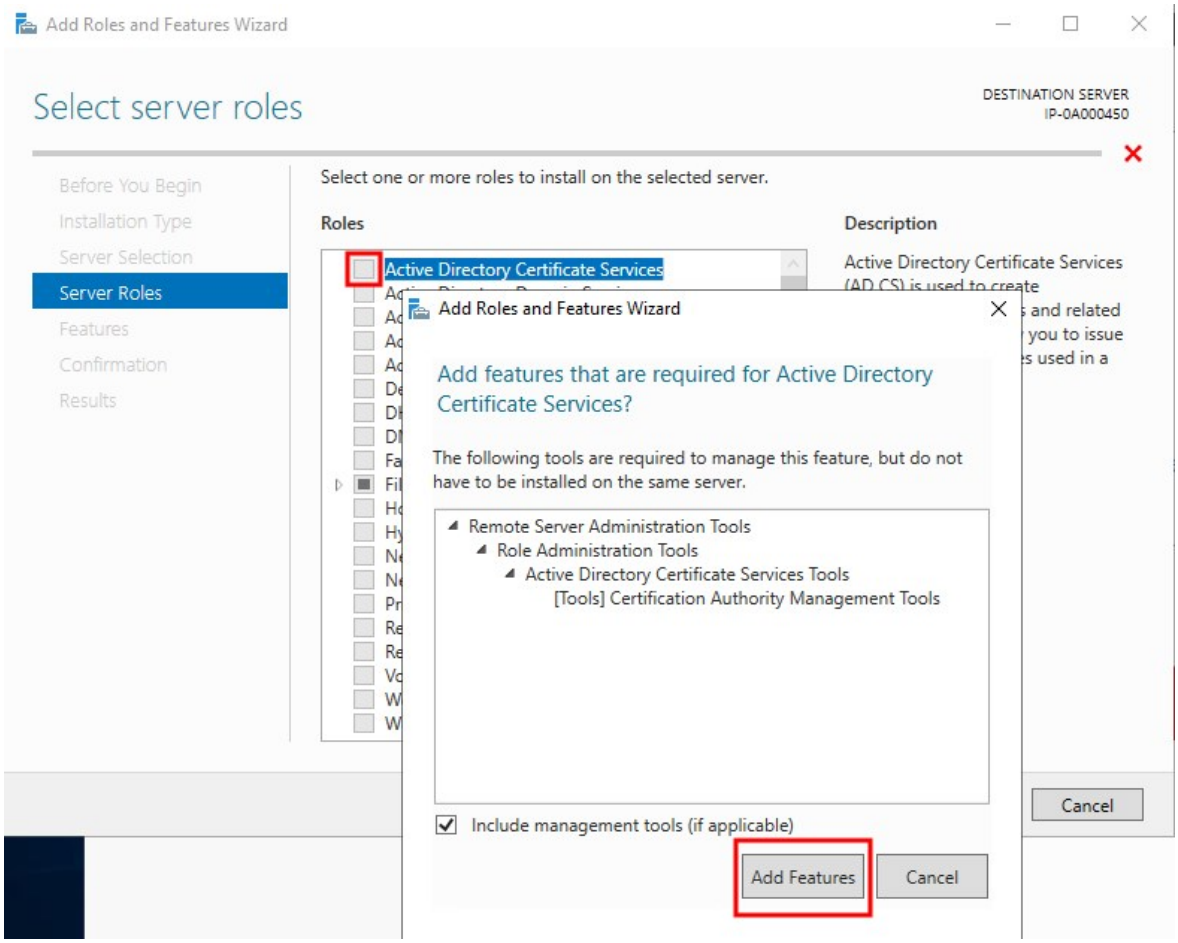
To install AD CS:

1. In the **Server Manager** application, select **Manage** > **Add Roles and Features**.



2. In **Before you begin**, click **Next**.
3. In **Installation Type**, select **Role-based or feature-based installation**, and click **Next**.
4. In **Server Selection**, select the local server as the destination for the installation, and click **Next**.

5. In **Server Roles**, select the **Active Directory Certificate Services** role. Review the list of features to install and click **Add Features**.

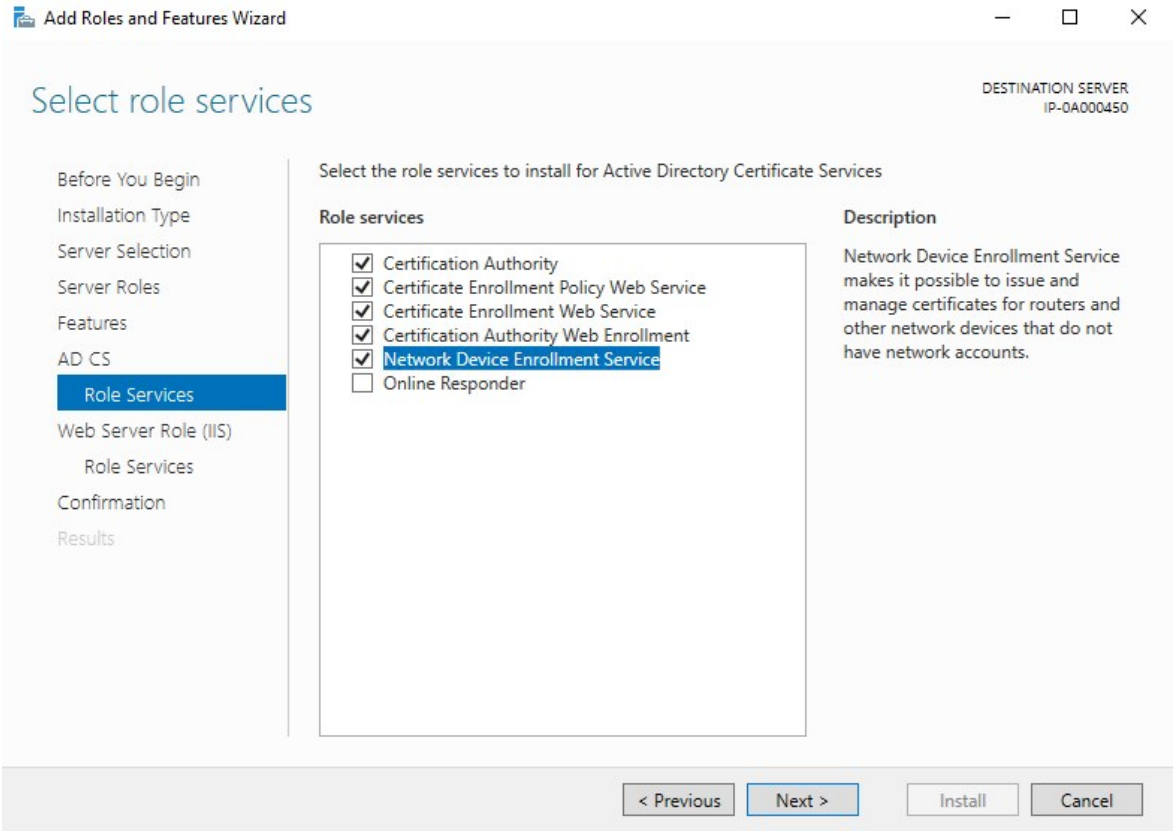


   Click **Next**.

6. In **Features**, click **Next**. All of the required features are selected for installation.
7. In **AD CS**, read the description of the Active Directory Certificated Services, and click **Next**.

8. In Role Services, select the following:
   - **Certification Authority**
   - **Certification Enrollment Policy Web Service**
   - **Certification Enrollment Web Service**
   - **Certification Authority Web Enrollment**
   - **Network Device Enrollment Service**

   As you select each of the role services, add the required features to support the installation of each service.

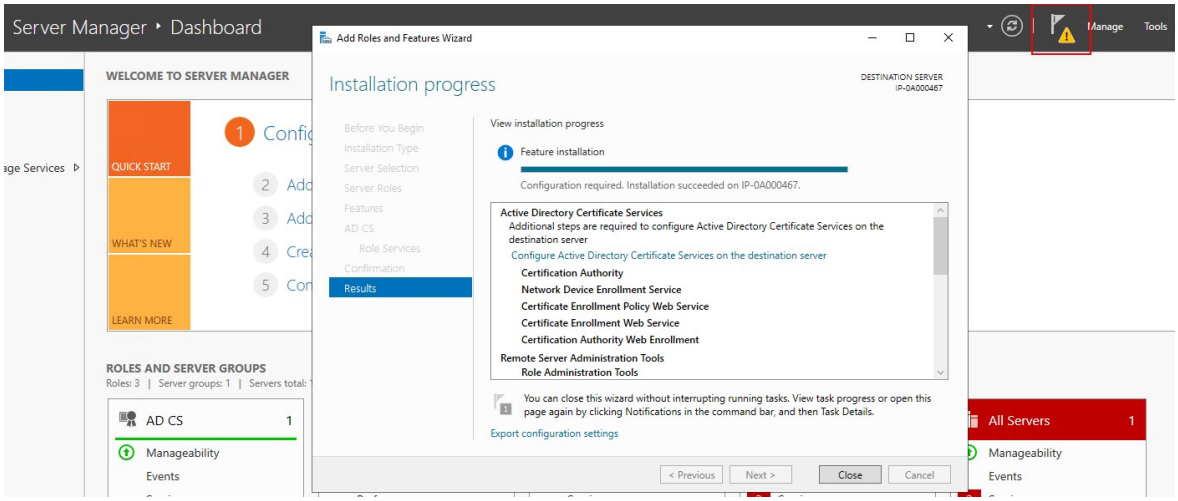


   Click **Next**.

9. In **Confirmation**, select **Restart the destination server automatically if required**, and click **Install**.

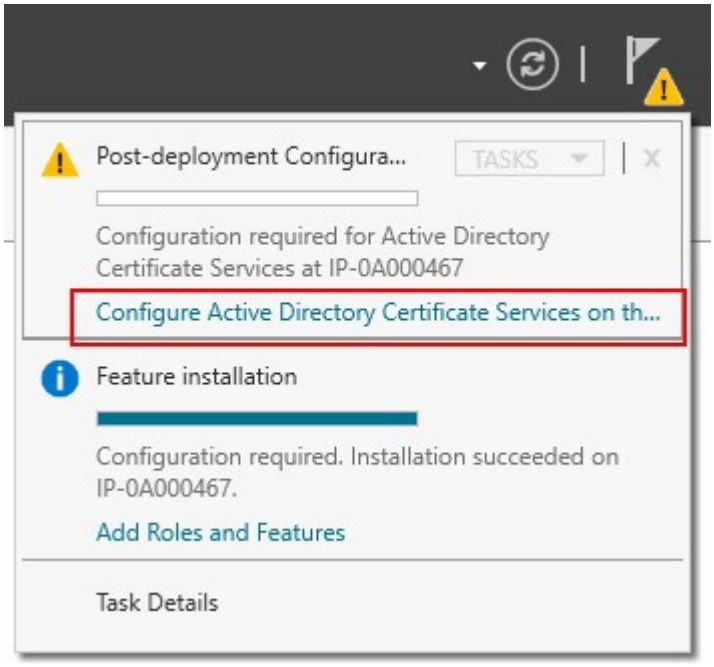
10. When the installation is done, click the **Close** button.

    Select the **Notification Flag** in the **Server Manager** application.



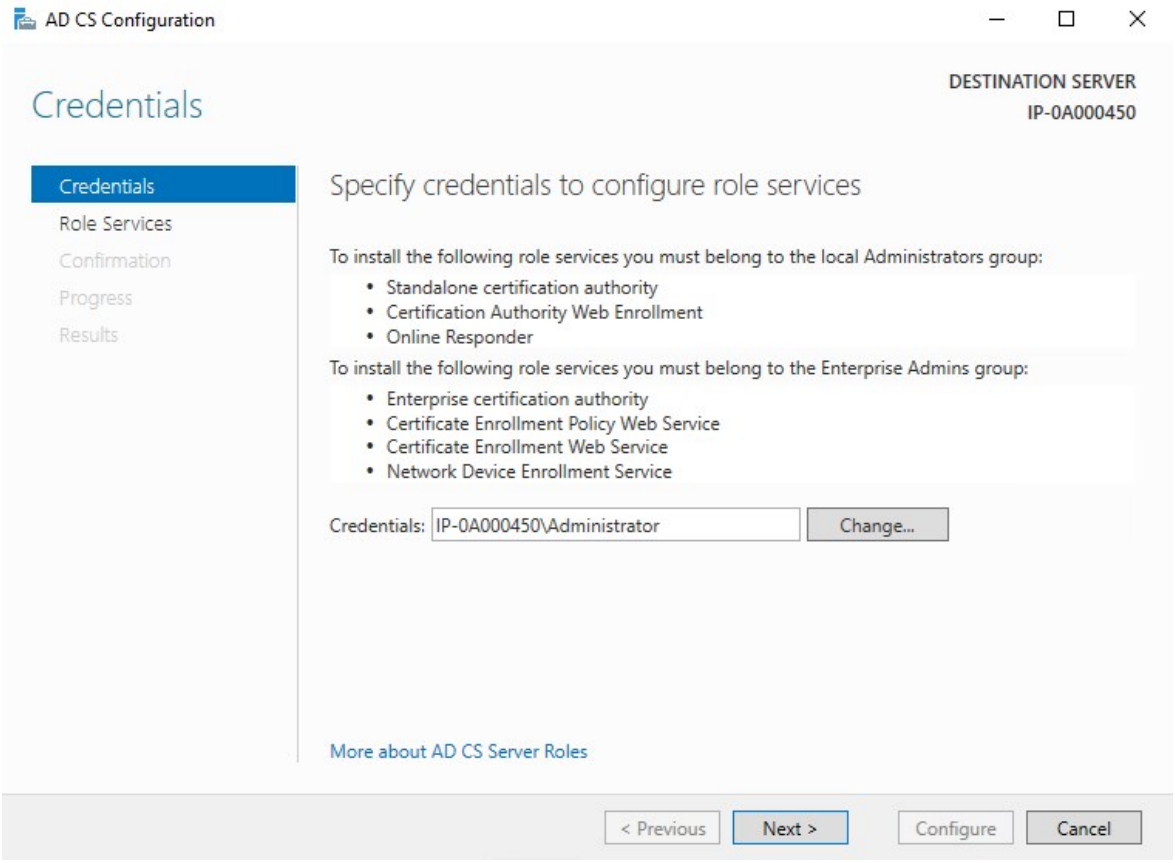
11. A message to begin post deployment configuration is listed under the **Notification Flag**.

    Click on the link to begin the configuration of the installed services.



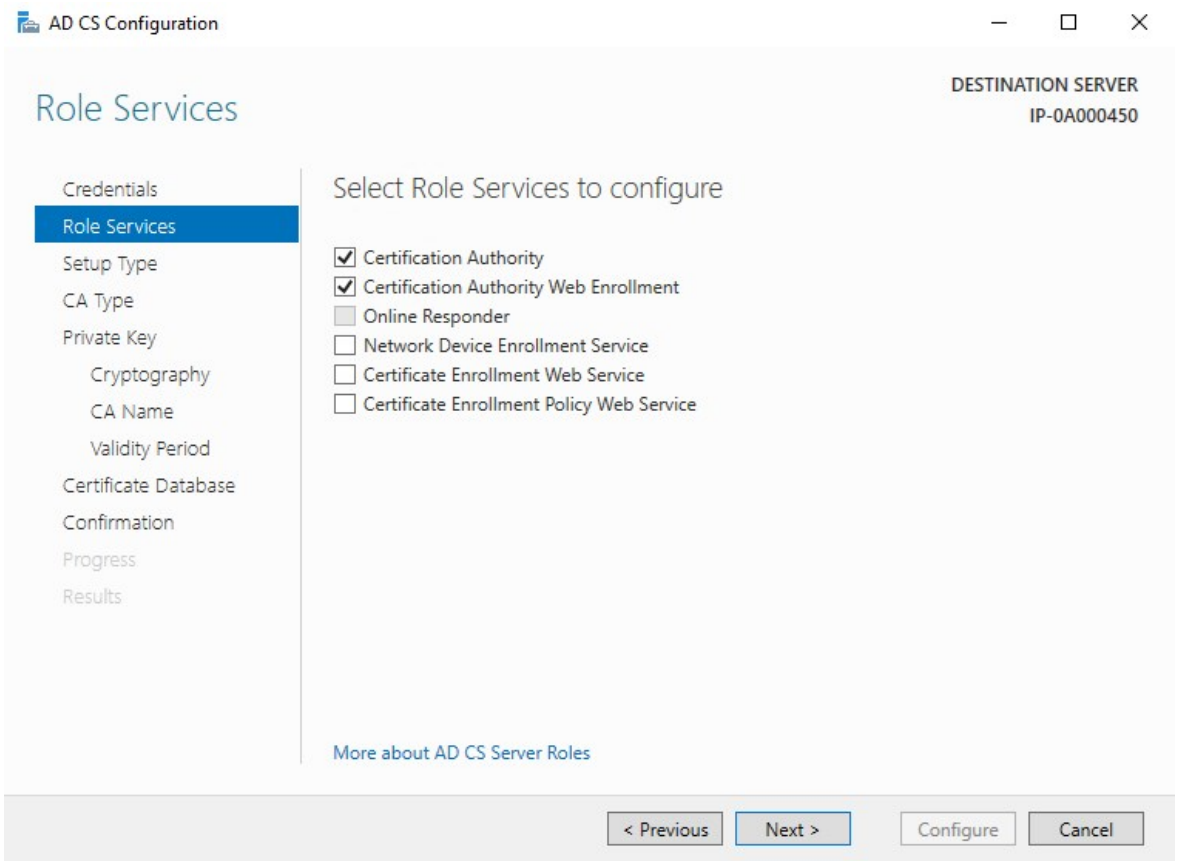
12. The **Active Directory Certificate Services** configuration wizard starts.

    In **Credentials**, select the user account required to run the installed services. As indicated in the text, membership in the local administrator and enterprise admin groups is required. Enter the required account information and click **Next**.

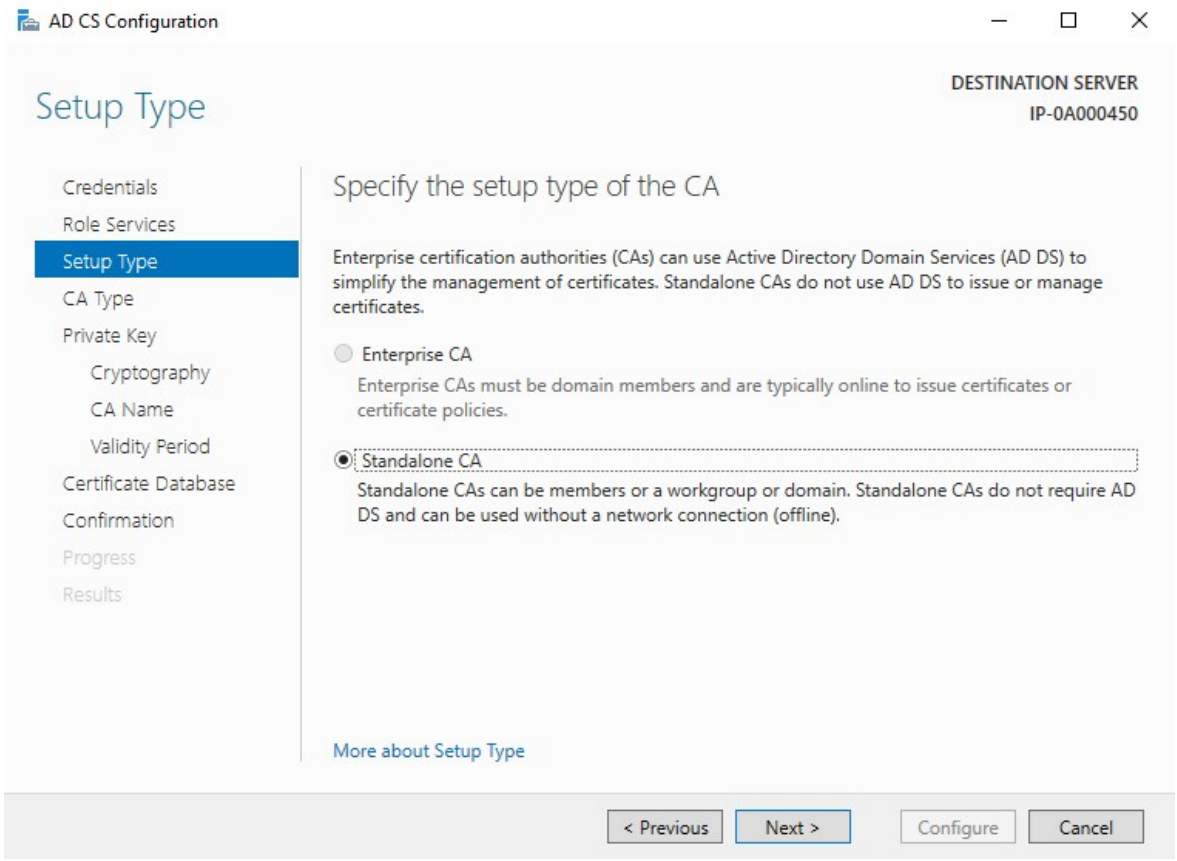


13. In **Role Services**, select the following services:
    - **Certification Authority**
    - **Certification Authority Web Enrollment**

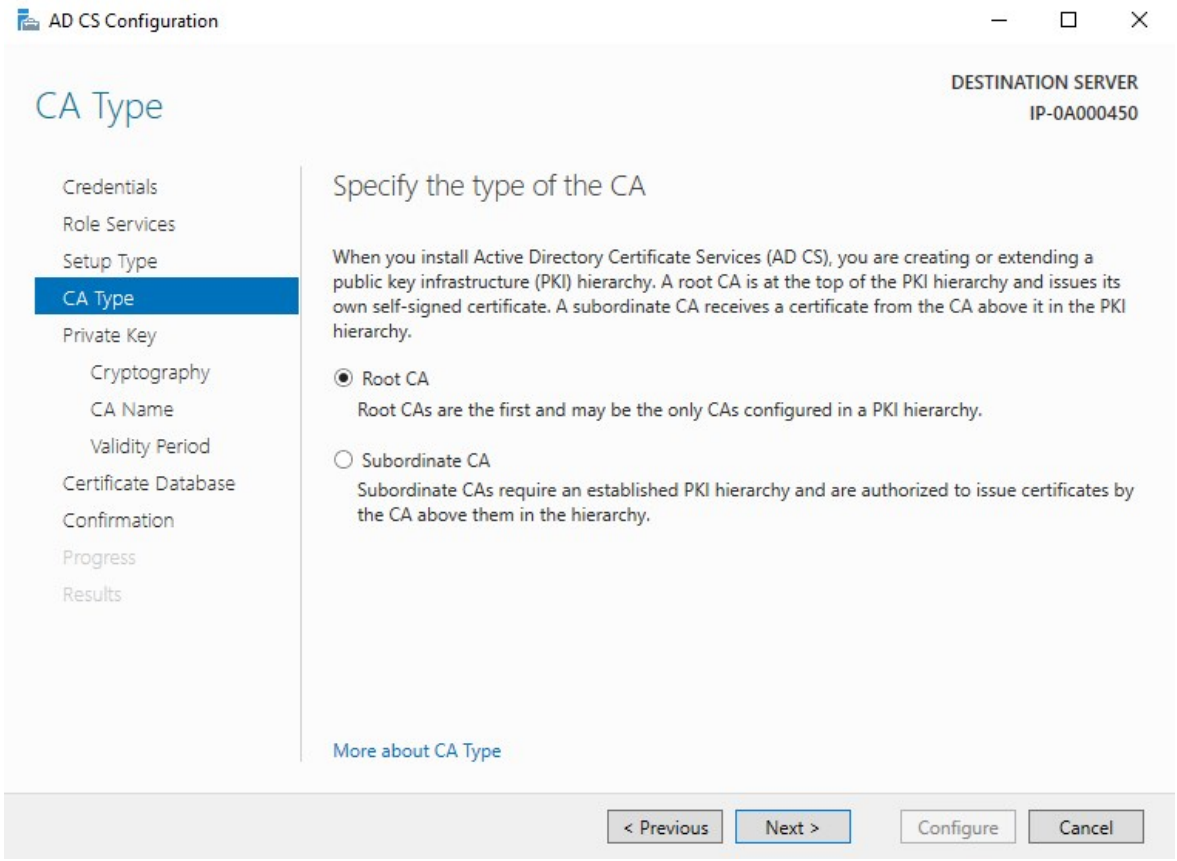
    Click **Next**.



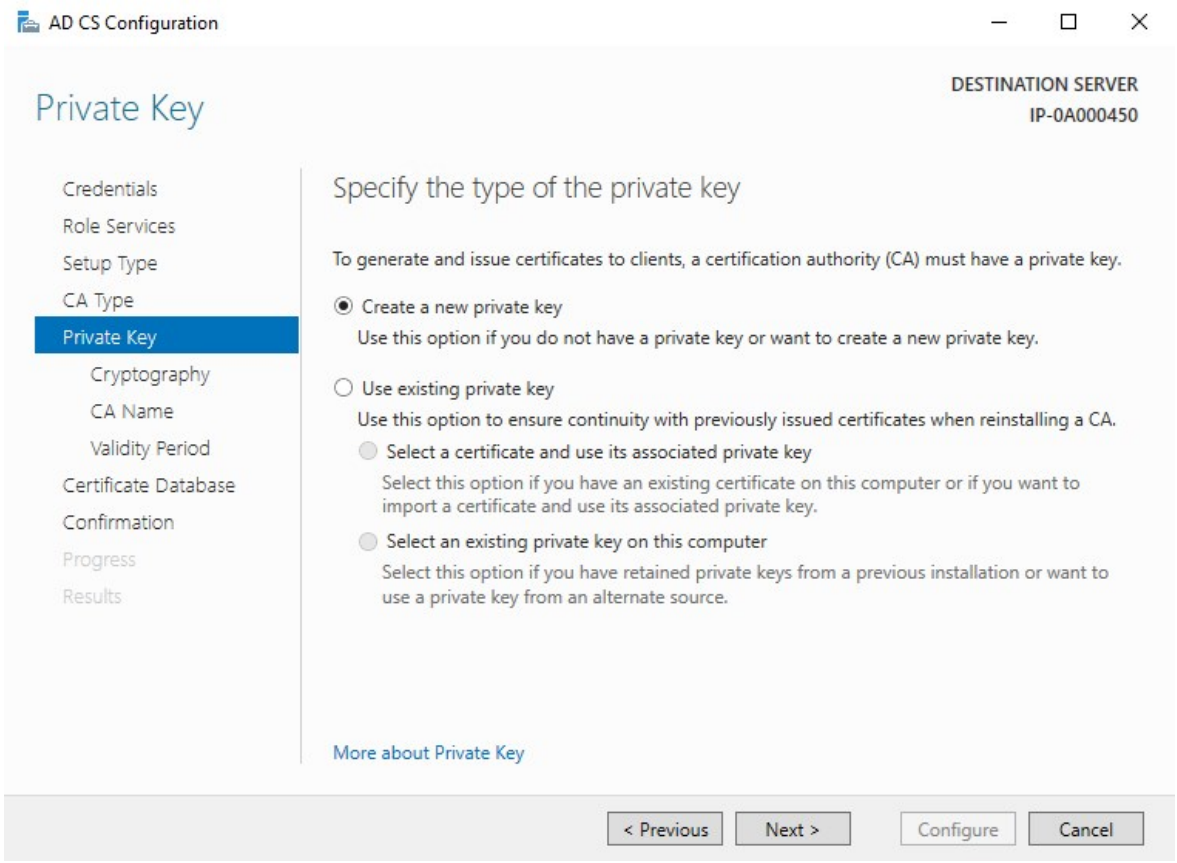
14. In **Setup Type**, select the **Standalone CA** option and click **Next**.



15. In **CA Type**, select the option to install a **Root CA**, and click **Next**.

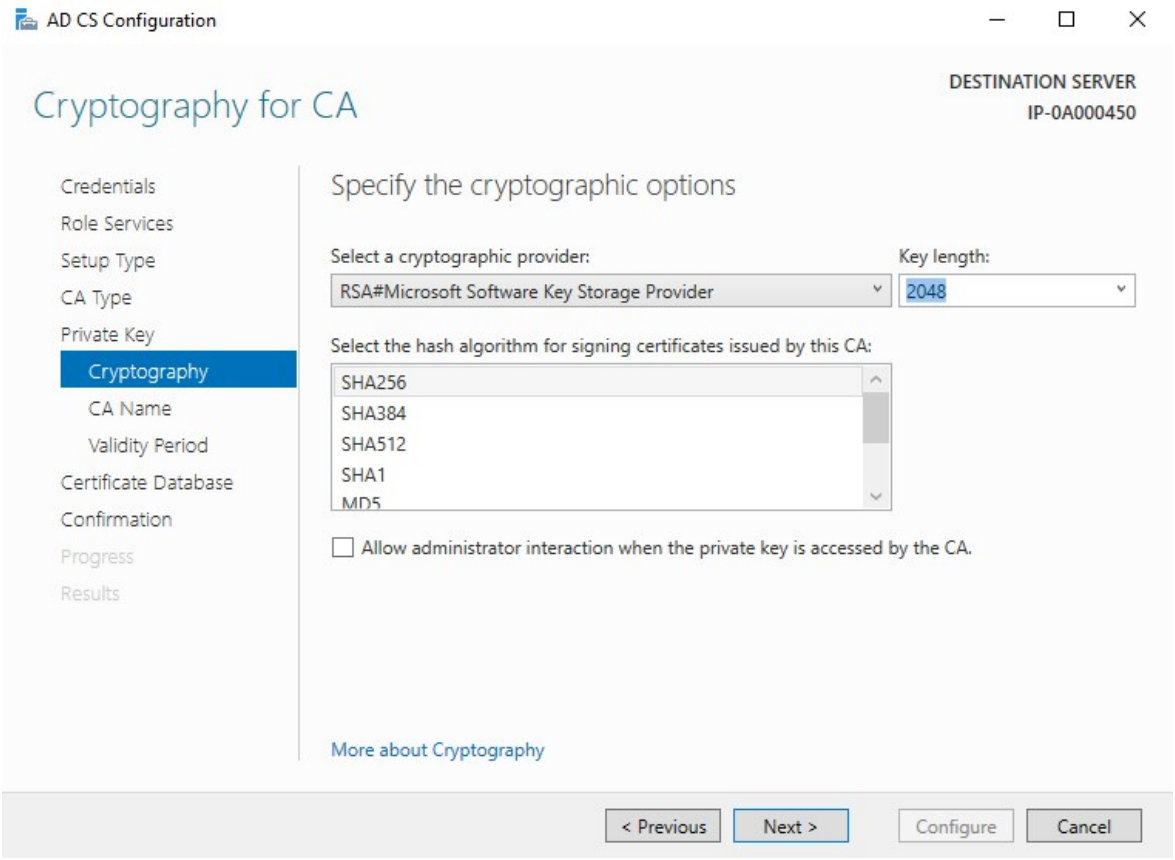


16. In **Private Key**, select the option to create a new private key, and click **Next**.



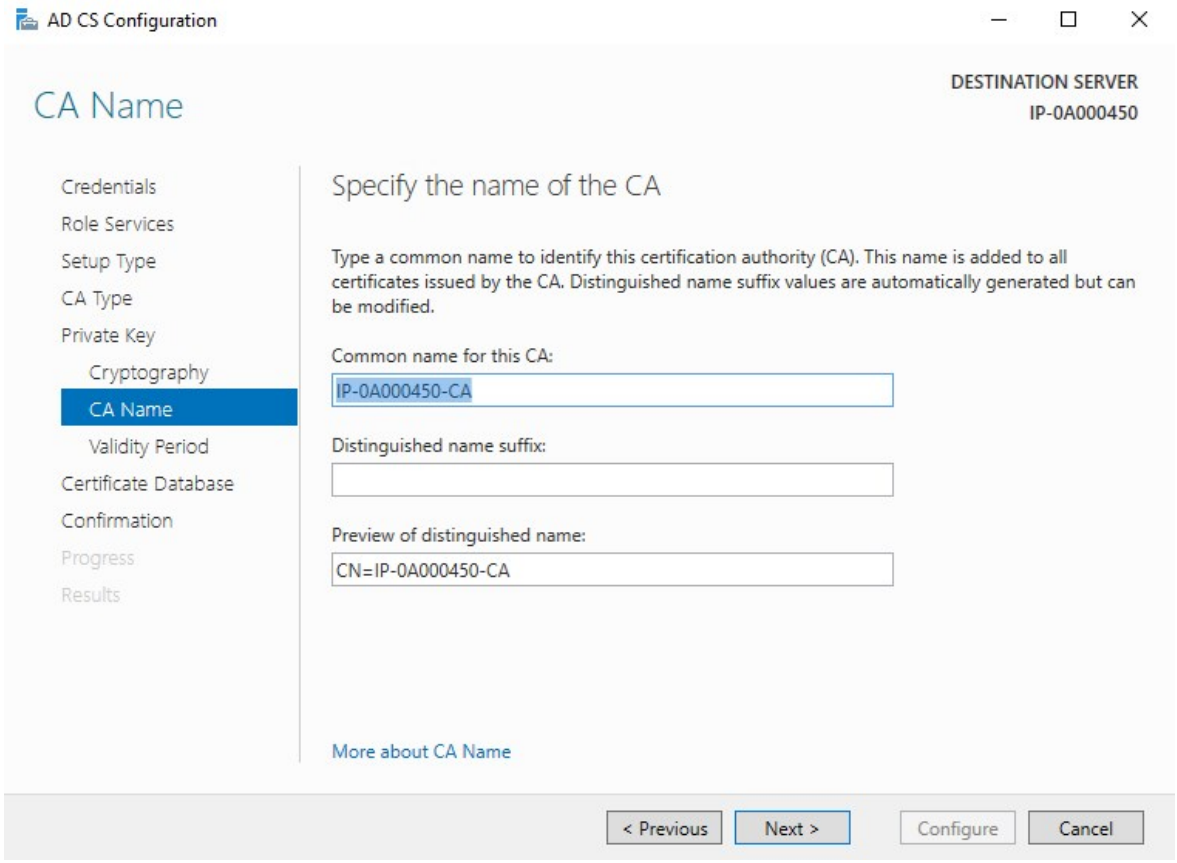
17. In **Cryptography**, select **RSA#Microsoft Software Key Storage Provider** for the cryptographic provider option with a **Key length** of 2048, and a hash algorithm of SHA256.

    Click **Next**.

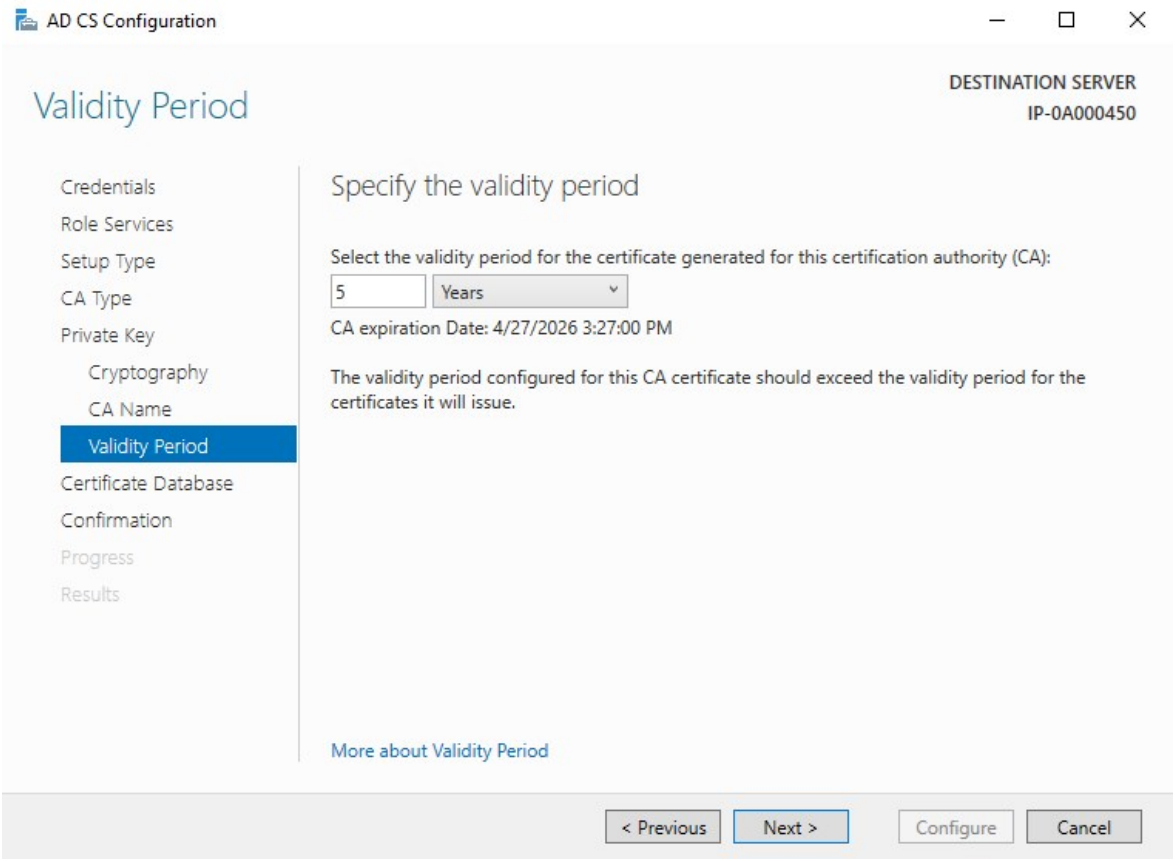


18. In **CA Name**, enter the name for the CA and click **Next**.

    By default the name is "localhost-CA" - assuming that the computer name of the local server is "localhost."



19. In **Validity Period**, select the default validity period of 5 years, and click **Next**.



20. In **Certificate Database**, enter the locations of the database and log database.

    The default database locations for the certificate store are: `C:\Windows\system32\CertLog`

    Click **Next**.

21. In **Confirmation**, review the selected configuration options and click **Configure** to begin the process of configuration.

22. When the configuration is done, click **Close**.

    When prompted to configure any additional role services, click **No**.

23. Reboot the local server to ensure it is ready to serve as the Active Directory Certificate Server.

Install certificates in a domain for communication with the Management Server or Recording Server

When client and server endpoints are all operating within a domain environment there is no requirement to distribute CA certificates to client workstations. Group Policy within the domain handles the automatic distribution of all trusted CA certificates to all users and computers in the domain.

This is because, when you install an enterprise root CA, it uses Group Policy to propagate its certificate to the Trusted Root Certification Authorities certificate store for all users and computers in the domain.

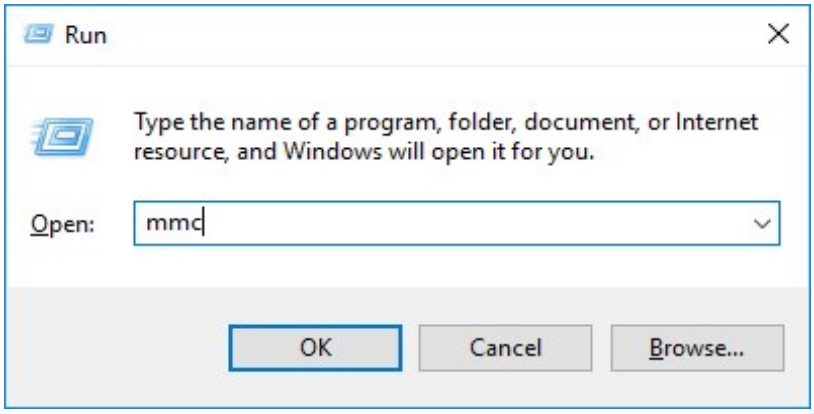
You must be a Domain Administrator or be an administrator with write access to Active Directory to install an enterprise root CA.

Microsoft provides extensive documentation for Windows Server operating systems, which includes templates for server certificates, installation of the CA, and certificate deployment can be found in Microsoft's Server Certificate Deployment Overview.

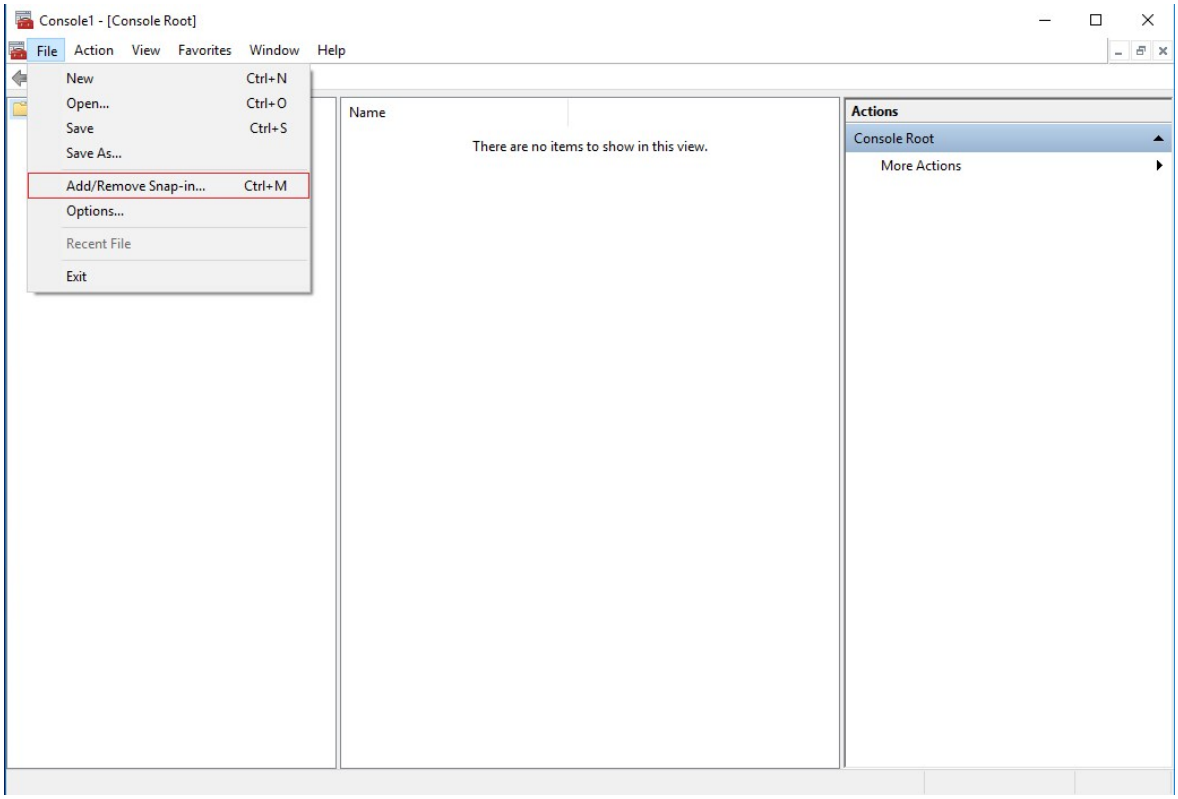
Add a CA certificate to the server

Add the CA certificate to the server by doing the following.

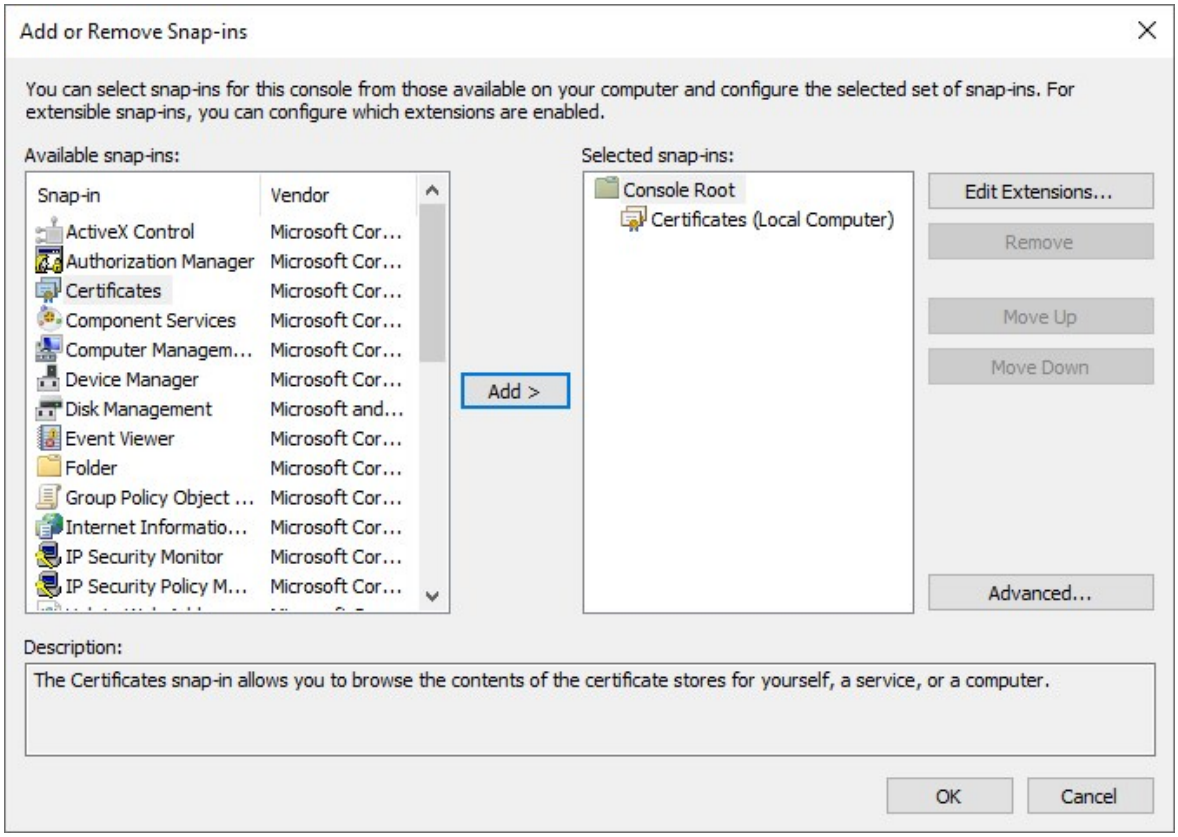
1. On the computer that hosts the XProtect server, open the Microsoft Management Console.



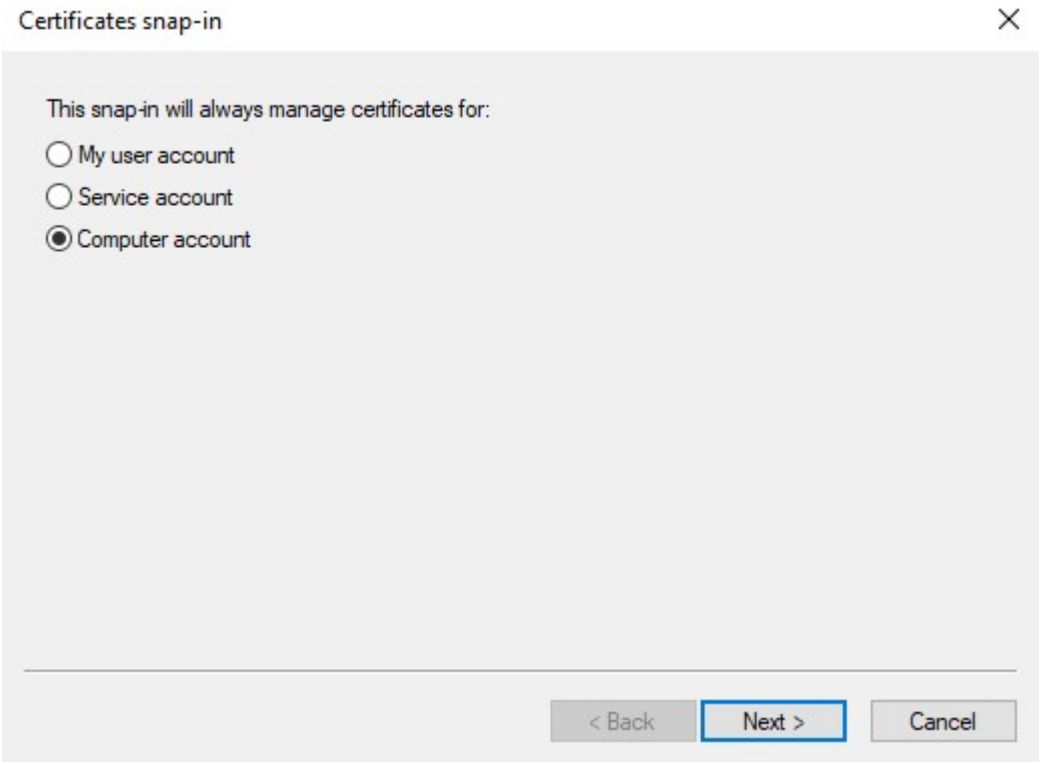
2. In the Microsoft Management Console, from the **File** menu select **Add/Remove Snap-in...**.



3. Select the **Certificates** snap-in and click **Add**.

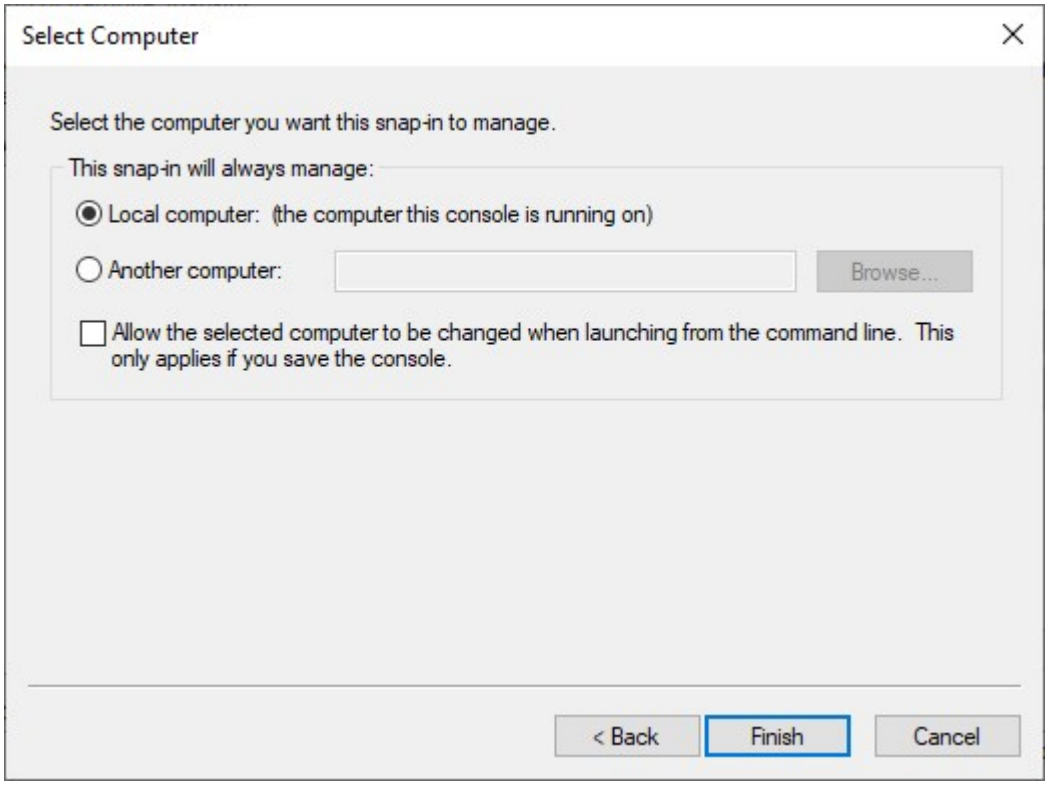


4. In **Certificates snap-in**, select **Computer account**.

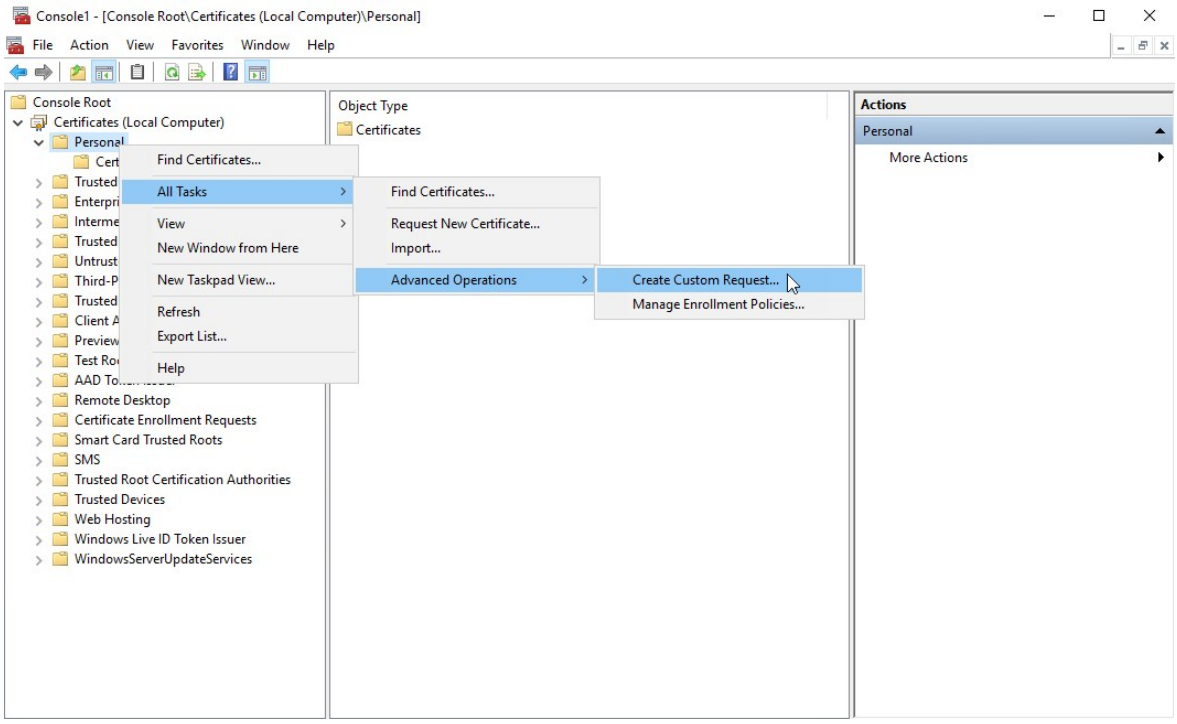


5. In **Select Computer**, select **Local computer**.

   Select **Finish**, then **OK**.



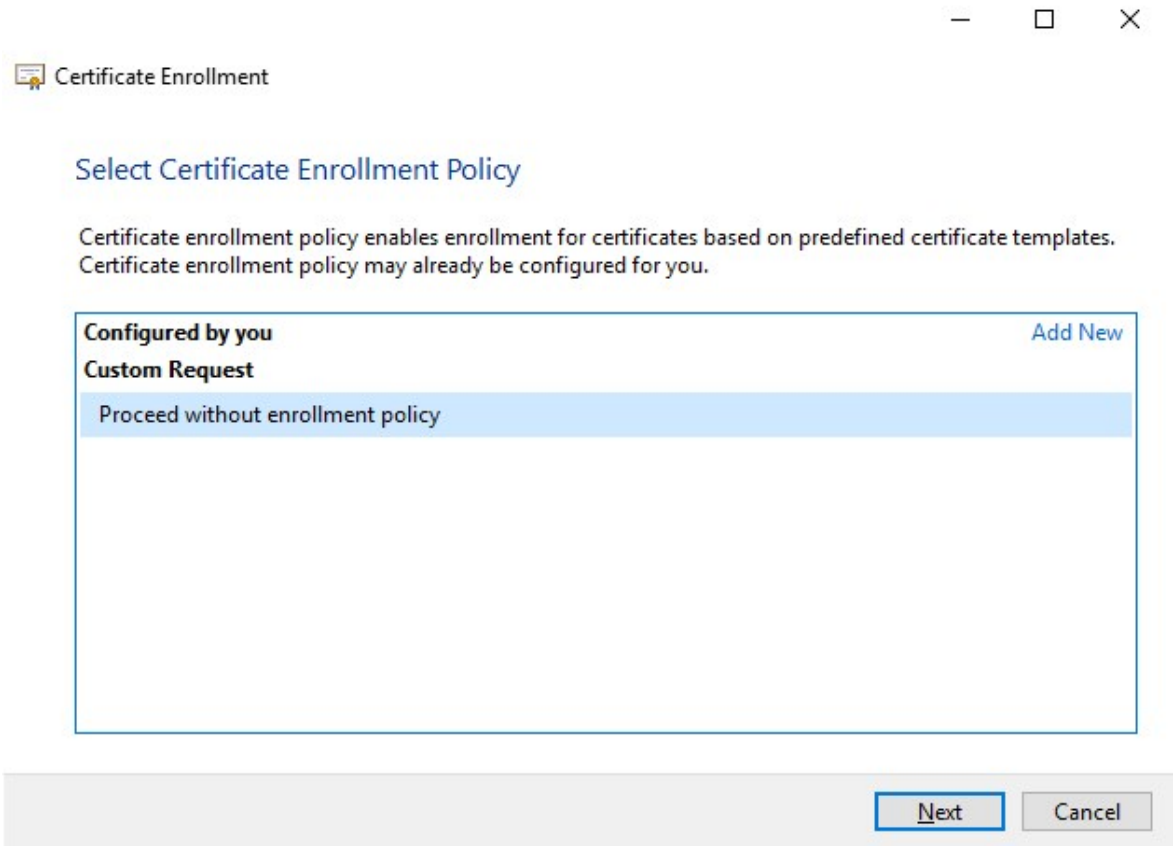
6. Expand the Certificates object. Right-click on the **Personal** folder and select **All Tasks** > **Advanced Operations** > **Create Custom Request**.



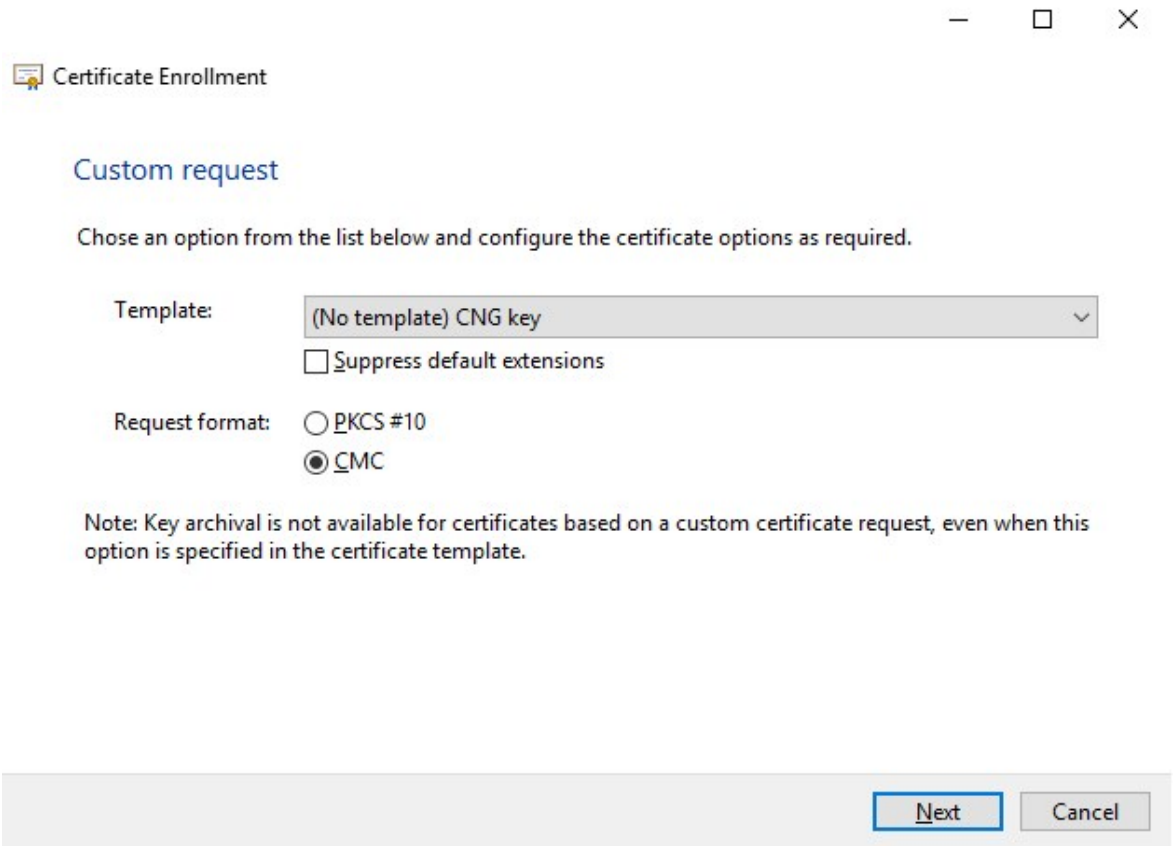
7. Click **Next** in the **Certificate Enrollment** wizard and select **Proceed without enrollment policy**.

> If your Group Policy already contains a Certificate Enrollment Policy, you will want to confirm the rest of this process with your Domain Administration team before proceeding.

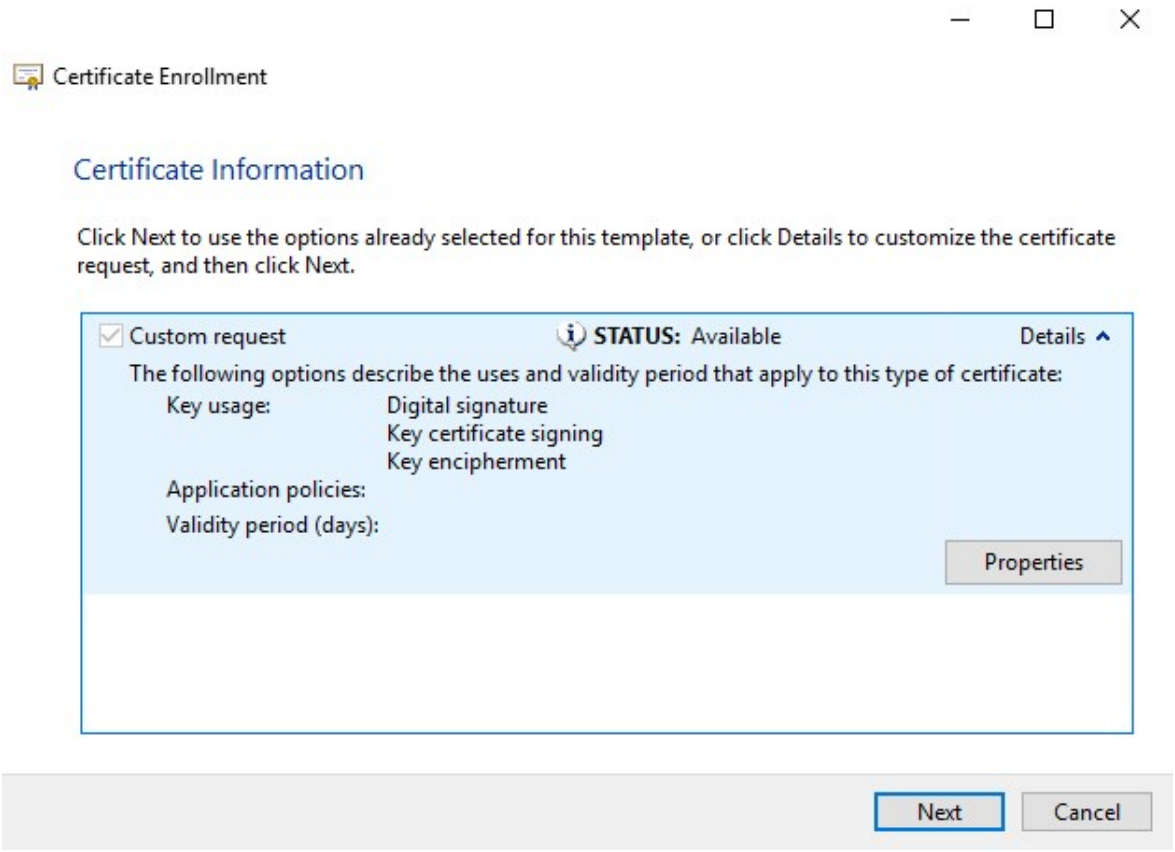
Click **Next**.



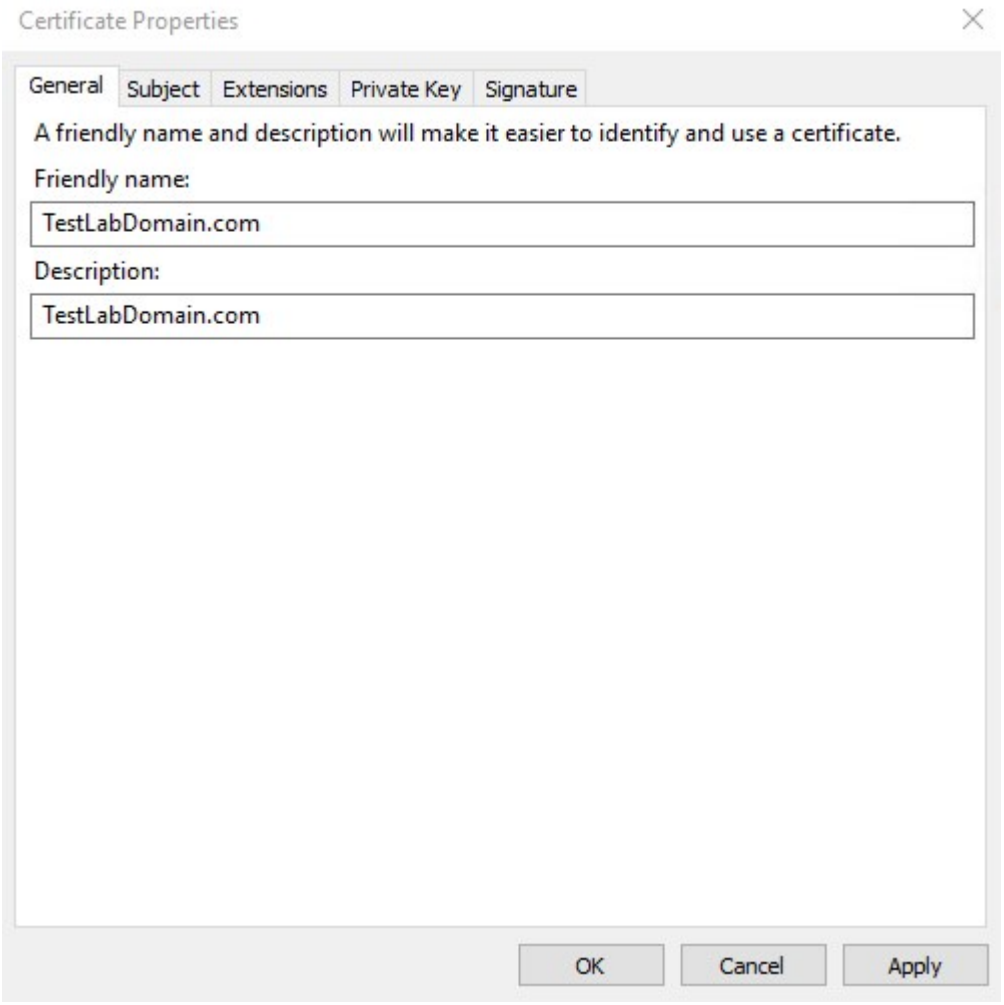
8. Select the **(No template) CNG Key** template and the **CMC** request format, and click **Next**.



9. Expand to view the **Details** of the custom request, and click **Properties**.

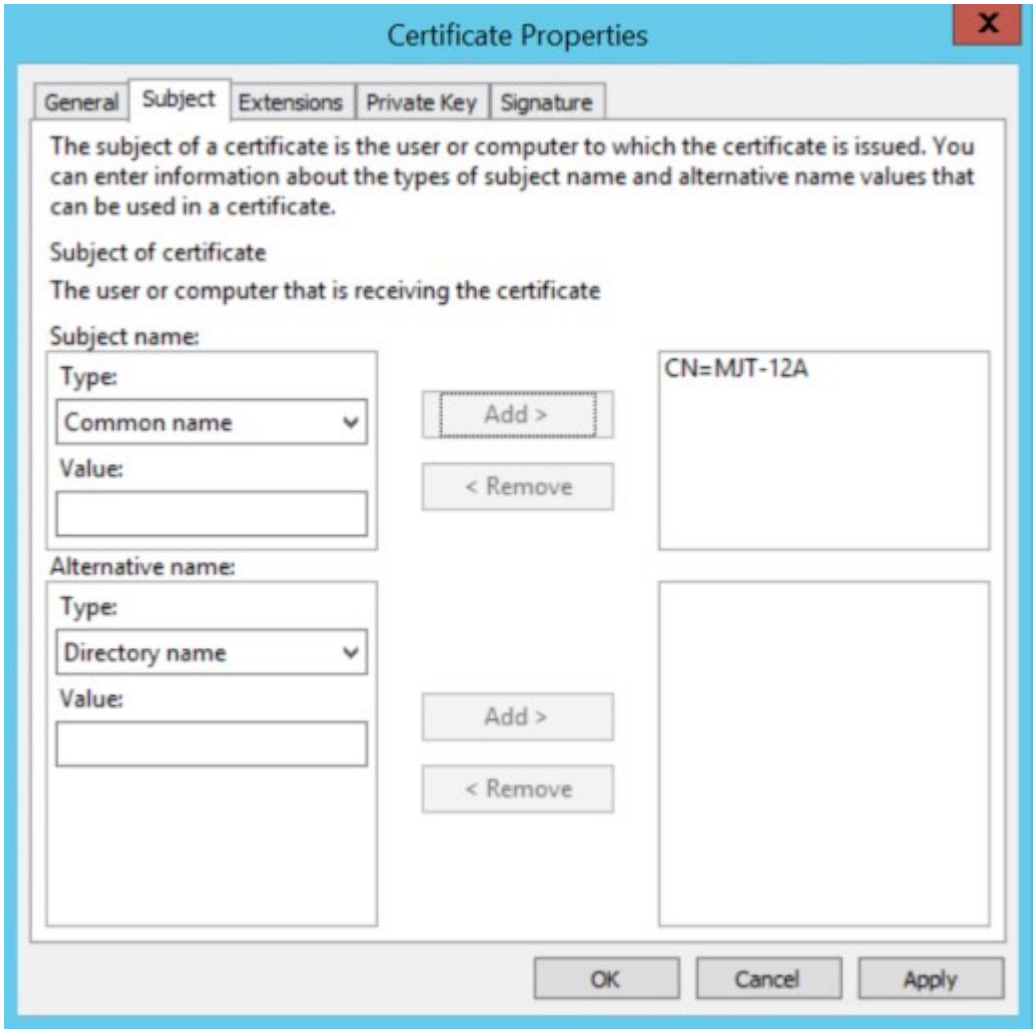


10. On the **General** tab, fill in the **Friendly name** and **Description** fields with the domain name, computer name, or organization.

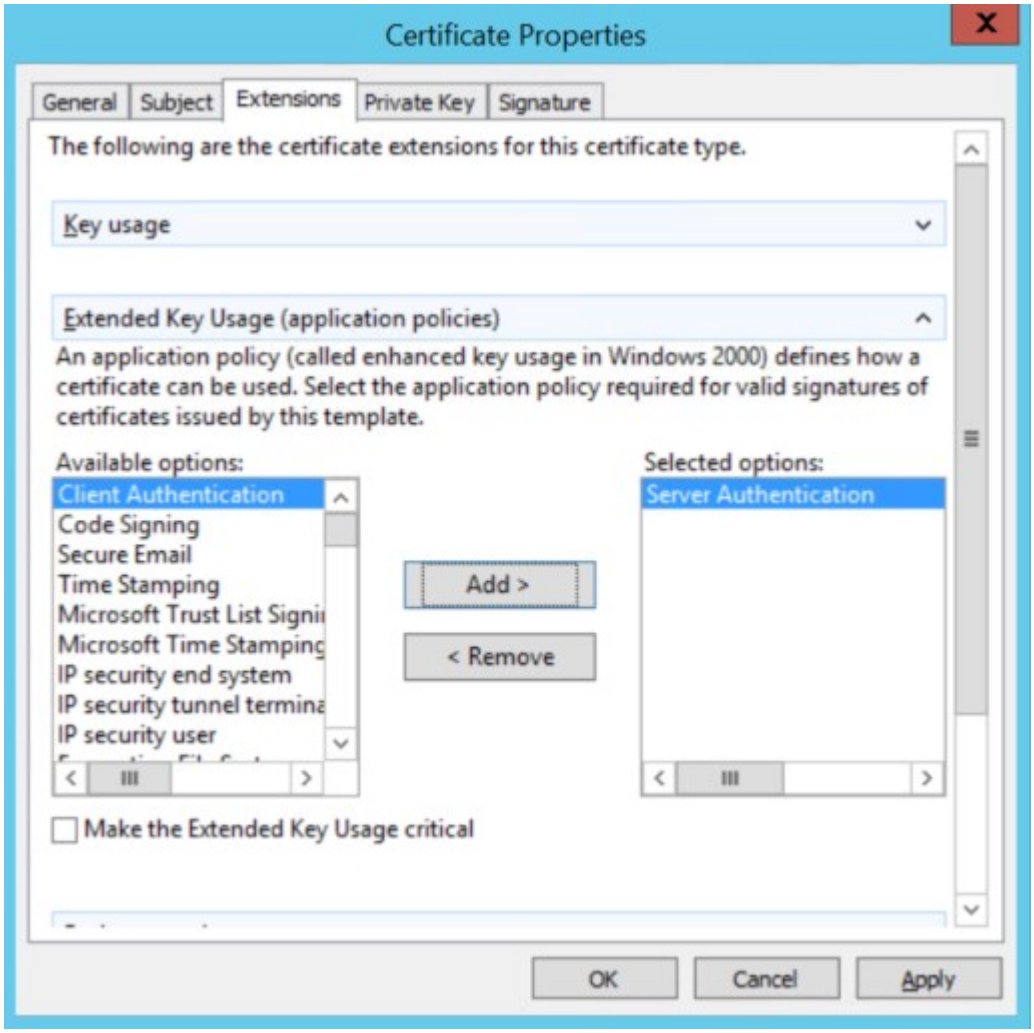


11. On the **Subject** tab, enter the required parameters for the subject name.

    In the subject name **Type**, enter in **Common Name** the host name of the computer where the certificate will be installed.



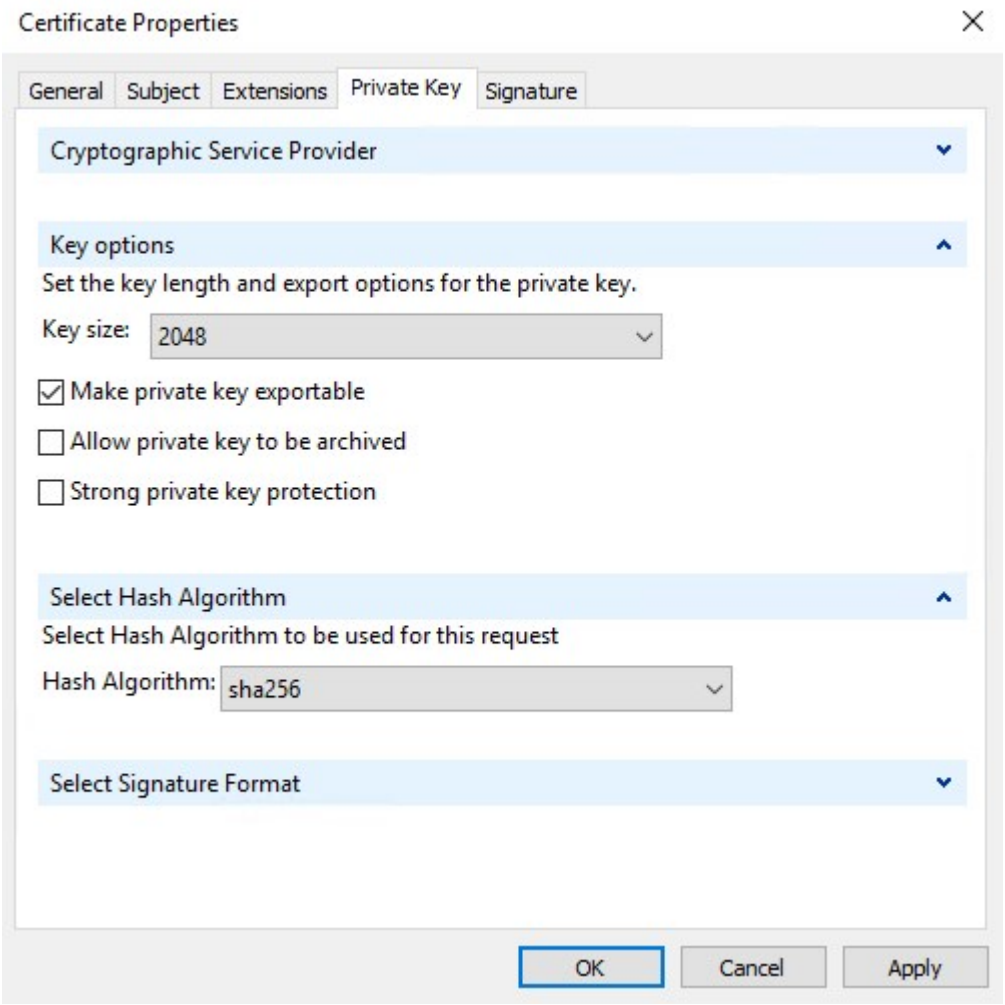
12. On the **Extensions** tab and expand the **Extended Key Usage (application policies)** menu. Add **Server Authentication** from the list of available options.



13. On the **Private Key** tab, expand the **Key options** menu.

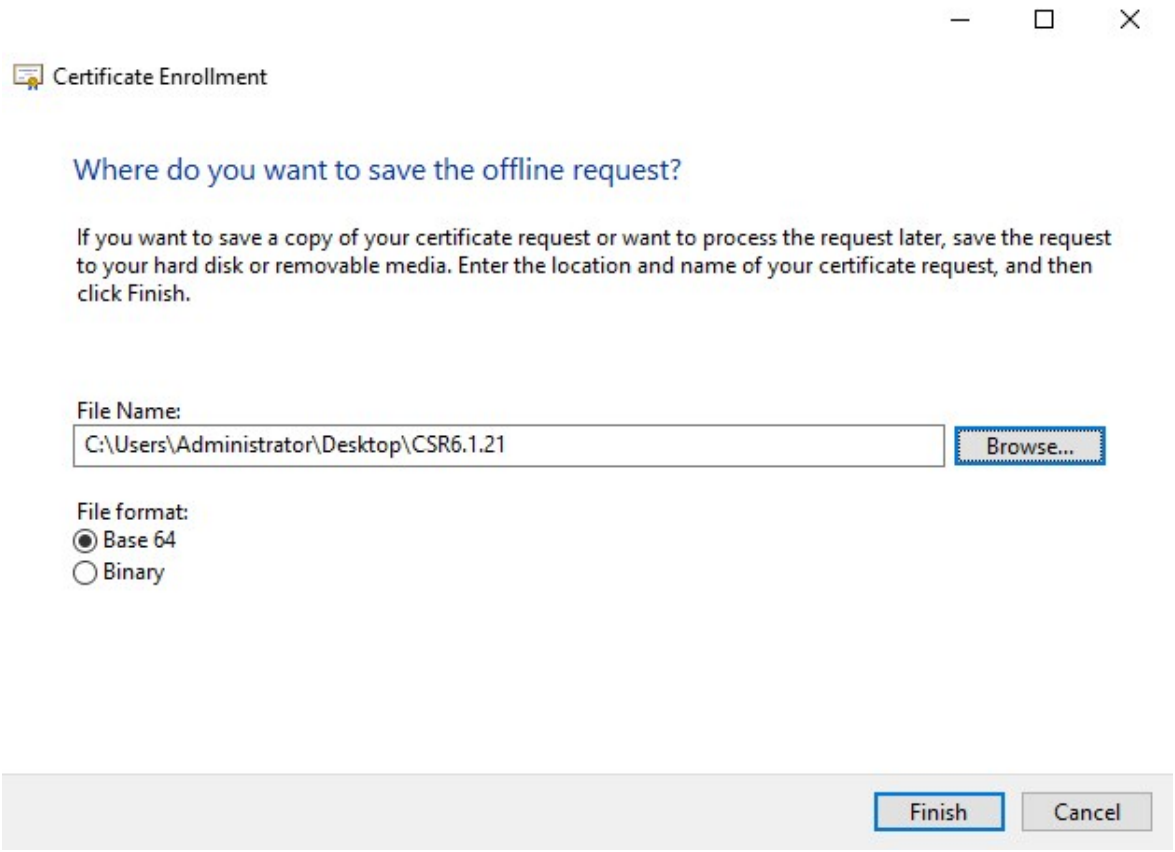
    Set the key size to 2048 and select the option to make the private key exportable.

    Click **OK**.



14. When all of the certificate properties have been defined, click **Next** on the **Certificate Enrollment** wizard.
15. Select a location to save the certificate request and a format. Browse to that location and specify a name for the .req file. The default format is base 64.

16. Click **Finish**.



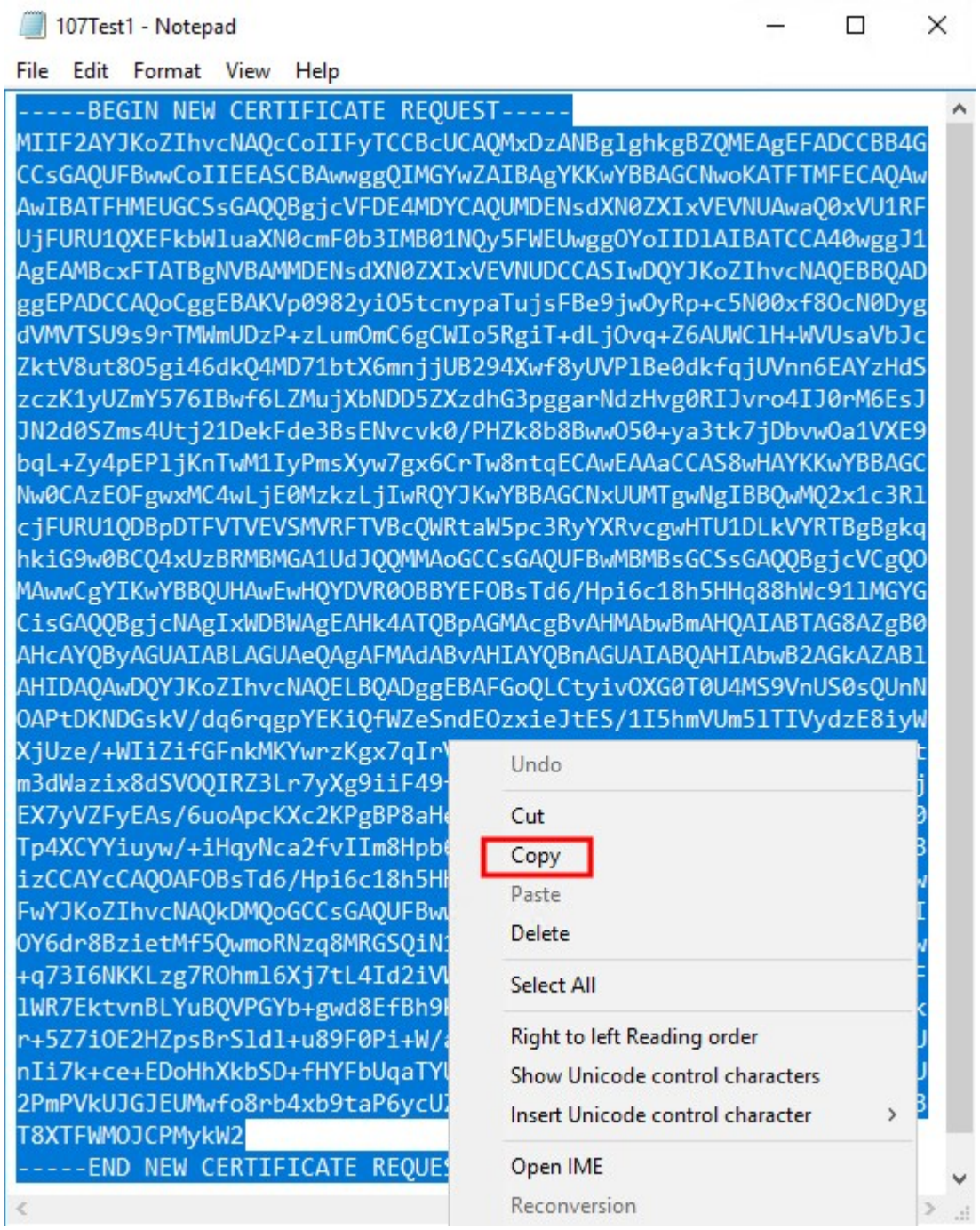
A .req file is generated, which you must use to request a signed certificate.

Upload the .req file to receive a signed certificate in return

You must copy the entire text of the .req file, including the begin and end lines, and paste the text to the internal Active Directory Certificate Services certificate authority in the network. See Install Active Directory Certificate Services on page 74.

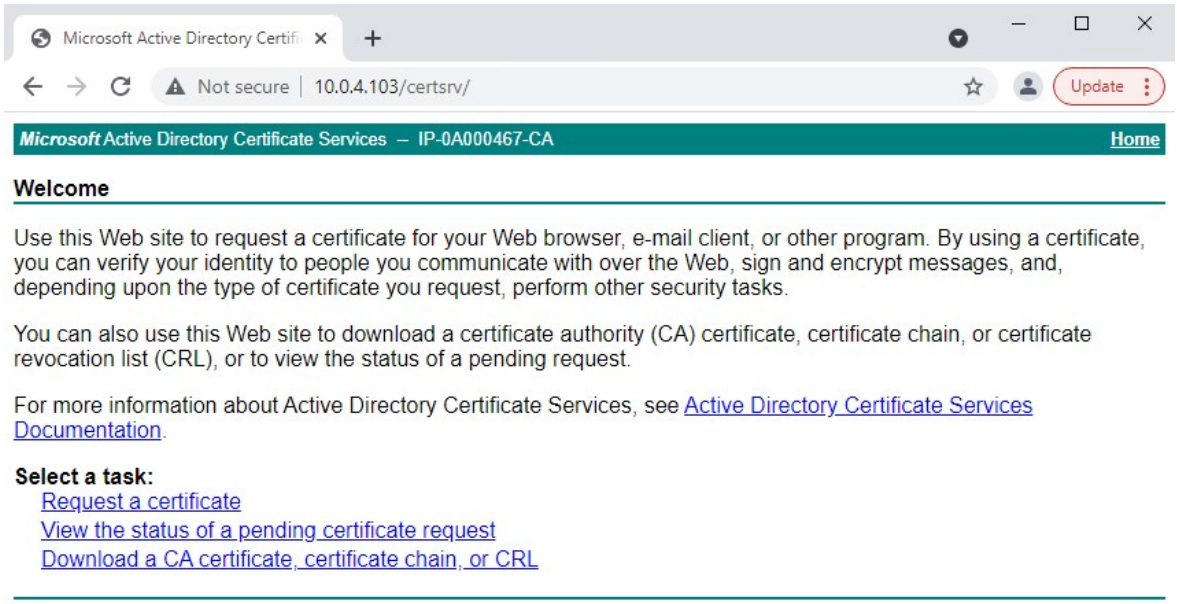
Unless your domain has only recently installed Active Directory Certificate Services, or it has been installed just for this purpose, you will need to submit this request following a separate procedure configured by your Domain Administration team. Please confirm this process with them before proceeding.

1. Browse to the location of the .req file and open it in Notepad.

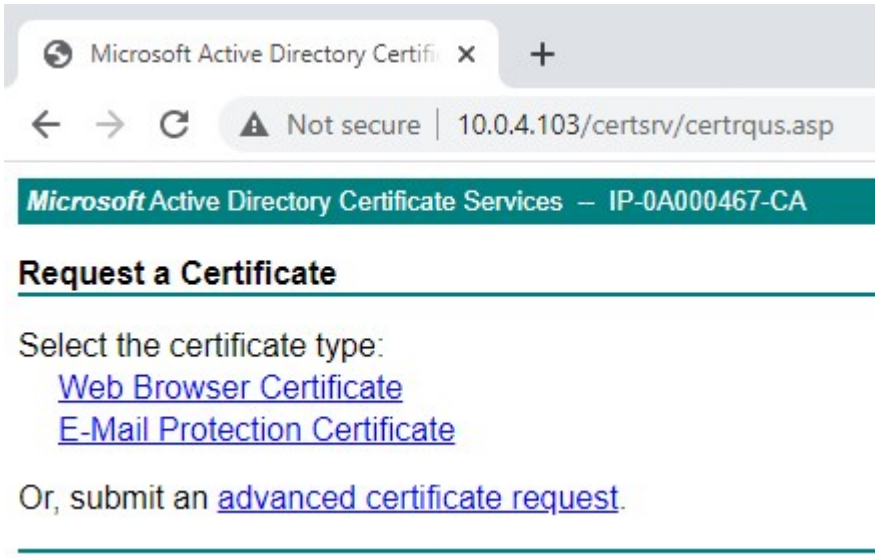


2. Copy the entire contents of the file. This includes the dashed lines marking the beginning and the end of the Certificate Request.

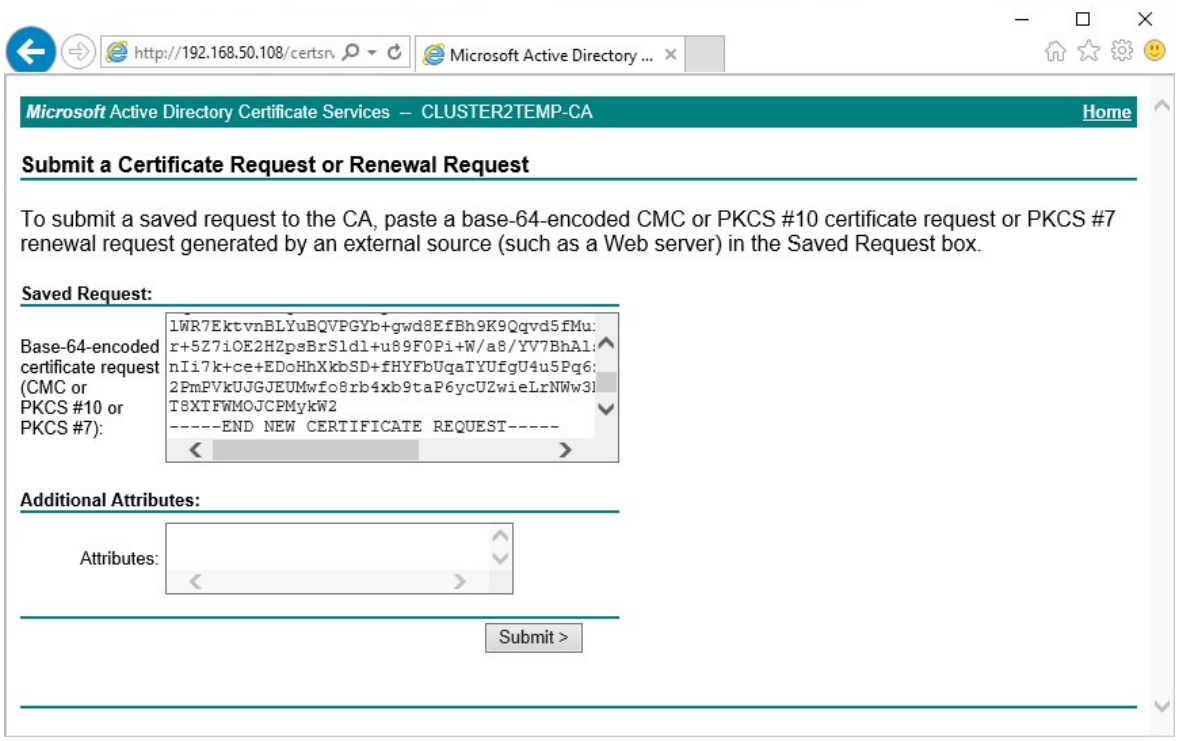
3. Open a web browser and enter the address of the Domain CA.



4. Click the **Request a certificate** link.
5. Click the **advanced certificate request** link.



6. Paste the contents of the .req file into the form. If it is required to select a Certificate Template, select **Web Server** from the Certificate Template list.



7. Click **Submit**.

   The site shows a message that the certificate will be issued in a few days.

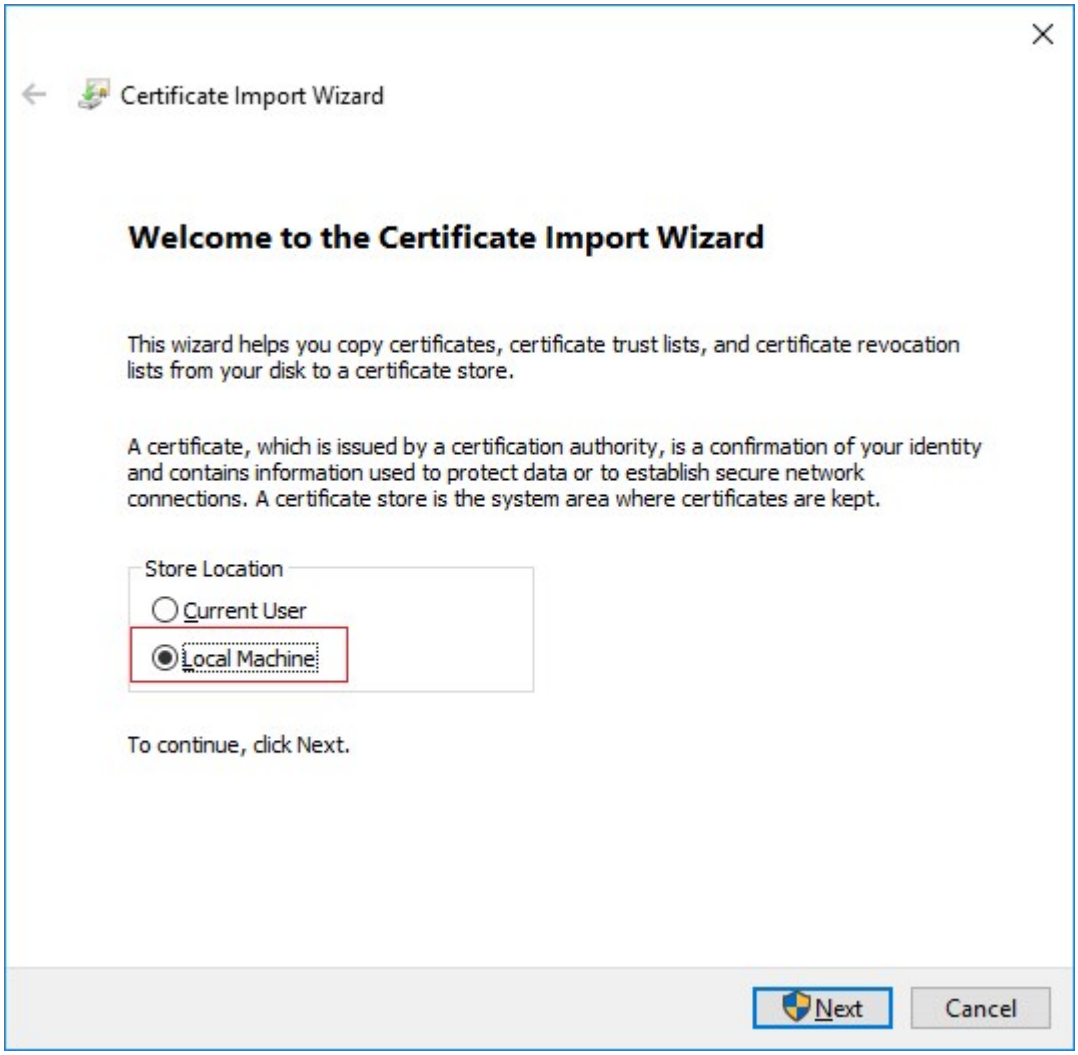
Your Domain Administration team will likely distribute and install the certificate for you. However, if the certificate is delivered to you, you can install it manually.

Install the certificate manually

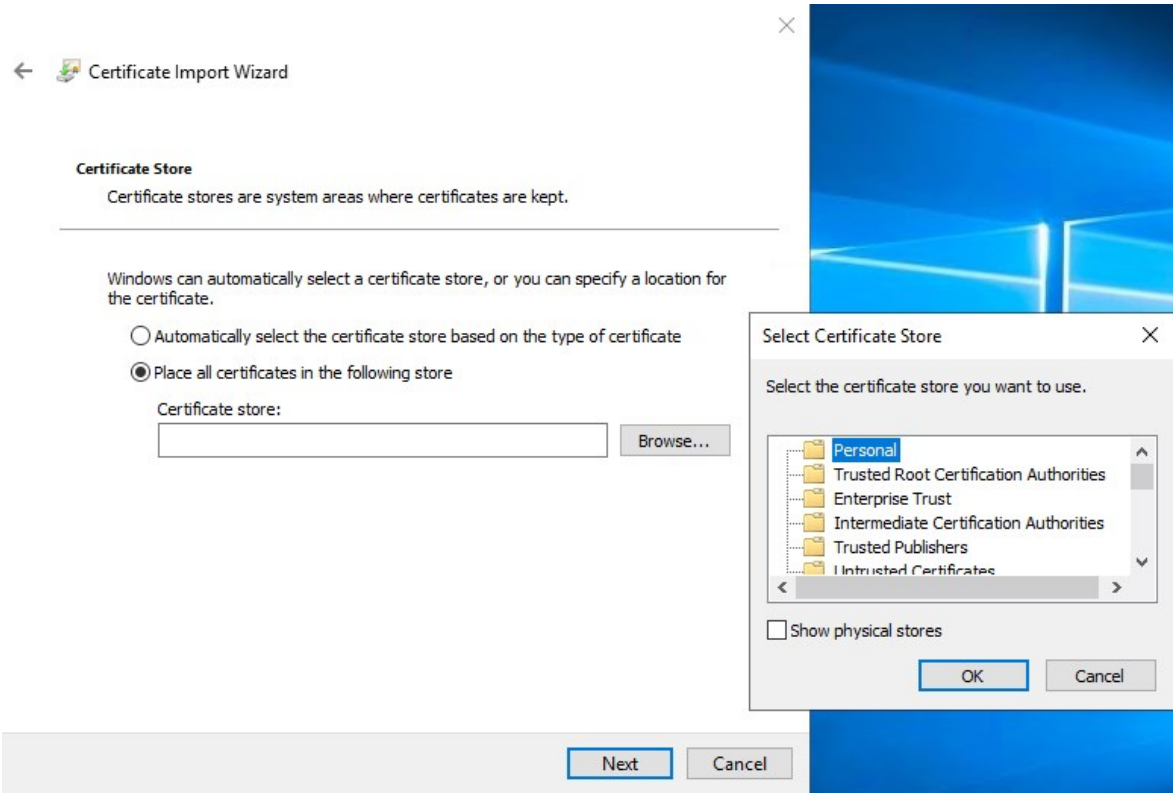
If the certificate is delivered to you, you can install it manually.

1. Locate the certificate file on the computer that hosts the Management Server or Recording Server .
2. Right-click the certificate and select **Install Certificate**.
3. Accept the security warning if it appears.

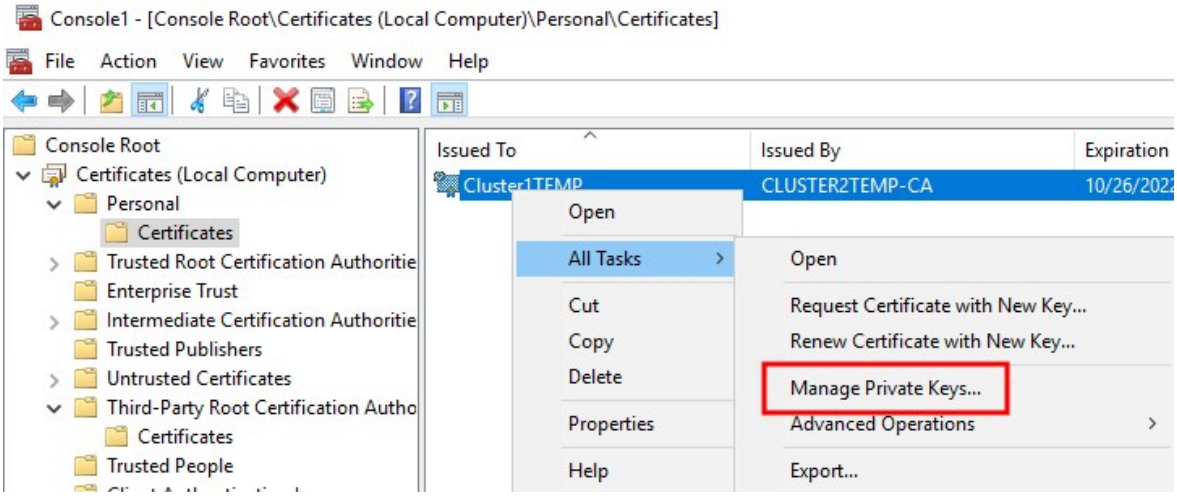
   Select to install the certificate for the current user and click **Next**.



4. Choose a storage location, and browse to the Personal certificate store, and click **Next**.



5. Finish the **Install Certificate** wizard.
6. Go to the Microsoft Management Console (MMC) certificates snap-in.
7. In the console, browse to the personal store where the certificate is installed. Right-click on the certificate and select **All Tasks** > **Manage Private Keys**.



8. Verify that the account that is running the Milestone XProtect Management Server, Recording Server, or Mobile Server software is in the list of users with permission to use the certificate.

   Make sure that the user has both Full Control and Read permissions enabled.

   > By default, XProtect software uses the NETWORK SERVICE account. In a domain environment, service accounts are commonly used to install and run XProtect services. You will need to discuss this with your Domain Administration team, and have the proper permissions added to the service accounts if it hasn't been configured properly already. Confirm this before proceeding.

Enable server encryption for Management Servers and Recording Servers

Once the certificate is installed with the correct properties and permissions, do the following.

1. On a computer with a Management Server or Recording Server installed, open the **Server Configurator** from:

   - The Windows Start menu

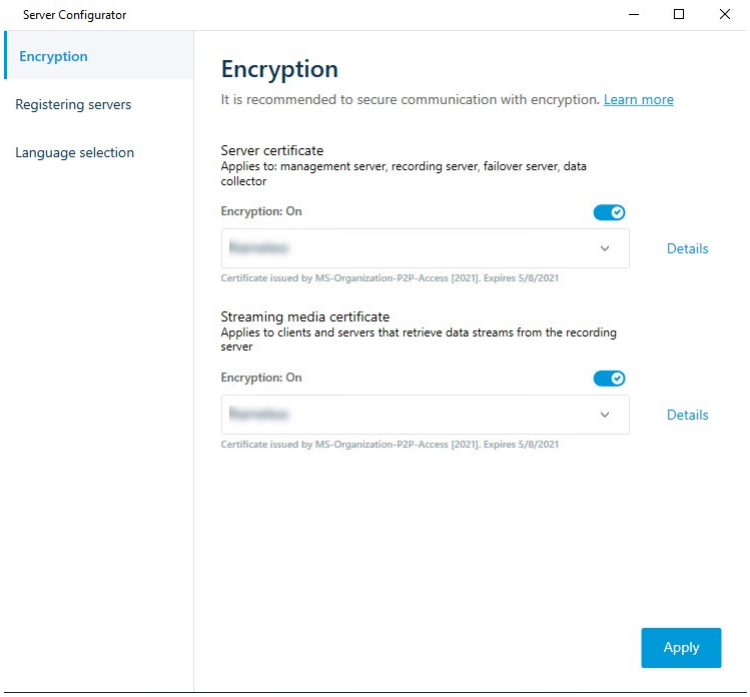
   or

   - The server manager, by right-clicking the server manager icon on the computer task bar

2. In the **Server Configurator**, under **Server certificate**, turn on **Encryption**.
3. Click **Select certificate** to open a list with unique subject names of certificates that have a private key and that are installed on the local computer in the Windows Certificate Store.
4. Select a certificate to encrypt communication between the recording server, management server, failover server, and data collector server.

   Select **Details** to view Windows Certificate Store information about the selected certificate.

   The Recording Server service user has been given access to the private key. It is required that this certificate is trusted on all clients.



5. Click **Apply**.

When you apply certificates, the recording server will be stopped and restarted. Stopping the Recording Server service means that you cannot record and view live video while you are verifying or changing the recording server's basic configuration.

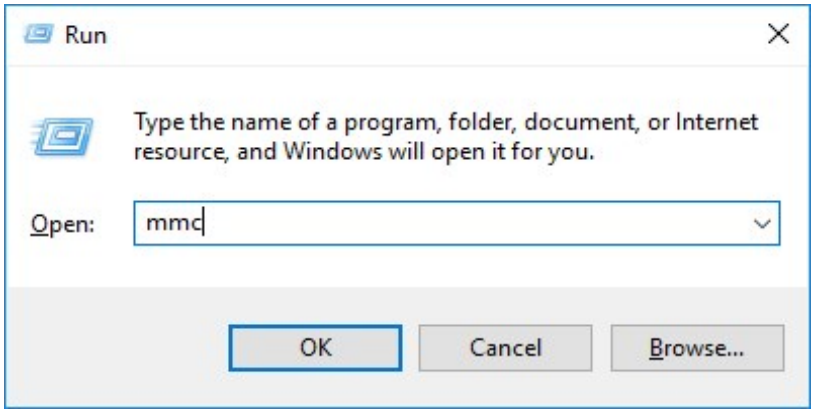
Install certificates in a Workgroup environment for communication with the Management Server or Recording Server

When operating in a Workgroup environment, it is assumed that there is no certificate authority infrastructure. To distribute certificates, it is required to create a certificate authority infrastructure. There is also a requirement to distribute the certificate keys to client workstations. Except for these requirements, the process of requesting and installing a certificate on a server is similar to both the domain and commercial CA scenarios.

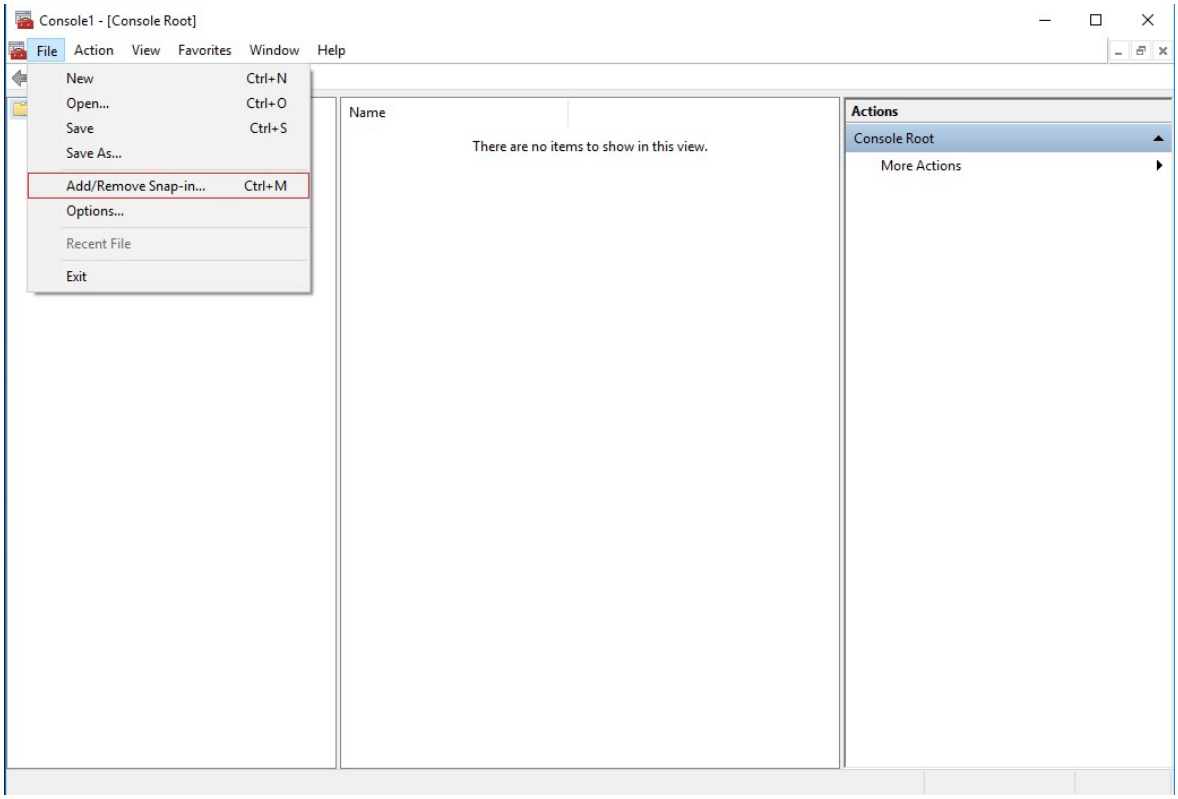
Add a CA certificate to the server

Add the CA certificate to the server by doing the following.

1. On the computer that hosts the XProtect server, open the Microsoft Management Console.

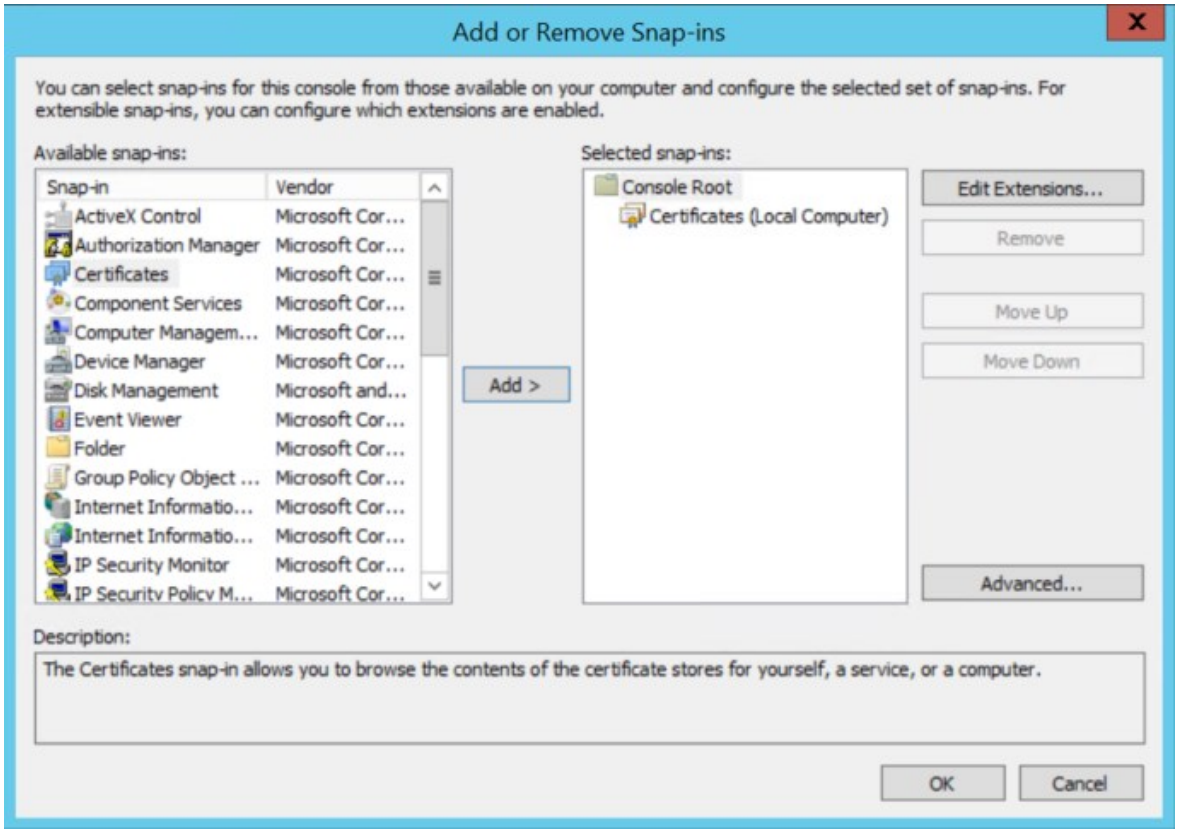


2. In the Microsoft Management Console, from the **File** menu select **Add/Remove Snap-in...**.

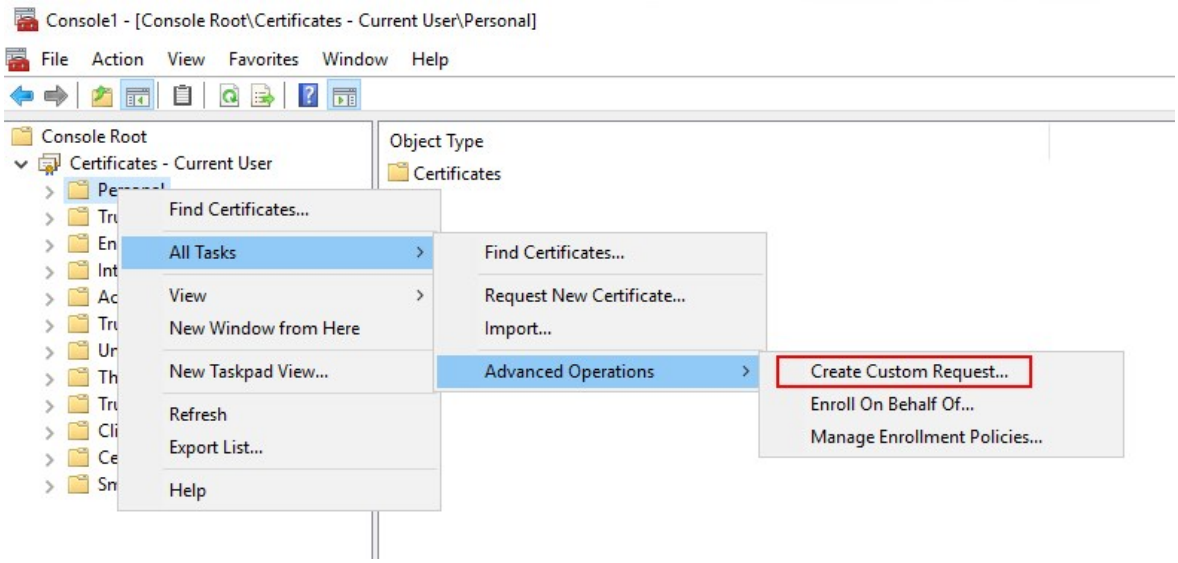


3. Select the **Certificates** snap-in and click **Add**.

   Click **OK**.

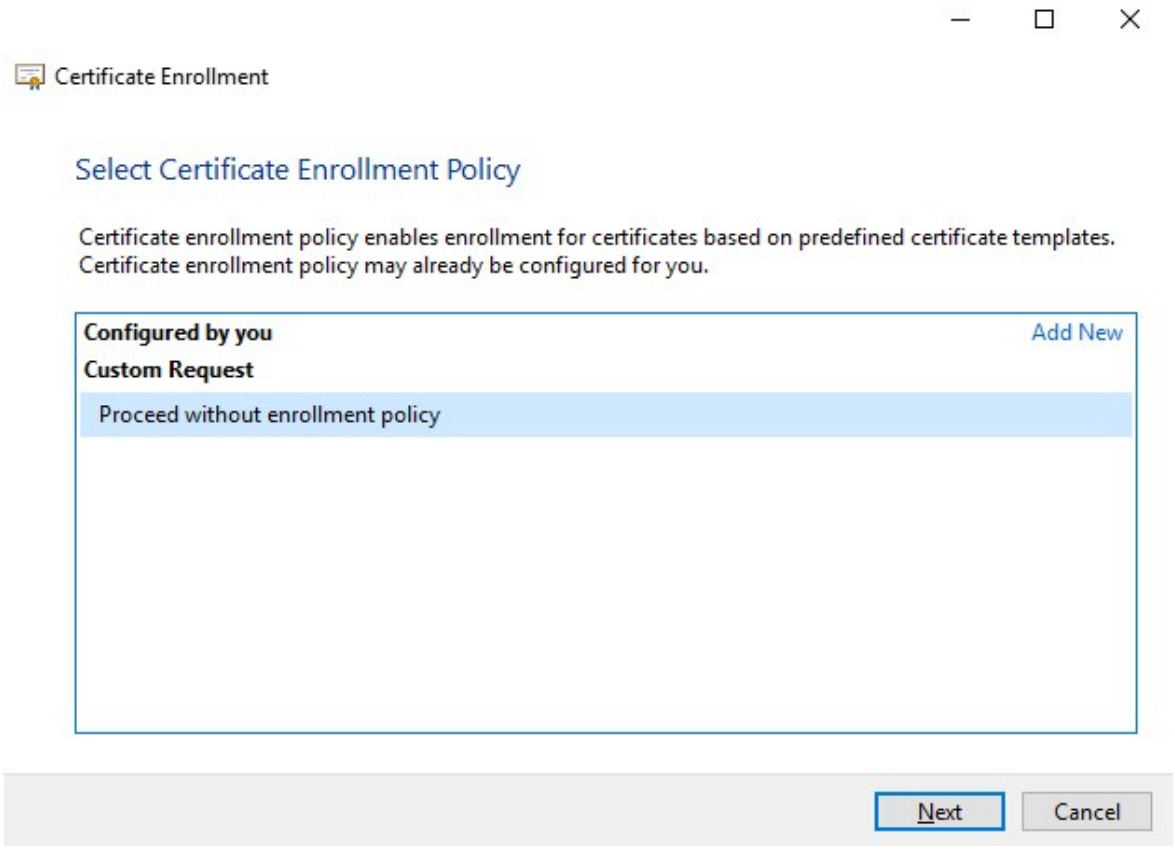


4. Expand the Certificates object. Right-click on the **Personal** folder and select **All Tasks** > **Advanced Operations** > **Create Custom Request**.

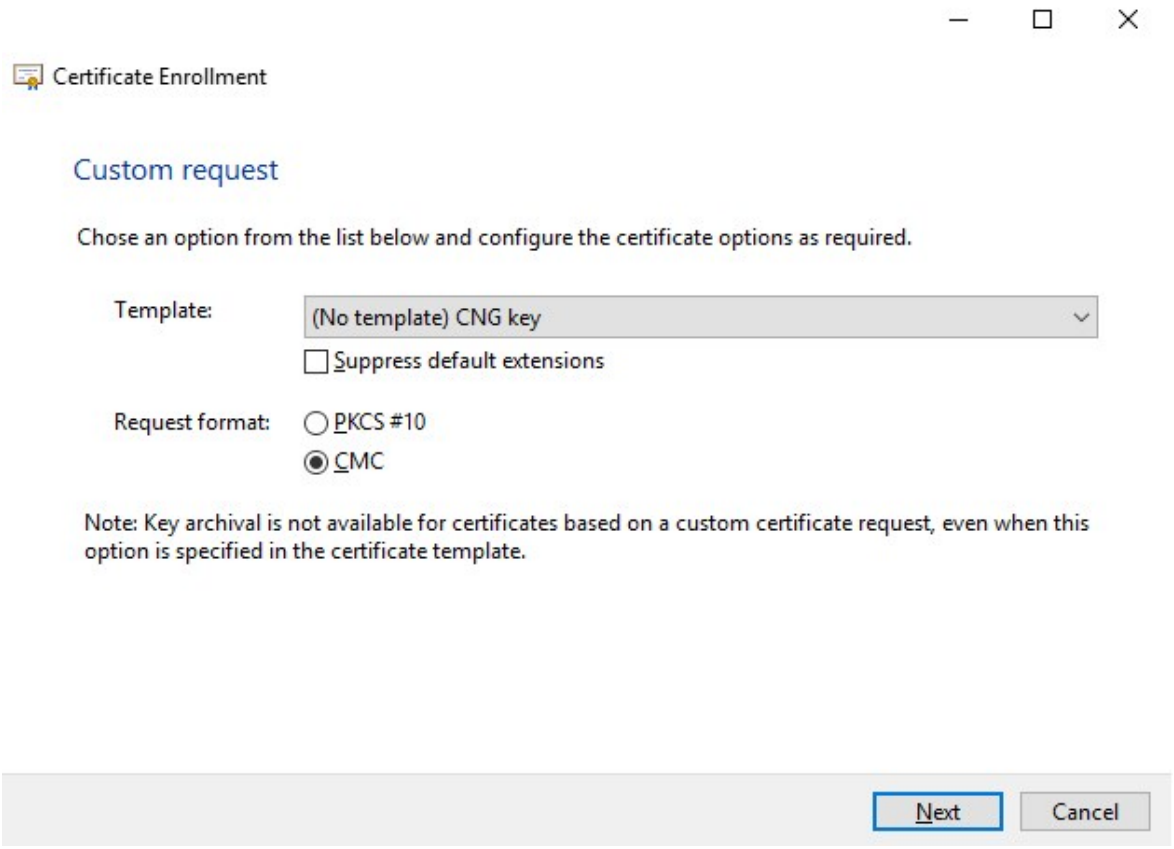


5. Click **Next** in the **Certificate Enrollment** wizard and select **Proceed without enrollment policy**.

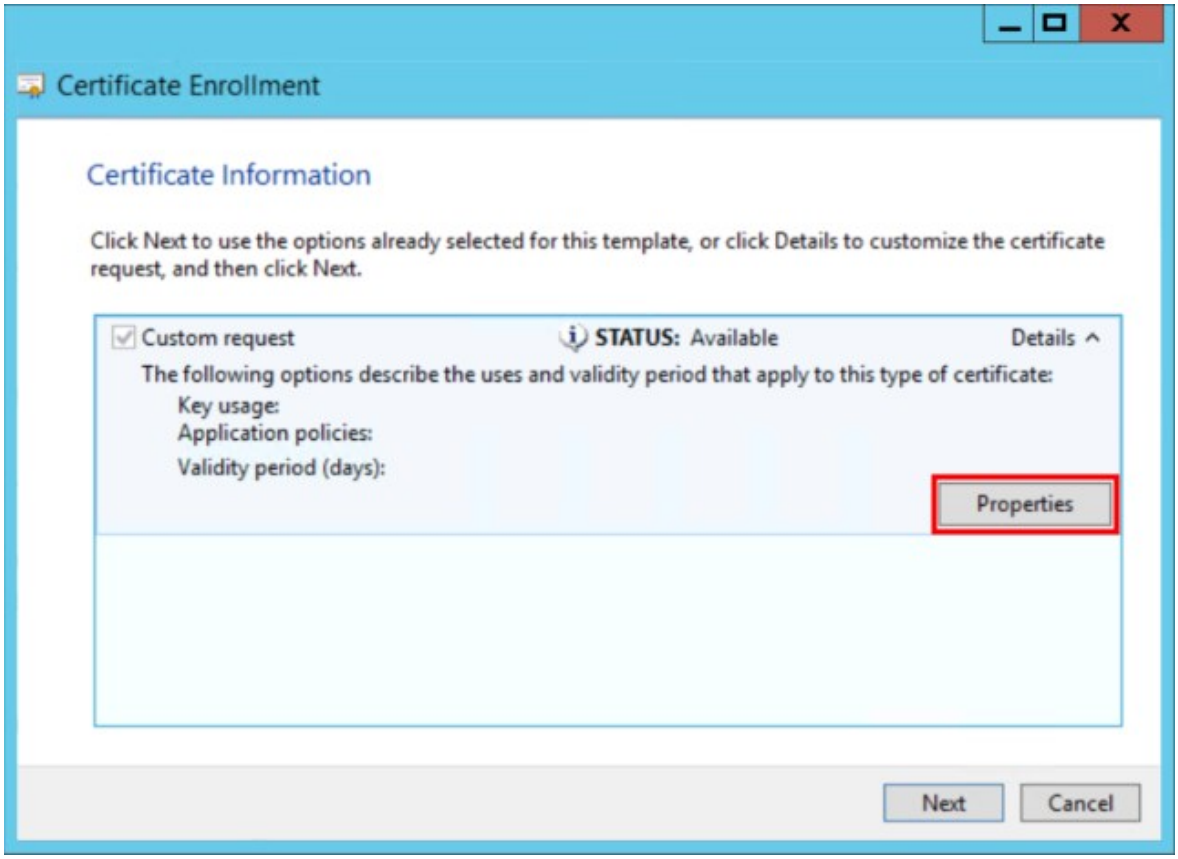
   Click **Next**.



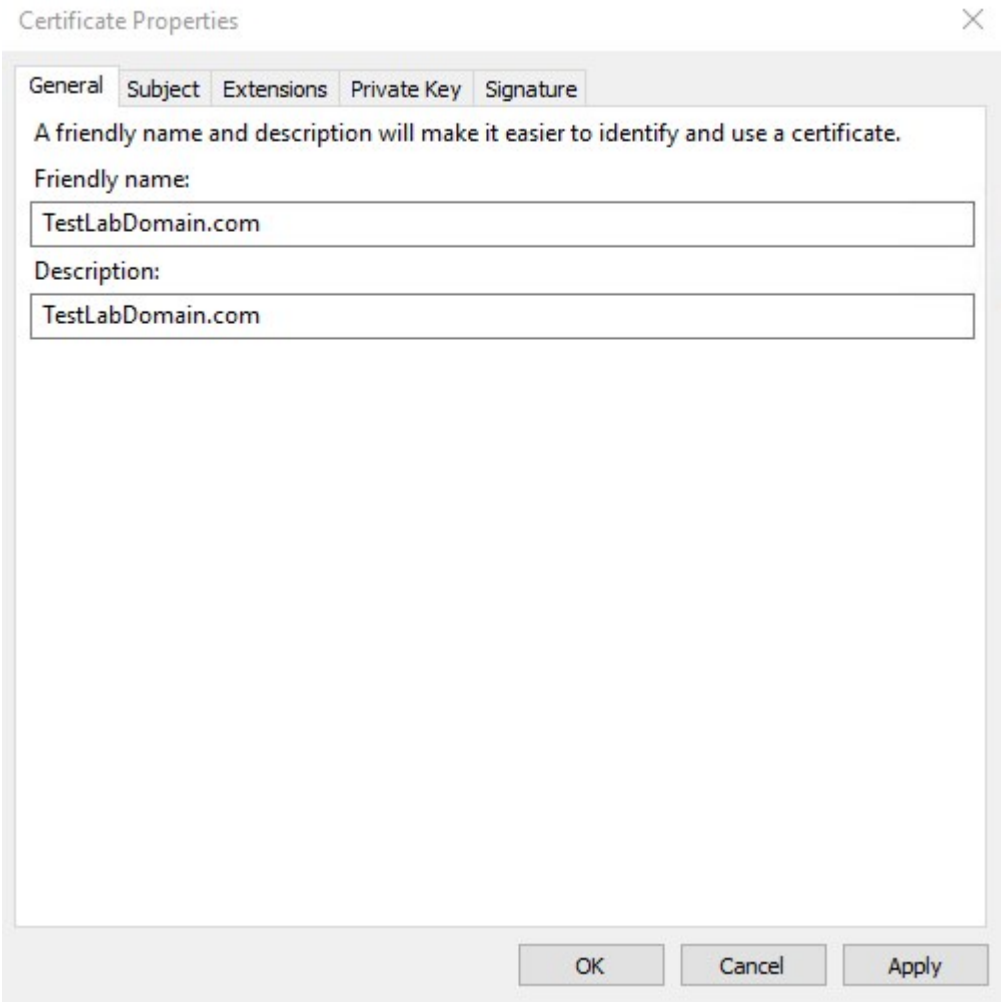
6. Select the **(No template) CNG Key** template and the **CMC** request format, and click **Next**.



7. Expand to view the **Details** of the custom request, and click **Properties**.

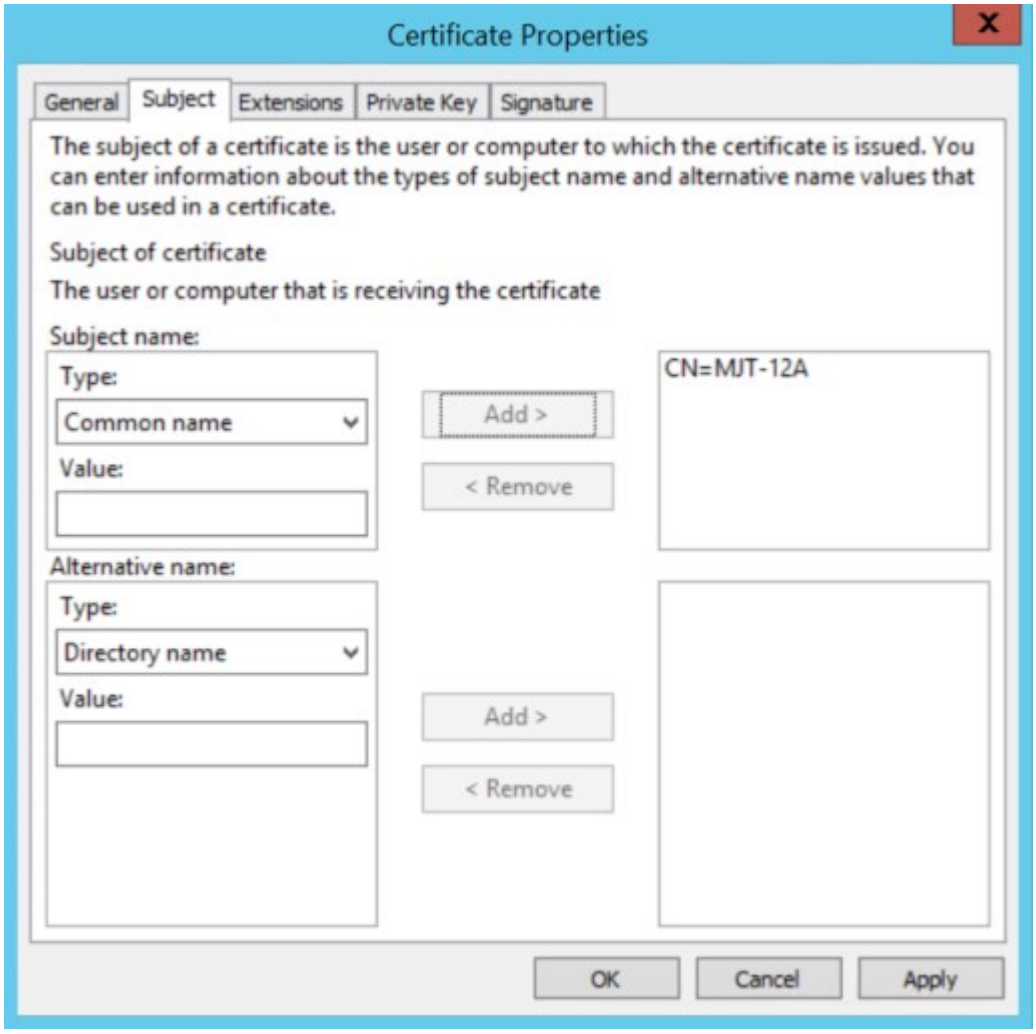


8. On the **General** tab, fill in the **Friendly name** and **Description** fields with the domain name, computer name, or organization.

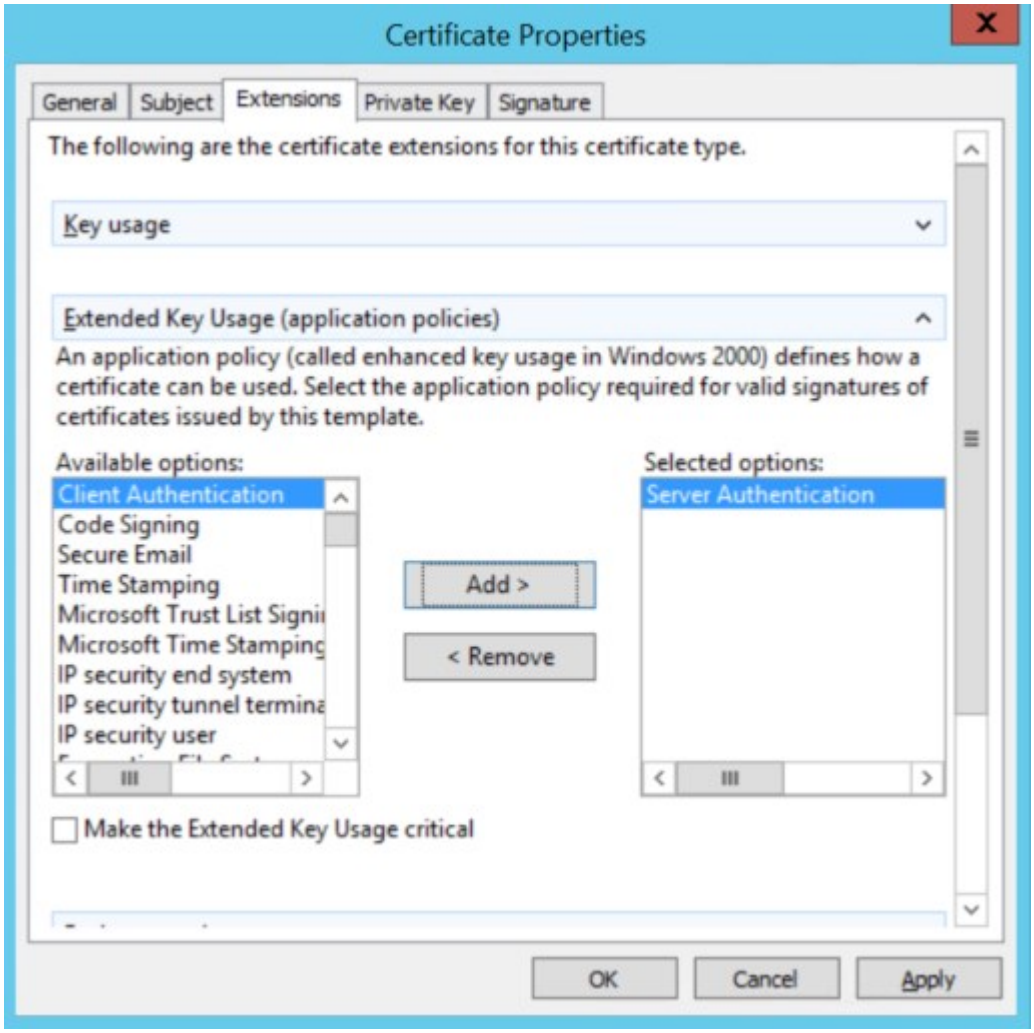


9. On the **Subject** tab, enter the required parameters for the subject name.

   In the subject name **Type**, enter in **Common Name** the host name of the computer where the certificate will be installed.



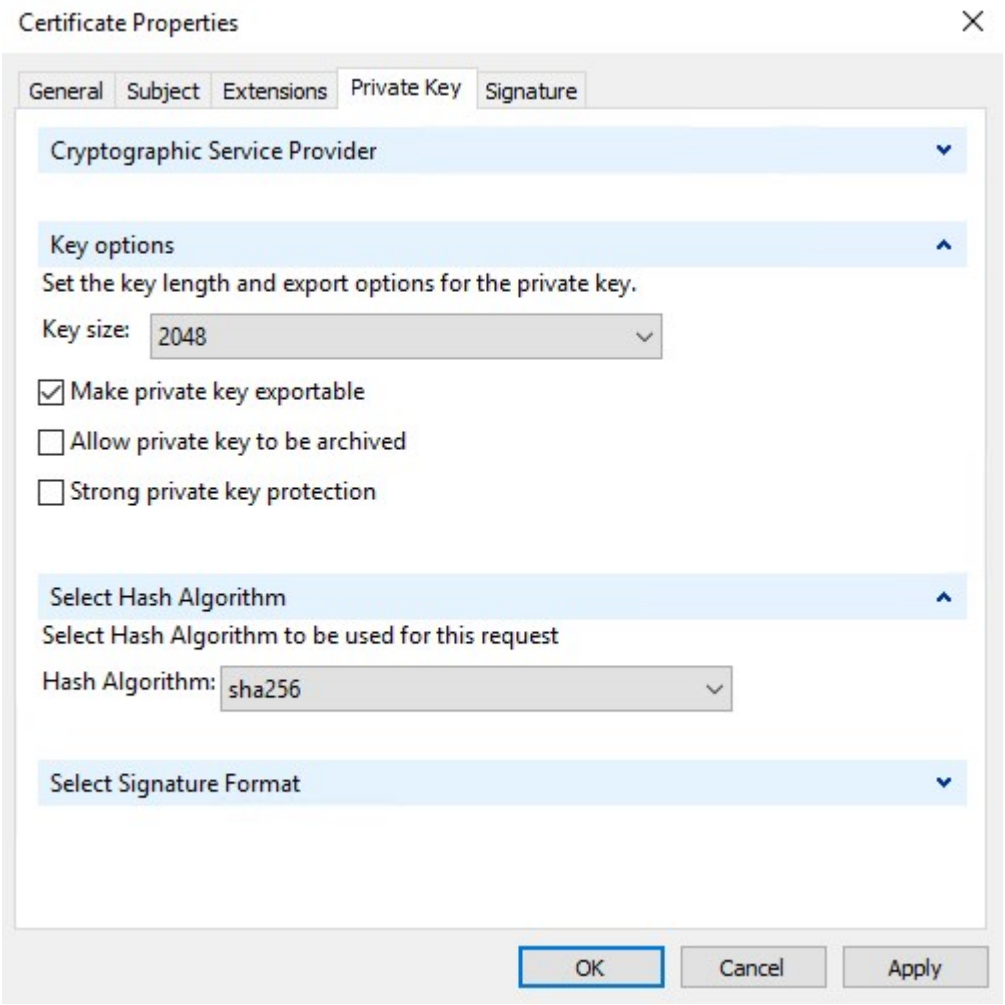
10. On the **Extensions** tab and expand the **Extended Key Usage (application policies)** menu. Add **Server Authentication** from the list of available options.



11. On the **Private Key** tab, expand the **Key options** menu.

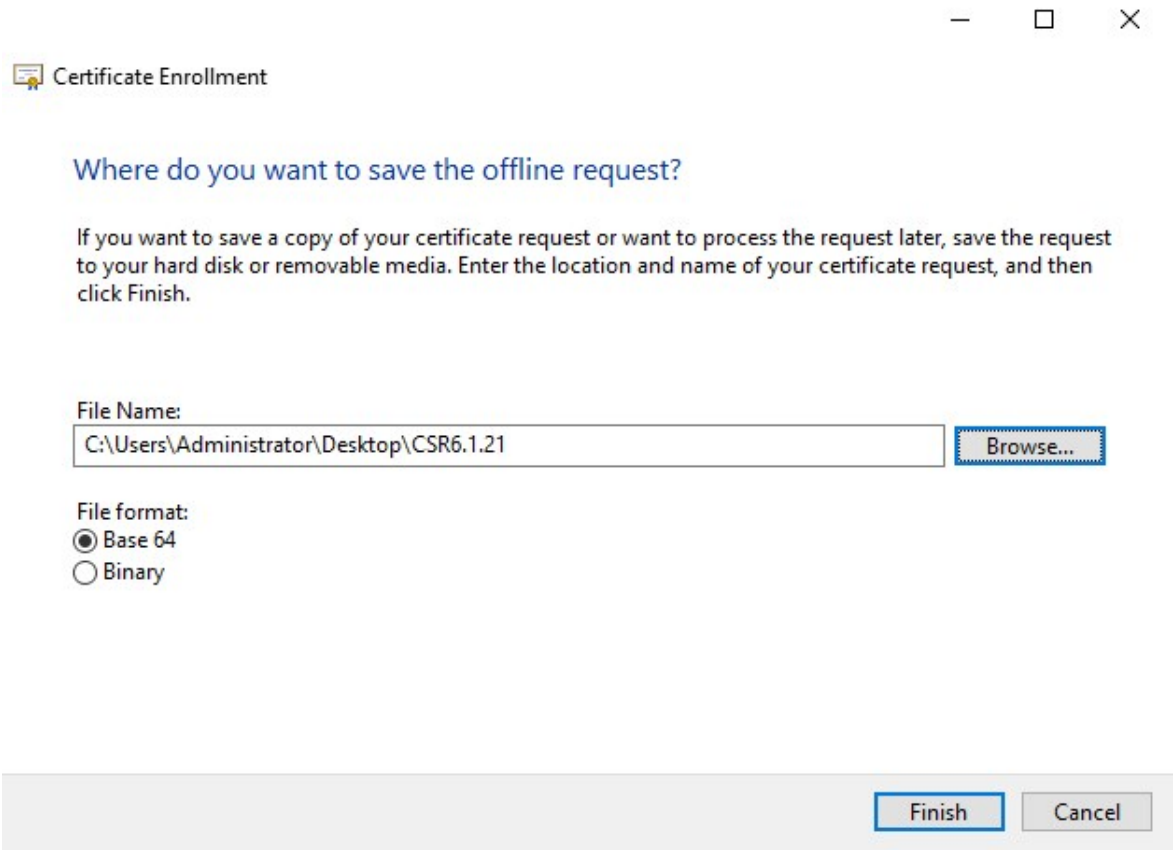
    Set the key size to 2048 and select the option to make the private key exportable.

    Click **OK**.



12. When all of the certificate properties have been defined, click **Next** on the **Certificate Enrollment** wizard.
13. Select a location to save the certificate request and a format. Browse to that location and specify a name for the .req file. The default format is base 64.

14. Click **Finish**.



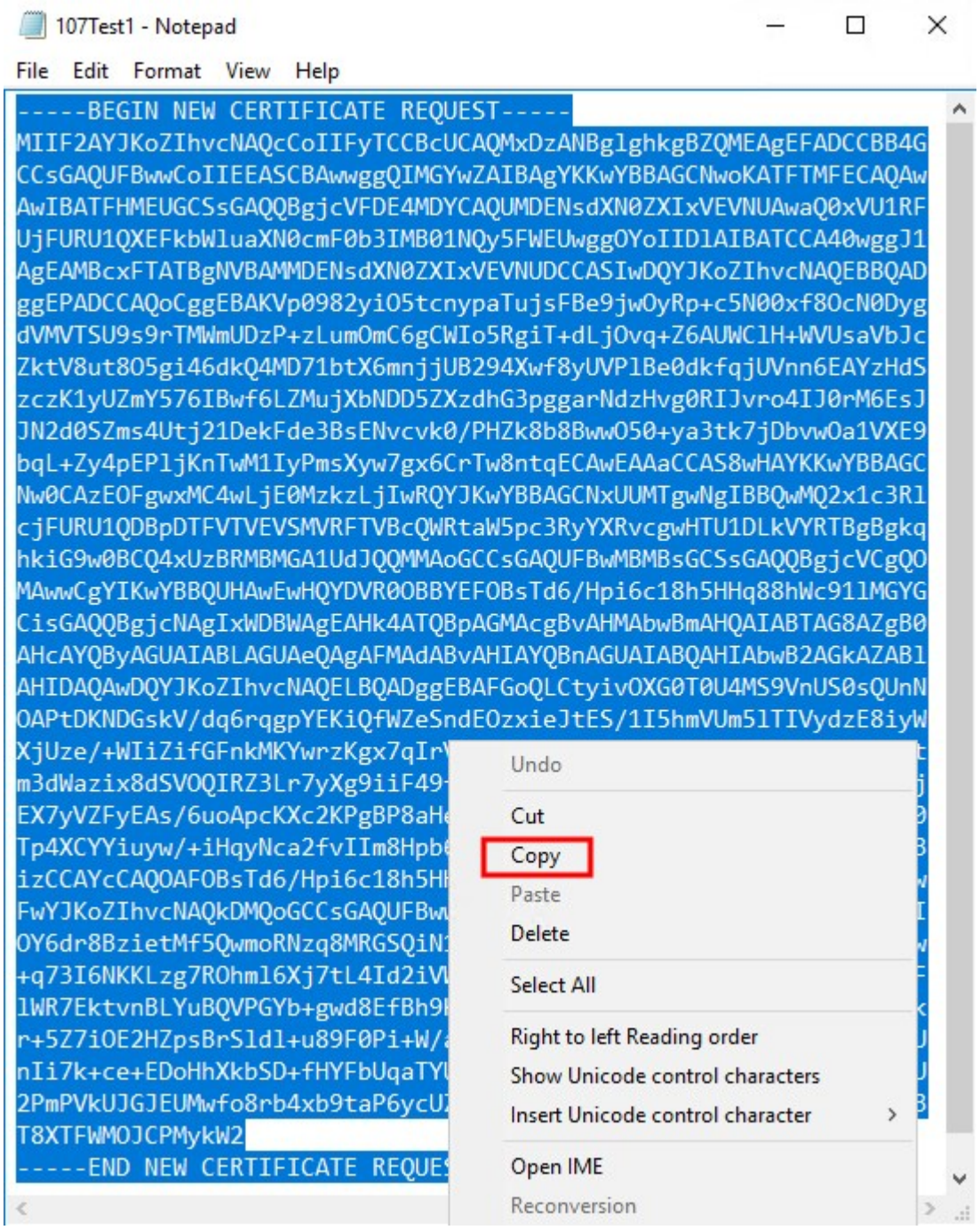
A .req file is generated, which you must use to request a signed certificate.

Upload the .req file to receive a signed certificate in return

You must copy the entire text of the .req file, including the begin and end lines, and paste the text to the internal Active Directory Certificate Services certificate authority in the network. See Install Active Directory Certificate Services on page 74.

Unless your domain has only recently installed Active Directory Certificate Services, or it has been installed just for this purpose, you will need to submit this request following a separate procedure configured by your Domain Administration team. Please confirm this process with them before proceeding.

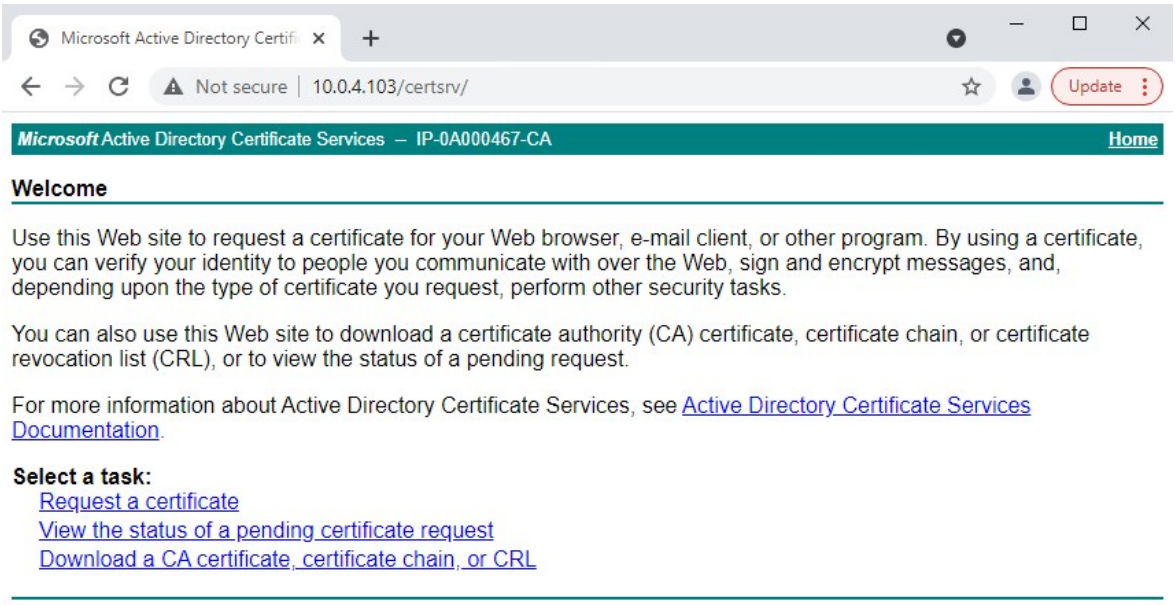
1. Browse to the location of the .req file and open it in Notepad.



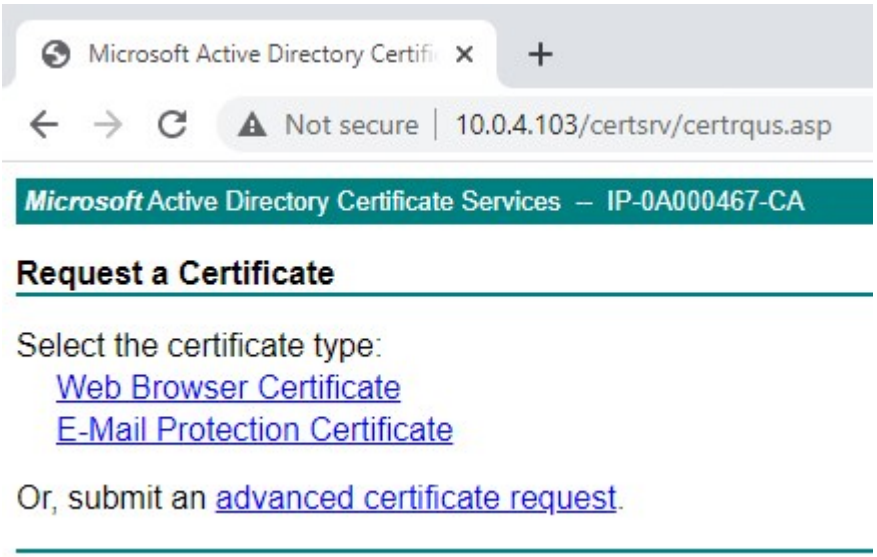
2. Copy the entire contents of the file. This includes the dashed lines marking the beginning and the end of the Certificate Request.

3. Open a web browser and enter the address of the internal CA, which should be located at: [ip.ad.dr.ess/certsrv].

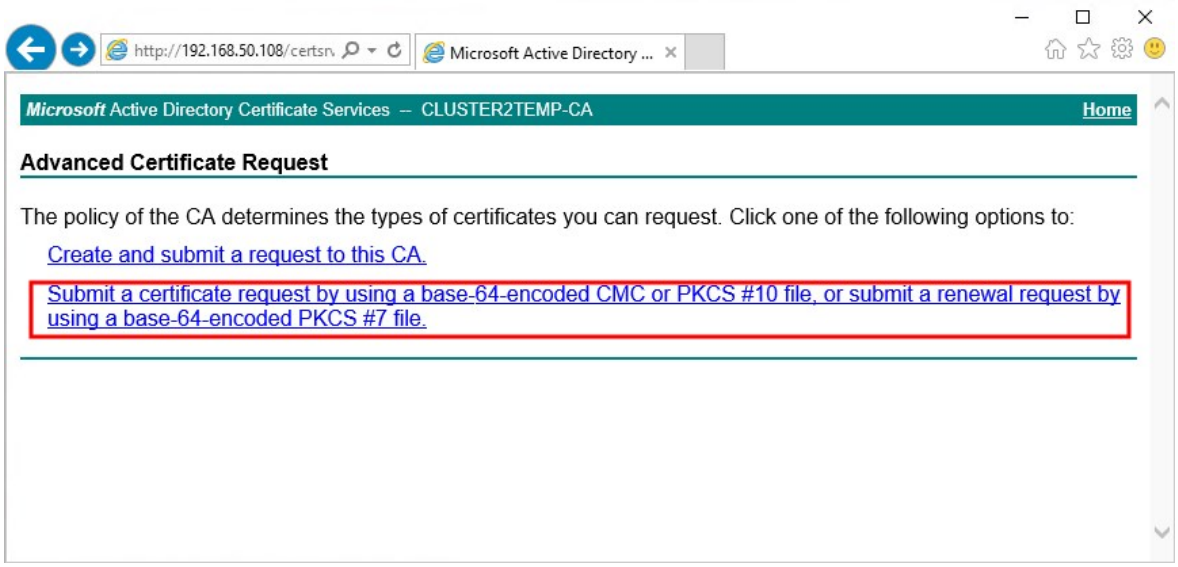
   Where, ip.ad.dr.ess is the IP address or DNS name of the internal network AD CS host server.



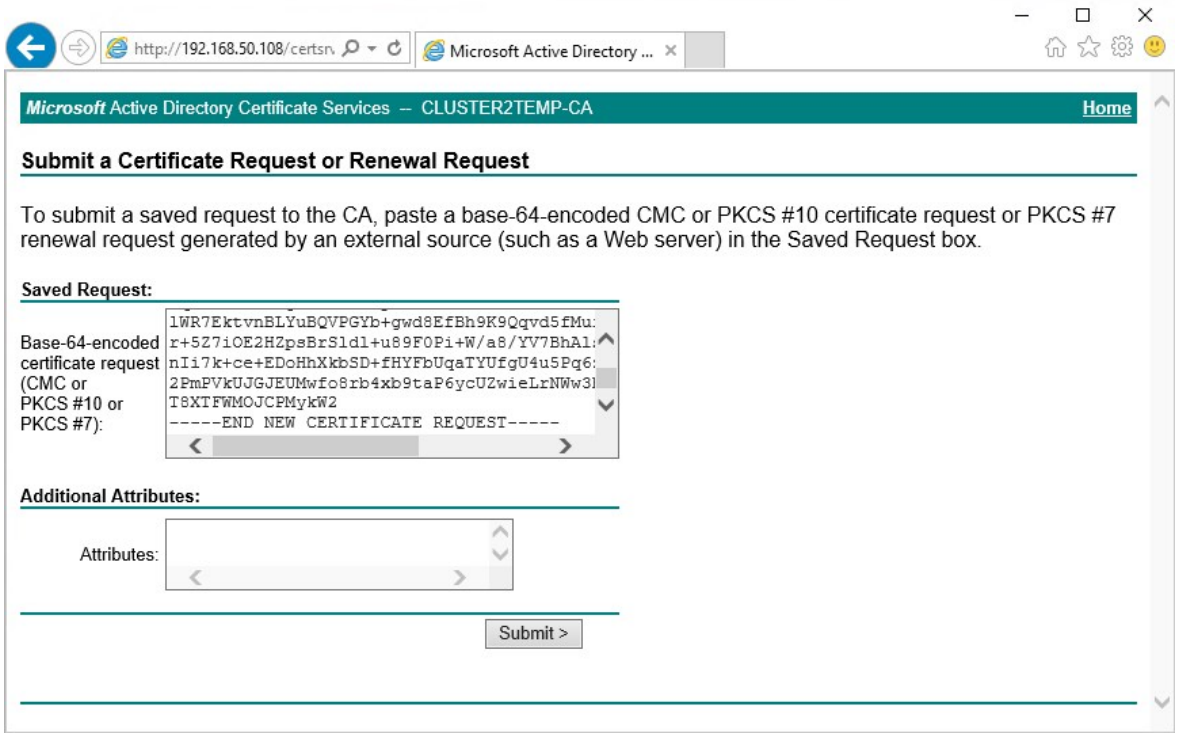
4. Click the **Request a certificate** link.
5. Click the **advanced certificate request** link.



6. Choose to Submit a certificate request by using a base-64-encoded CMC file.



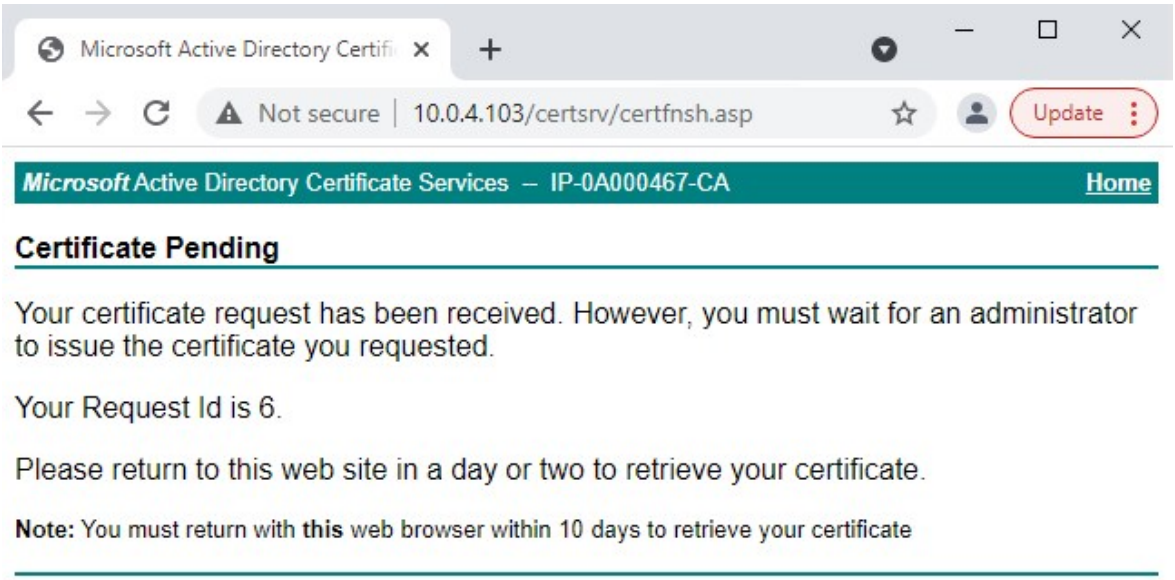
7. Paste the contents of the .req file into the form. If it is required to select a Certificate Template, select **Web Server** from the Certificate Template list.



8. Click **Submit**.

   The site shows a message that the certificate will be issued in a few days.

   - Internal CA servers can be used to manually issue certificates
   - Make a note of the date and time when the certificate request was submitted

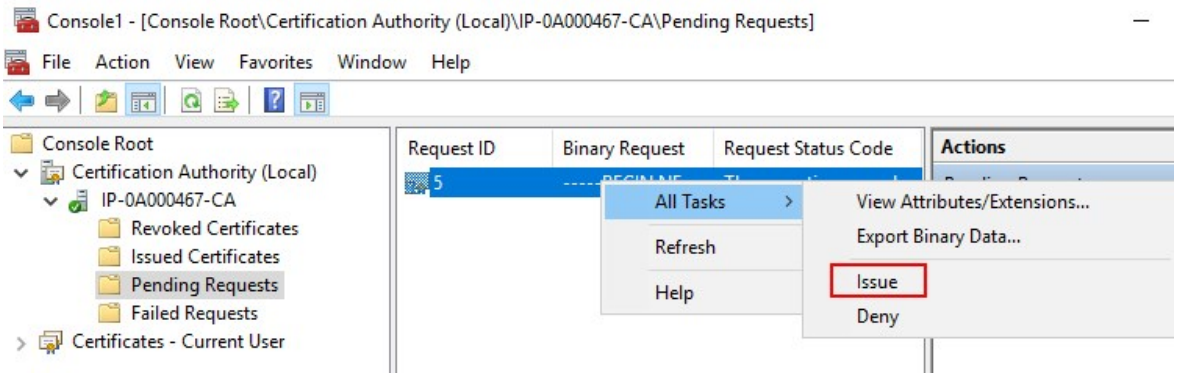


Issue certificates manually

You can issue certificates manually from the computer that hosts the Active Directory Certificate Services (AD CS).

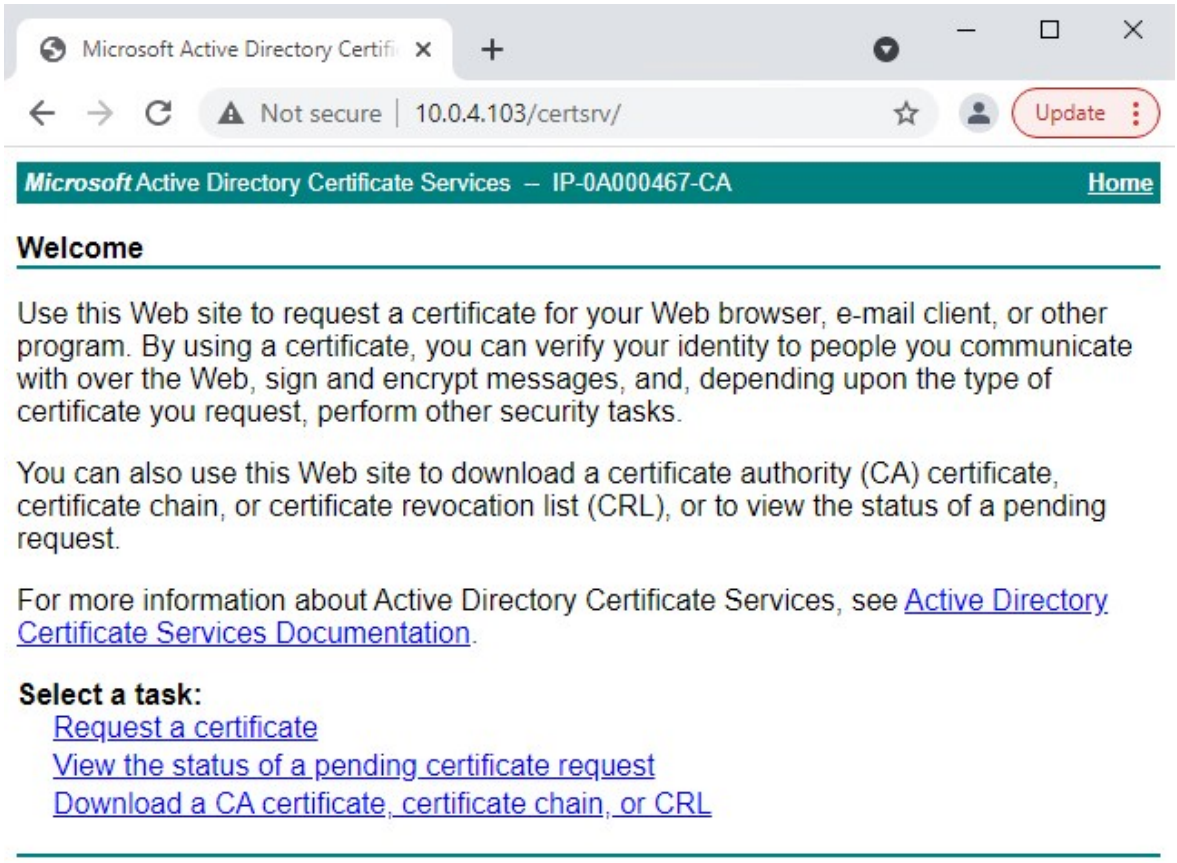
1. Open the Microsoft Management Console (MMC).
2. Navigate to the **Certificate Authority** snap-in.
3. Expand the **Certificate Authority** object.

   In the **Pending Requests** folder, right-click on the matching Request ID, and from the **All Tasks** list, select **Issue**.

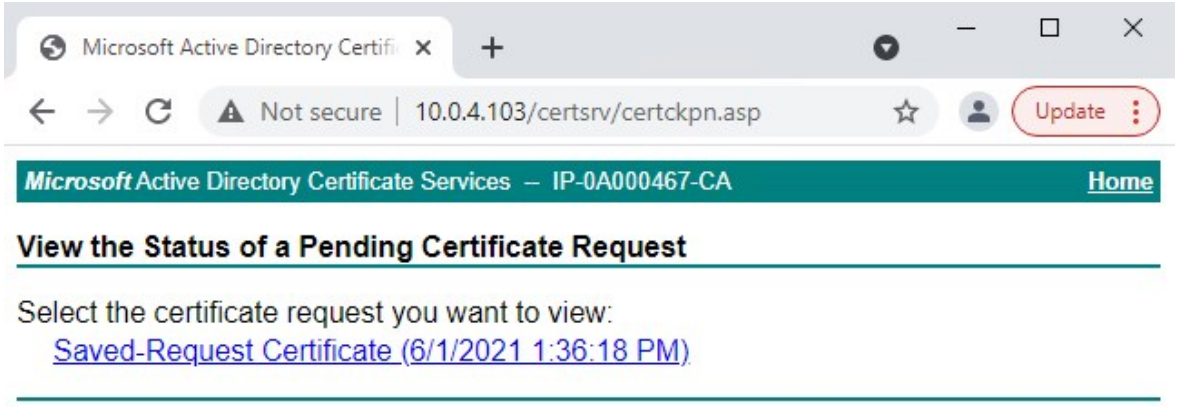


4. Open a browser and go to the Internal CA IIS site located at [ip.ad.dr.ess/certsrv].

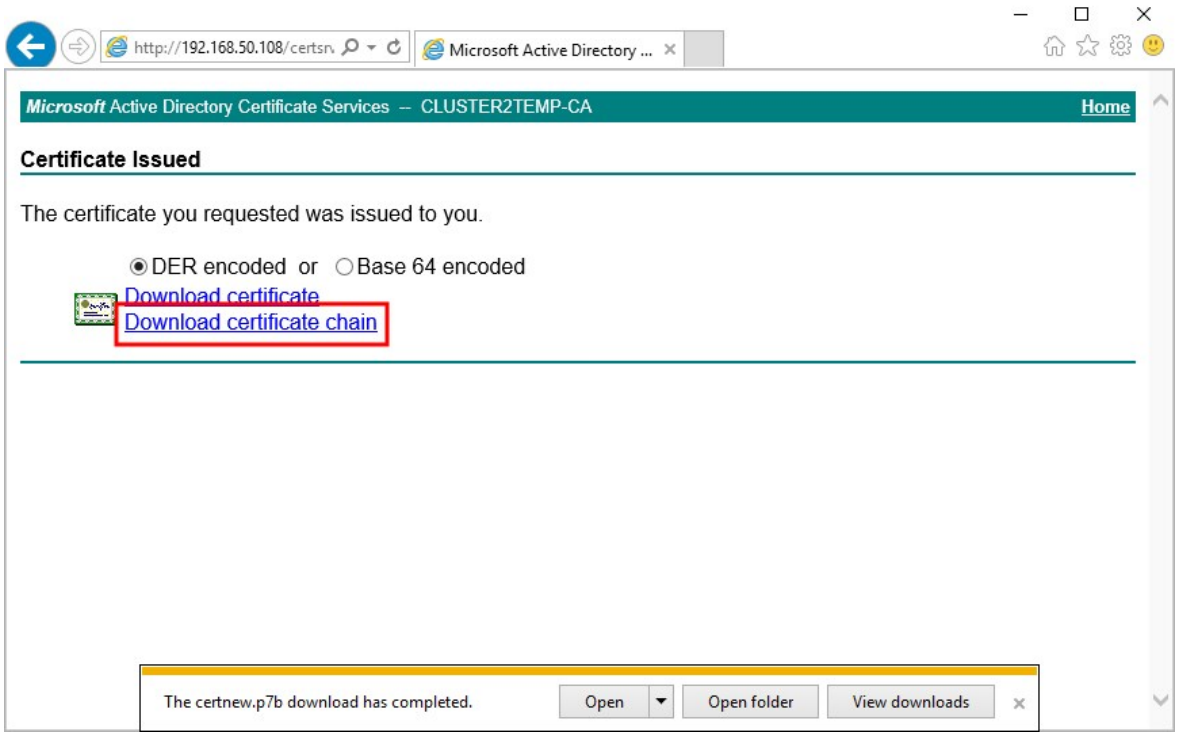
   Click the **View the status of a pending certificate request** link.



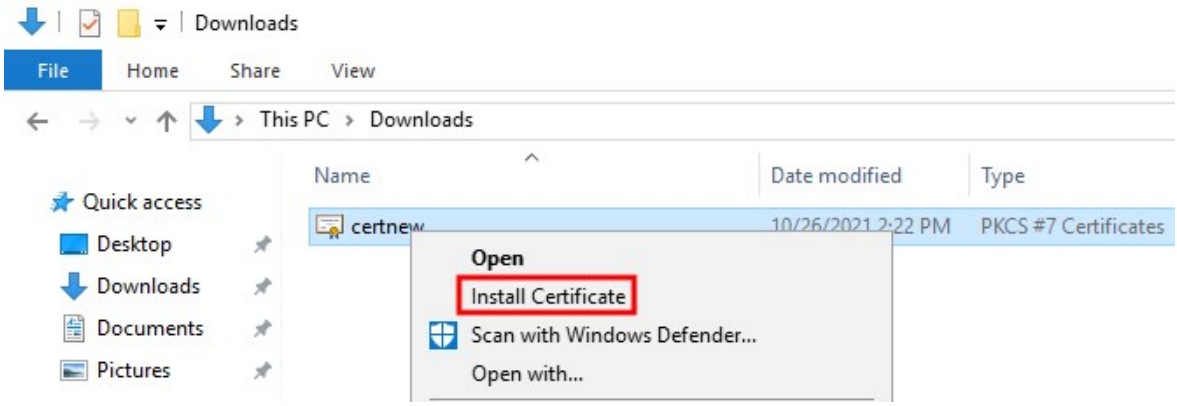
5. If the certificate has been issued, a link will be available on the resulting page that contains the date of the certificate request.



6. Select **DER encoded**, and download the certificate chain.

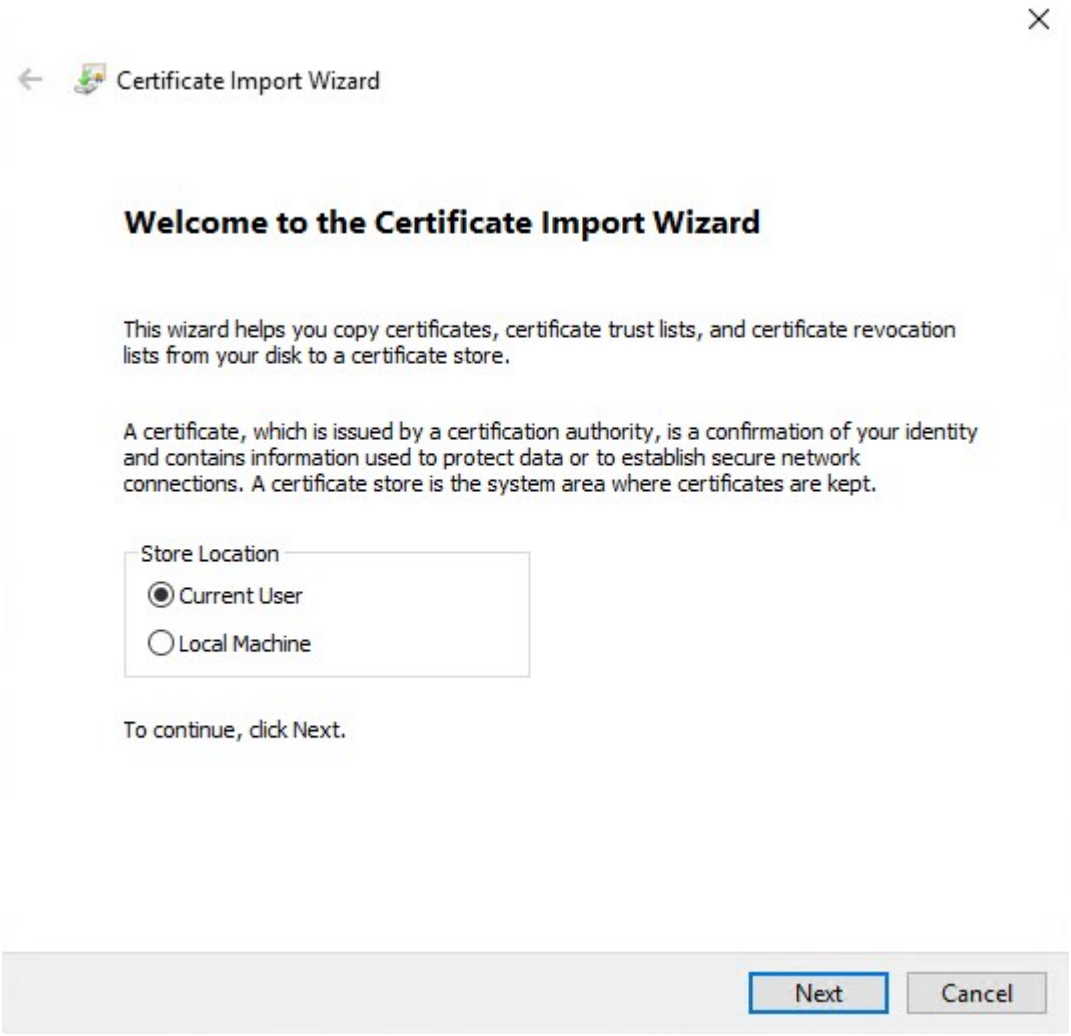


7. Browse to the downloads folder, right-click the certificate, and select **Install Certificate** from the shortcut menu.



8. Accept the security warning if it appears.

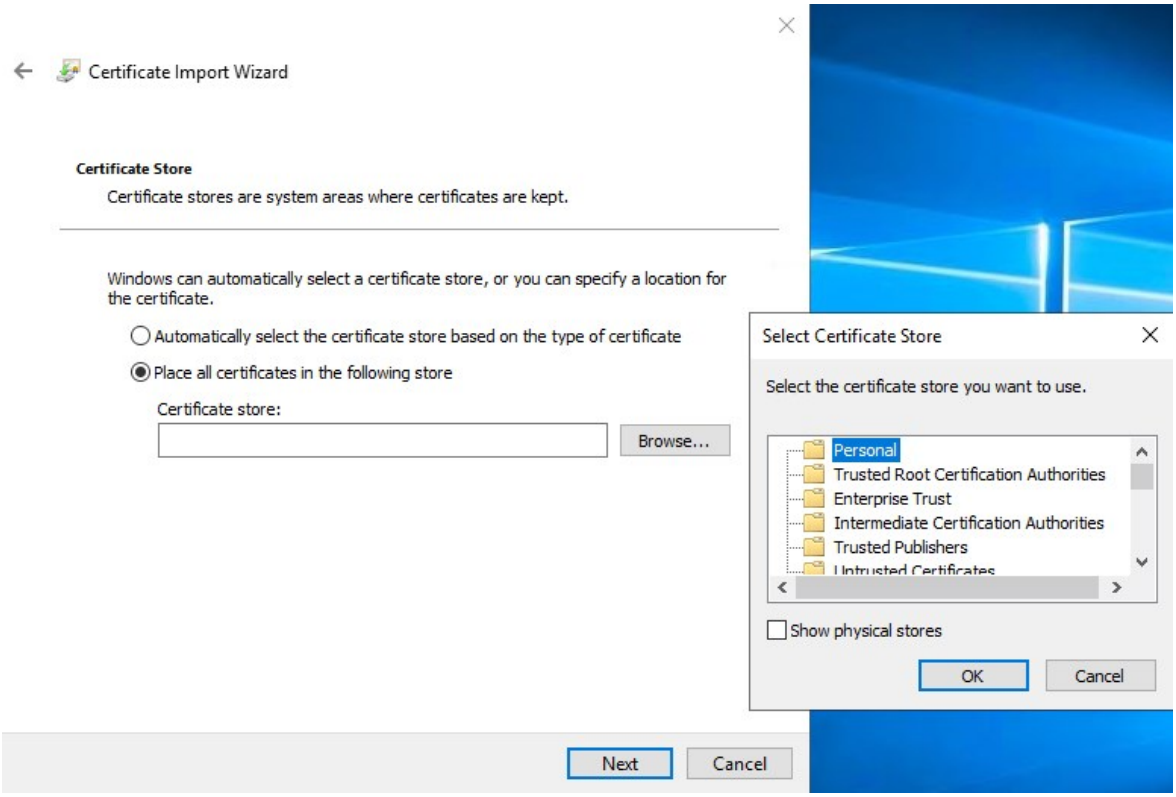
   Select to install the certificate for the current user and click **Next**.



9. Choose a store location. Select **Place all certificates in the following store**, and click the **Browse** button to open the **Select Certificate Store** window.

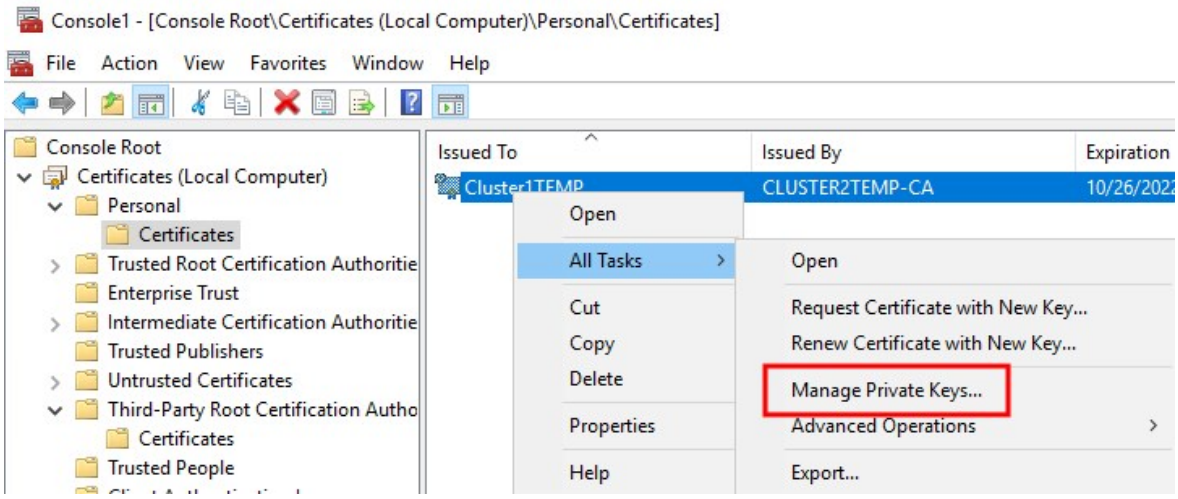
   Navigate to the **Personal** certificate store and click **OK**.

   Click **Next**.



10. Finish the **Certificate Import Wizard**.
11. Go to the Microsoft Management Console (MMC) certificates snap-in.

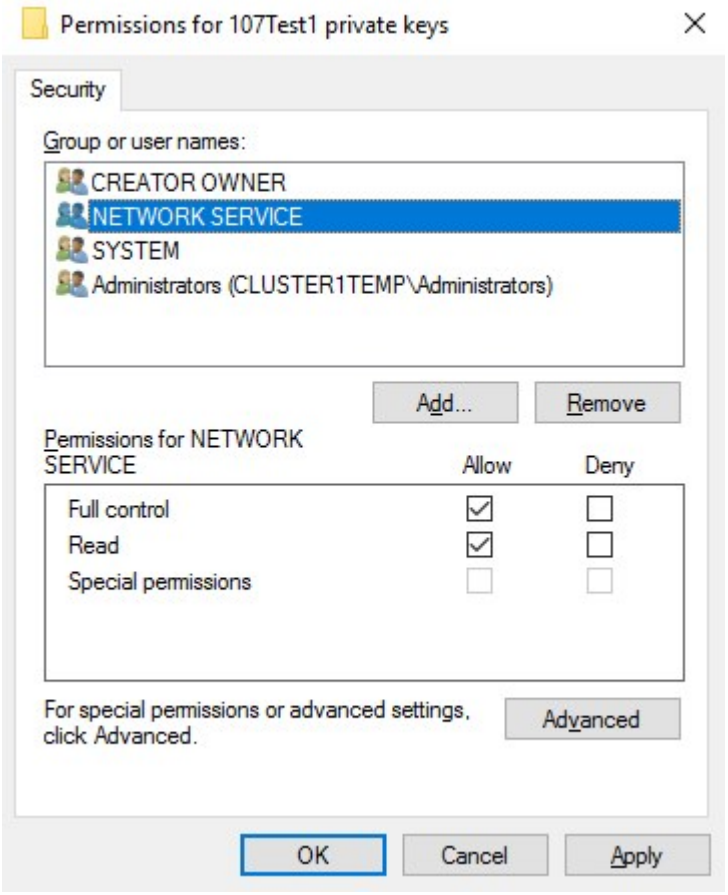
12. In the console, browse to the personal store where the certificate is installed. Right-click on the certificate and select **All Tasks** > **Manage Private Keys**.



13. Add the account that is running the Milestone XProtect Management Server, Recording Server, or Mobile Server software to the list of users with permission to use the certificate.

    Make sure that the user has both Full Control and Read permissions enabled.

    By default, XProtect software uses the NETWORK SERVICE account.



Enable server encryption for Management Servers and Recording Servers

Once the certificate is installed with the correct properties and permissions, do the following.

1. On a computer with a Management Server or Recording Server installed, open the **Server Configurator** from:

    - The Windows Start menu

    or

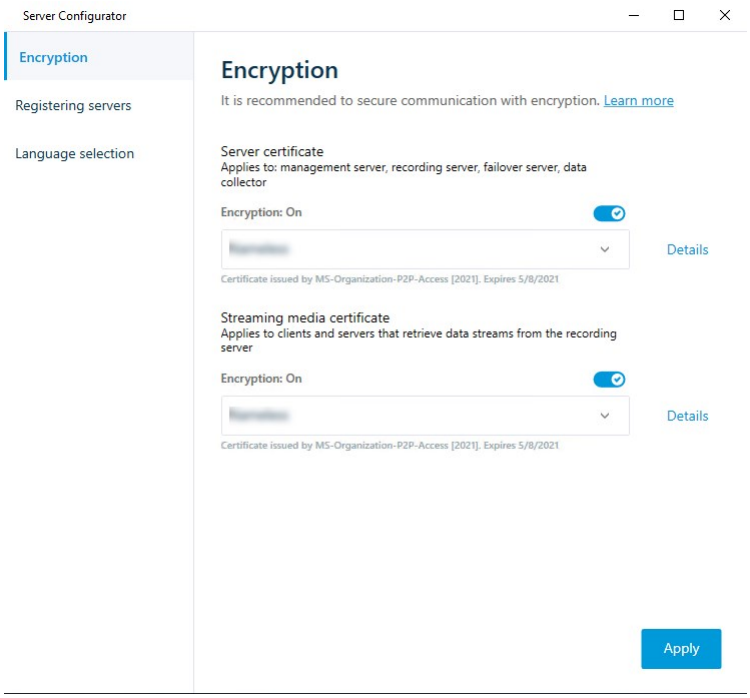
    - The server manager, by right-clicking the server manager icon on the computer task bar

2. In the **Server Configurator**, under **Server certificate**, turn on **Encryption**.

3. Click **Select certificate** to open a list with unique subject names of certificates that have a private key and that are installed on the local computer in the Windows Certificate Store.
4. Select a certificate to encrypt communication between the recording server, management server, failover server, and data collector server.

   Select **Details** to view Windows Certificate Store information about the selected certificate.

   The Recording Server service user has been given access to the private key. It is required that this certificate is trusted on all clients.



5. Click **Apply**.

> When you apply certificates, the recording server will be stopped and restarted. Stopping the Recording Server service means that you cannot record and view live video while you are verifying or changing the recording server's basic configuration.

Install certificates for communication with the Event Server

You can encrypt the two-way connection between the Event Server and the components that communicate with the Event Server, including the LPR Server. When you enable encryption on the Event Server, it applies to connections from all the components that connect to the Event Server. Before you enable encryption, you must install security certificates on the Event Server and all connecting components.

When the Event Server communication is encrypted, this applies to all communication with that Event Server. That is, only one mode is supported at a time, either http or https, but not at the same time.

Encryption applies to every service hosted in the Event Server, including Transact, Maps, GisMap, and Intercommunication.

Before you enable encryption in the Event Server, all clients (Smart Client and Management Client) and the XProtect LPR plug-in must be updated to at least version 2022 R1.
HTTPS is only supported if every component is updated to at least version 2022 R1.

Creation of the certificates is the same as described in these sections, depending on the certificate environment:

- Install third-party or commercial CA certificates for communication with the Management Server or Recording Server on page 57
- Install certificates in a domain for communication with the Management Server or Recording Server on page 86
- Install certificates in a Workgroup environment for communication with the Management Server or Recording Server on page 107

Enable XProtect Event Server encryption

After the certificate is installed, you can enable it to be used with all communication with the Event Server.

After all clients are updated to at least version 2022 R1, you can enable encryption on the Event Server.

You can encrypt the two-way connection between the event server and the components that communicate with the event server, including the LPR Server.

When you configure encryption for a server group, it must either be enabled with a certificate belonging to the same CA certificate or, if the encryption is disabled, then it must be disabled on all computers in the server group.

Prerequisites:

- A server authentication certificate is trusted on the computer that hosts the event server

First, enable encryption on the event server.

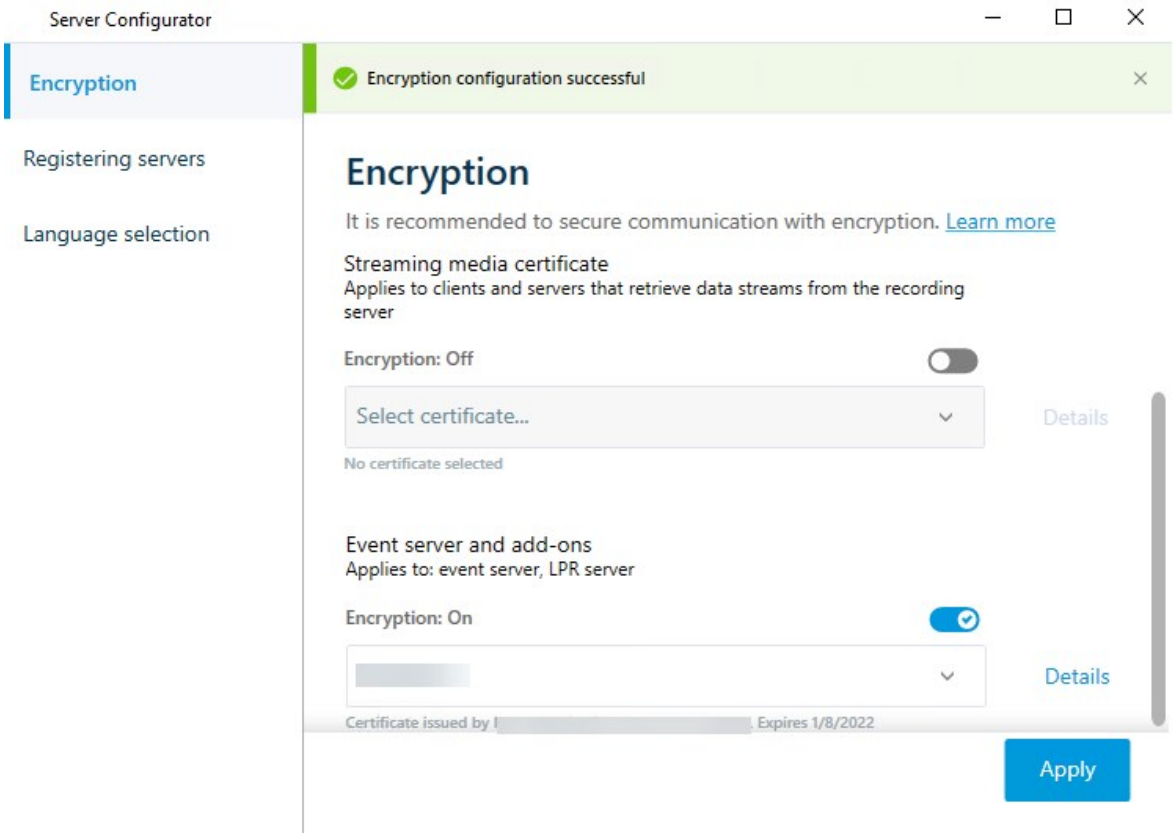
Steps:

1. On a computer with an event server installed, open the **Server Configurator** from:
   - The Windows Start menu

   or

   - The Event Server by right-clicking the Event Server icon on the computer task bar
2. In the **Server Configurator**, under **Event server and add-ons**, turn on **Encryption**.
3. Click **Select certificate** to open a list with unique subject names of certificates that have a private key and that are installed on the local computer in the Windows Certificate Store.
4. Select a certificate to encrypt communication between the event server and related add-ons.

Select **Details** to view Windows Certificate Store information about the selected certificate.



5. Click **Apply**.

To complete the enabling of encryption, the next step is to update the encryption settings on each related extension LPR Server.

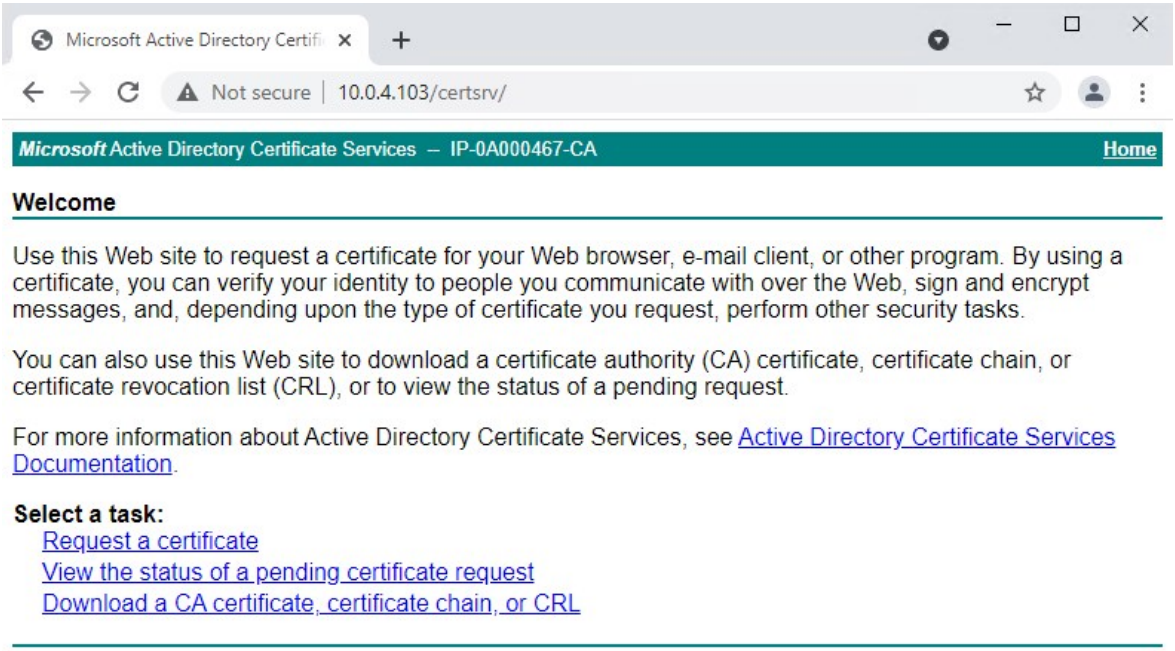
Import client certificates

This section describes how to import client certificates onto a client workstation or device.

1. After you import a CA certificate to the Management Server or Recording Server, you can access it from any workstation or server in the network by going to the following address:

   - http://localhost/certsrv/

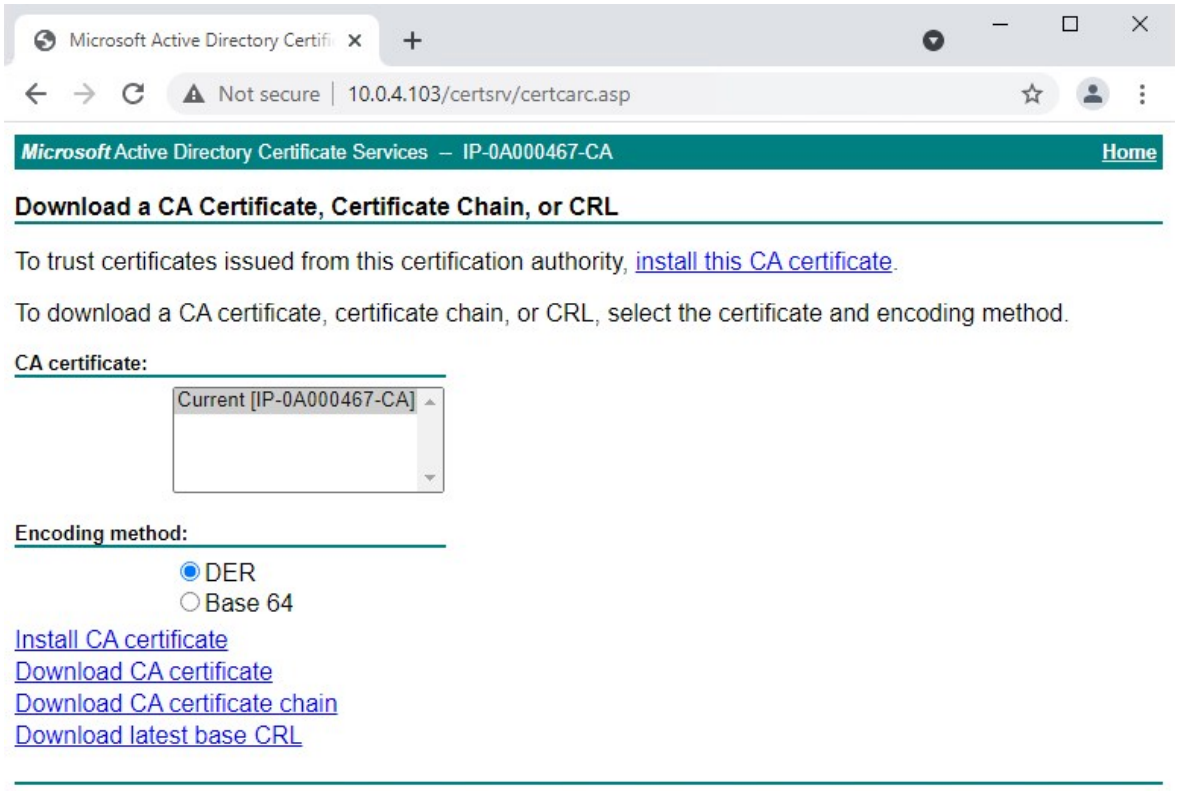
   However, the address of the server that holds the certificate (private key) will take the place of "localhost." For example:



   This web-server is hosted on the Active Directory Certificate Services (AD CS) host server that holds the CA certificate.

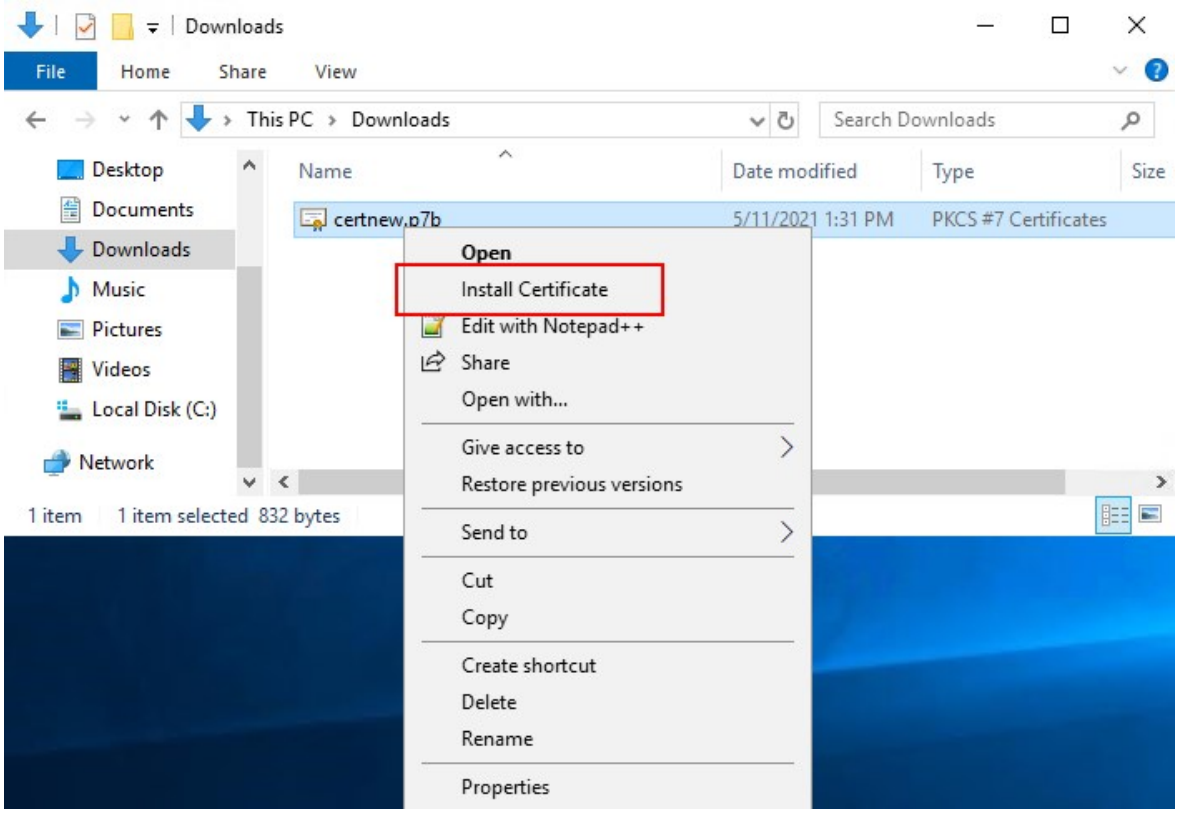
2. Click **Download a CA certificate, certificate chain, or CRL**.

3. In the **CA certificate** field, select the CA certificate to be used with the XProtect system, and click **Download CA certificate chain**.



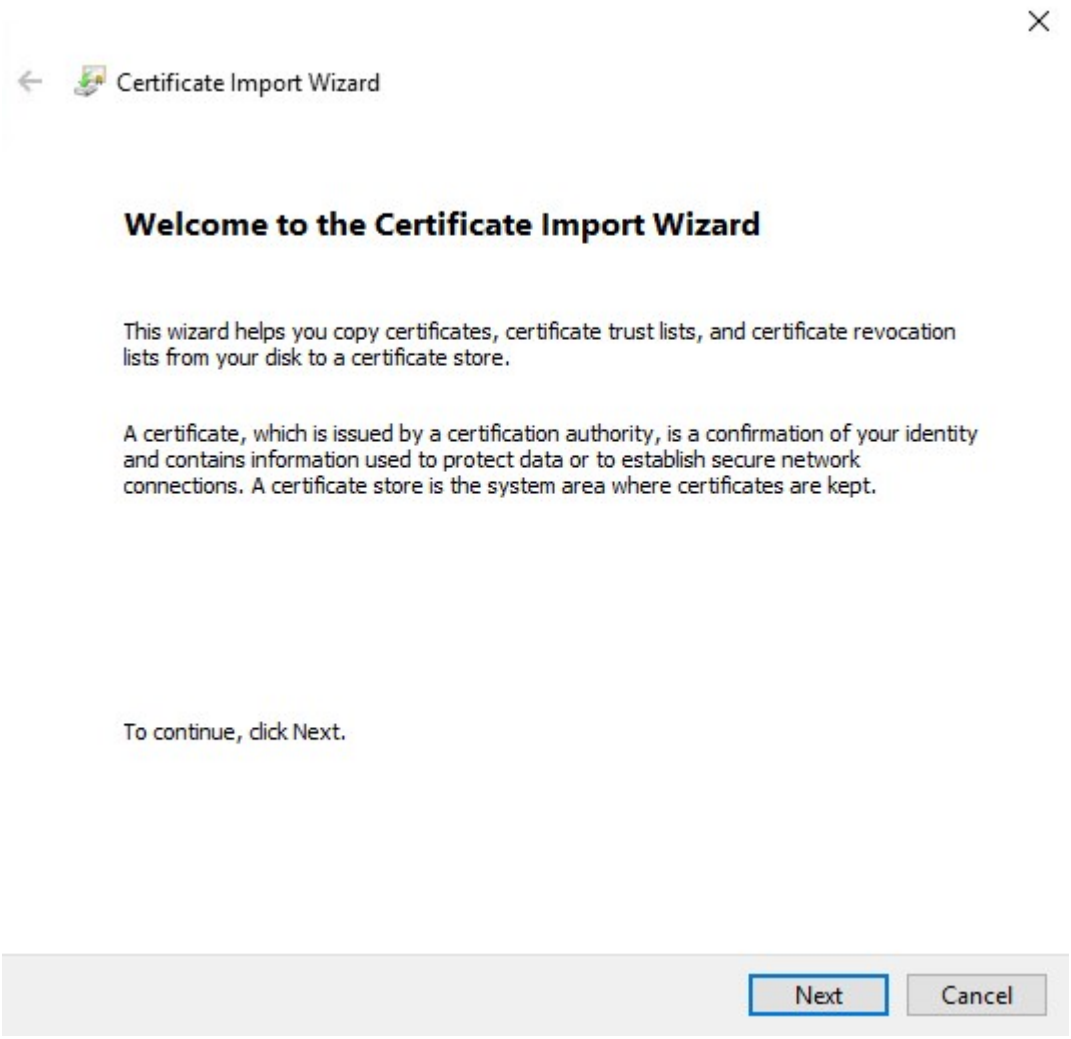
4. Select **DER encoded**, and download the certificate chain.

5. Browse to the downloads folder, right-click the certificate, and select **Install Certificate** from the shortcut menu.

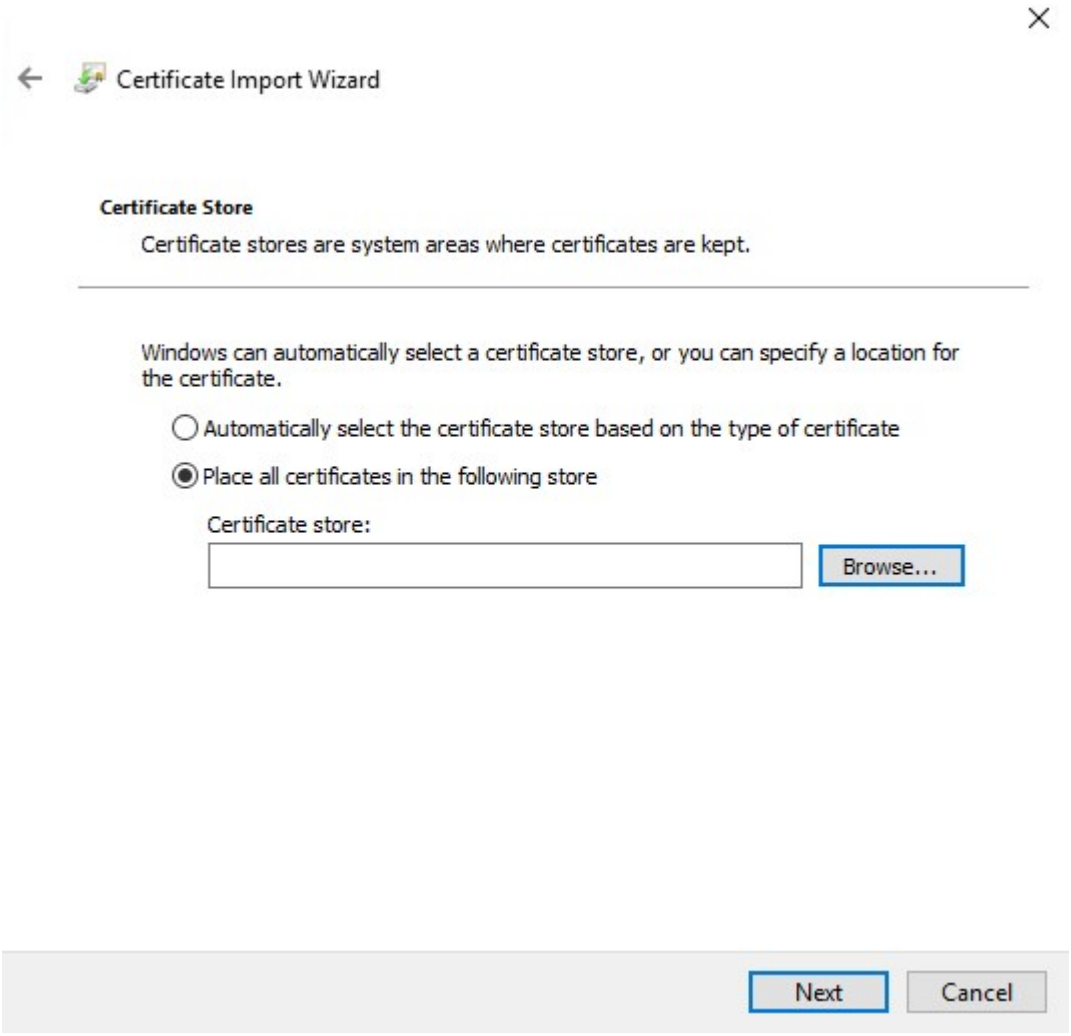


6. This launches the **Certificate Import Wizard**.

   Click **Next**.

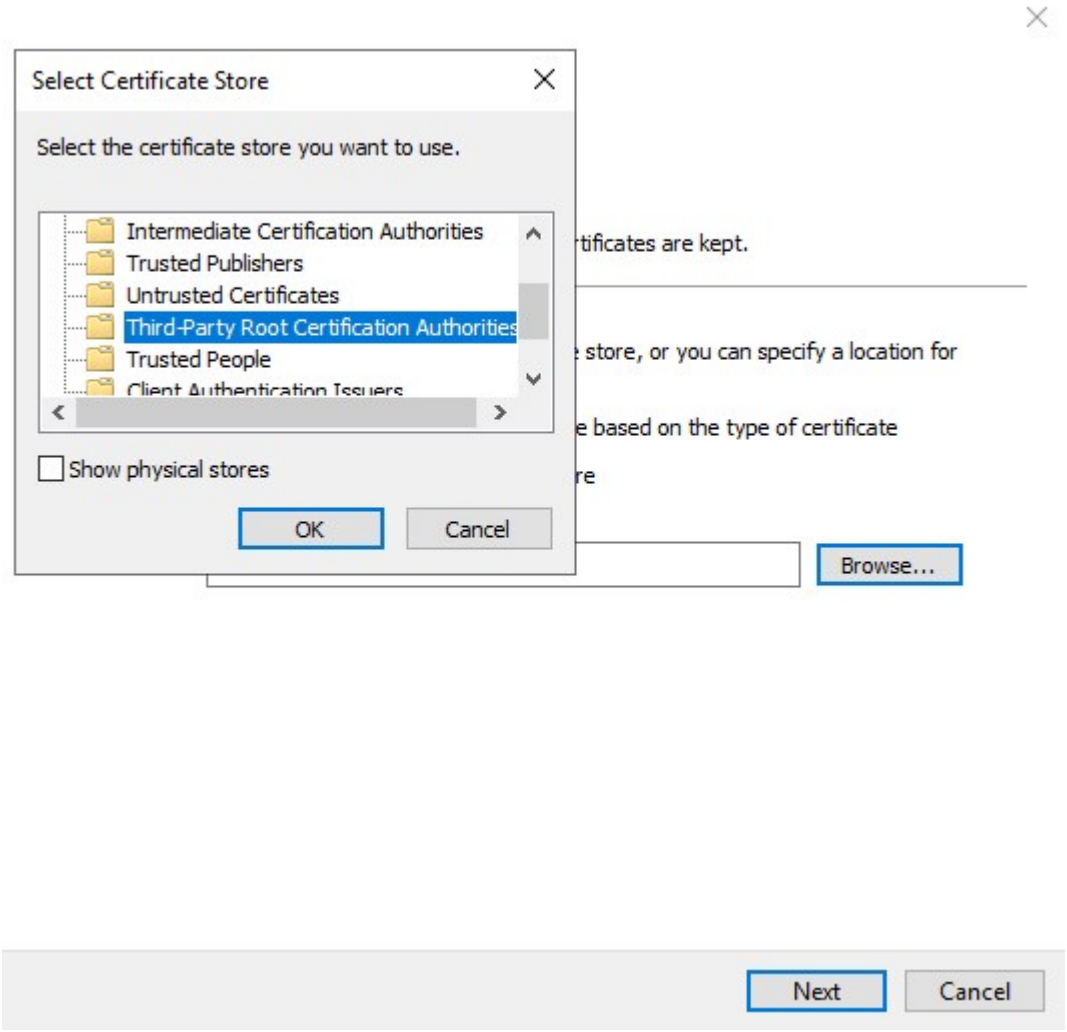


7. Choose a store location. Select **Place all certificates in the following store**, and click the **Browse** button to open the **Select Certificate Store** window.



8. Navigate to the **Third-Party Root Certification Authorities** certificate store and click **OK**.

   Click **Next**.



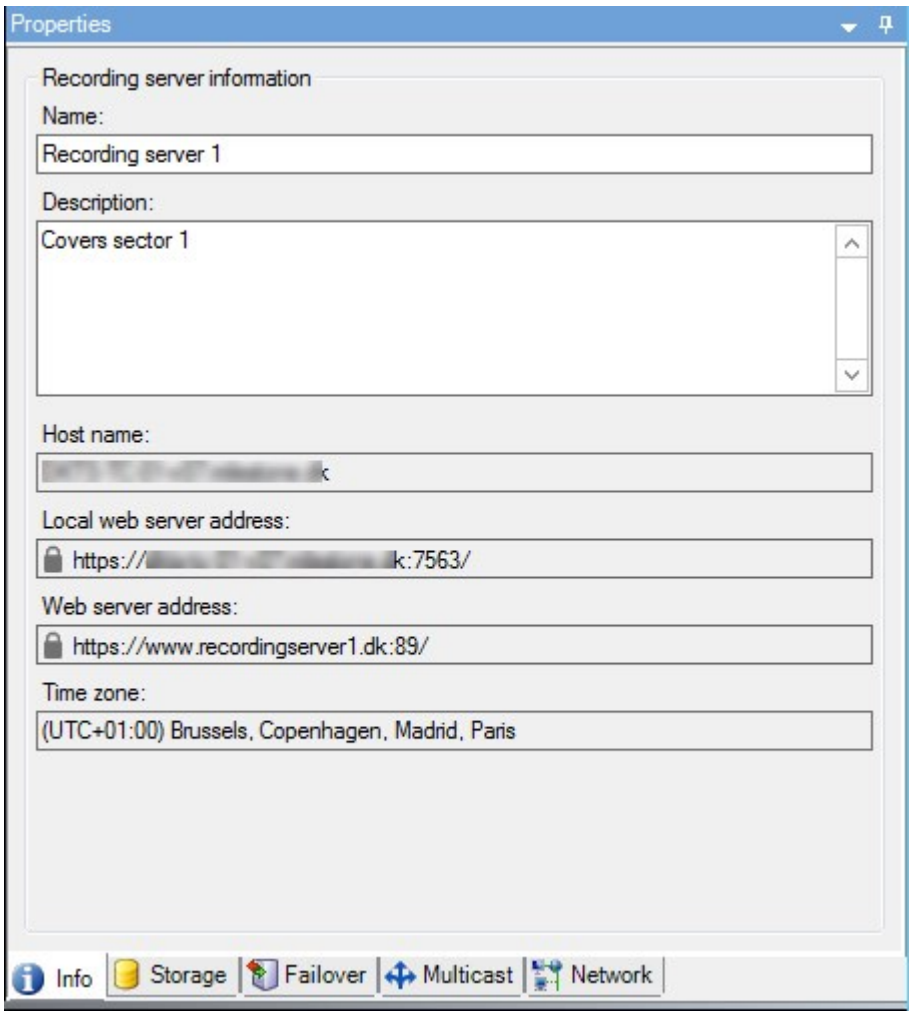
9. Finish the **Certificate Import Wizard**.

Now the workstation has imported the certificate components required to establish secure communications with the Management Server or Recording Server.

View encryption status to clients

To verify if your recording server encrypt connections:

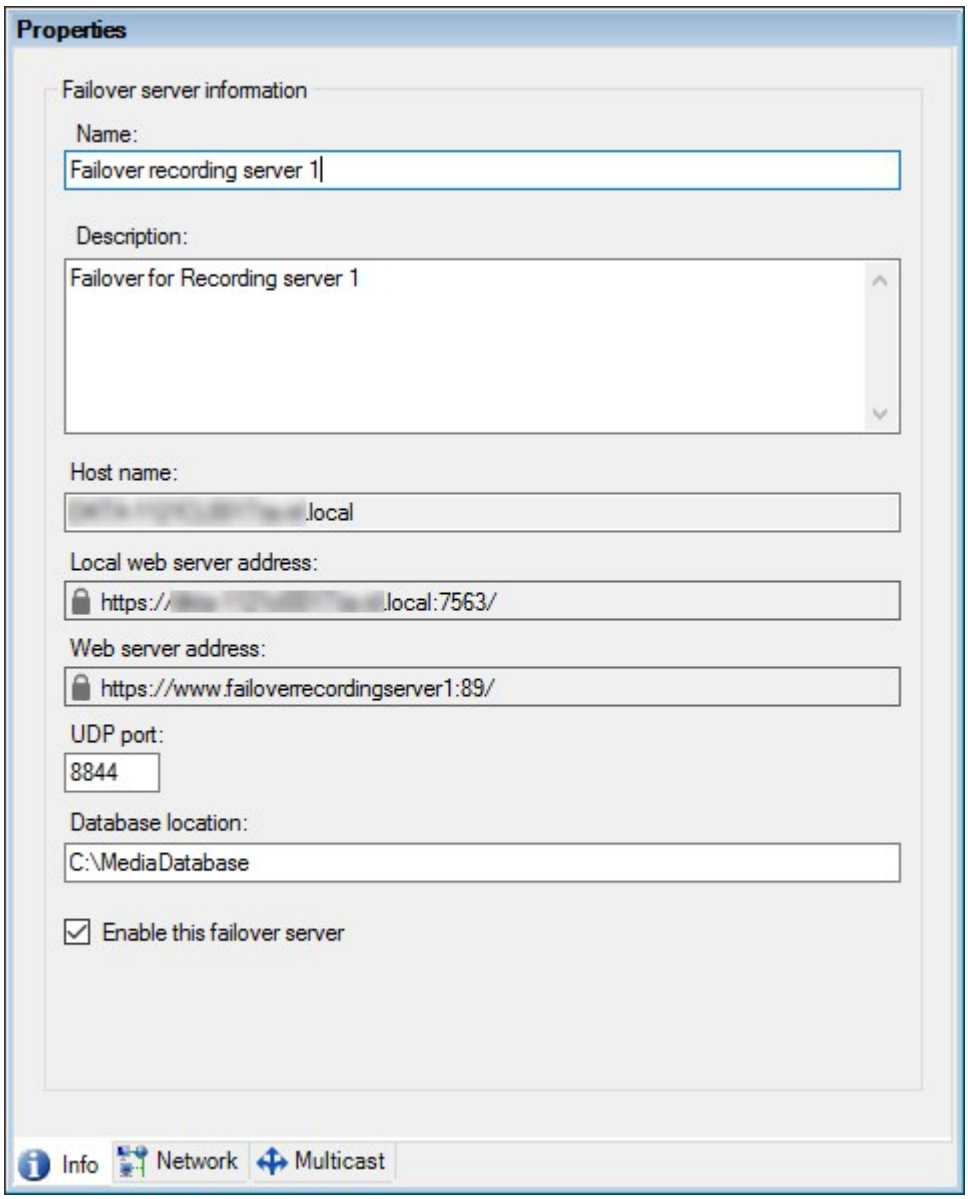
1. Open the Management Client.
2. In the **Site Navigation** pane, select **Servers** > **Recording Servers**. This opens a list of recording servers.
3. In the **Overview** pane, select the relevant recording server and go to the **Info** tab.
   If encryption is enabled to clients and servers that retrieve data streams from the recording server, a padlock icon appears in front of the local web server address and the optional web server address.



View encryption status on a failover recording server

To verify if your failover recording server uses encryption, do the following:

1. In the **Site Navigation** pane, select **Servers** > **Failover Servers**. This opens a list of failover recording servers.
2. In the **Overview** pane, select the relevant recording server and go to the **Info** tab.
   If encryption is enabled to clients and servers that retrieve data streams from the recording server, a padlock icon appears in front of the local web server address and the optional web server address.



```
# Run this script once, to create a certificate that can sign multiple server SSL certificates

# Private certificate for signing other certificates (in certificate store)
$ca_certificate = New-SelfSignedCertificate -CertStoreLocation cert:\CurrentUser\My -DnsName 'VMS Certificate Authority' -KeyusageProperty All `
                                            -KeyUsage CertSign, CRLSign, DigitalSignature -FriendlyName 'VMS CA Certificate' `
                                            -TextExtension @("2.5.29.19={critical}{text}ca=TRUE")

# Thumbprint of private certificate used for signing other certificates
Set-Content -Path "$PSScriptRoot\ca_thumbprint.txt" -Value $ca_certificate.Thumbprint

# Public CA certificate to trust (Third-Party Root Certification Authorities)
Export-Certificate -Cert "Cert:\CurrentUser\My\$($ca_certificate.Thumbprint)" -FilePath "$PSScriptRoot\root-authority-public.cer"
```

```
# Run this script once for each server for which an SSL certificate is needed.
# Certificate should be executed on the single computer where the CA certificate is located.
# The created server SSL certificate should then be moved to the server and imported in the
# certificate store there.
# After importing the certificate, allow access to the private key of the certificate for
# the service user(s) of the services that must use the certificate.

# Load CA certificate from store (thumbprint must be in ca_thumbprint.txt)
$ca_thumbprint = Get-Content -Path "$PSScriptRoot\ca_thumbprint.txt"
$ca_certificate = (Get-ChildItem -Path cert:\CurrentUser\My\$ca_thumbprint)

# Prompt user for DNS names to include in certificate
$dnsNames = Read-Host 'DNS names for server SSL certificate (delimited by space - 1st entry is also subject of certificate)'
$dnsNamesArray = @($dnsNames -Split ' ' | foreach { $_.Trim() } | where { $_ })

if ($dnsNamesArray.Length -eq 0) {
    Write-Host -ForegroundColor Red 'At least one dns name should be specified'
    exit
}
$subjectName = $dnsNamesArray[0]
$dnsEntries = ($dnsNamesArray | foreach { "DNS=$_" }) -Join '&'

# Optionally allow the user to type in a list of IP addresses to put in the certificate
$ipAddresses = Read-Host 'IP addresses for server SSL certificate (delemited by space)'
$ipAddressesArray = @($ipAddresses -Split ' ' | foreach { $_.Trim() } | where { $_ })
if ($ipAddressesArray.Length -gt 0) {
    $ipEntries = ($ipAddressesArray | foreach { "IPAddress=$_" }) -Join '&'
    $dnsEntries = "$dnsEntries&$ipEntries"
}

# Build final dns entries string (e.g. "2.5.29.17={text}DNS=myhost&DNS=myhost.domain.com&IPAddress=10.0.0.103")
$dnsEntries = "2.5.29.17={text}$dnsEntries"

# The only required purpose of the sertificate is "Server Authentication"
$serverAuthentication = '2.5.29.37={critical}{text}1.3.6.1.5.5.7.3.1'

# Now - create the server SSL certificate
$certificate = New-SelfSignedCertificate -CertStoreLocation Cert:\CurrentUser\My -Subject $subjectName -Signer $ca_certificate `
                                         -FriendlyName 'VMS SSL Certificate' -TextExtension @($dnsEntries, $serverAuthentication)

# Export certificate to disk - protect with a password
$password = Read-Host -AsSecureString "Server SSL certificate password"
Export-PfxCertificate -Cert "Cert:\CurrentUser\My\$($certificate.Thumbprint)" -FilePath "$PSScriptRoot\$subjectName.pfx" -Password $password

# Delete the server SSL certificate from the local certificate store
$certificate | Remove-Item
```

```
# Run this script once for each management server for which a certificate is needed.
# Certificate should be executed on the single computer where the CA certificate is located.
# The created certificate should then be moved to the management servers and
# imported in the certificate store there.

# Load CA certificate from store (thumbprint must be in ca_thumbprint.txt)
$ca_thumbprint = Get-Content -Path "$PSScriptRoot\ca_thumbprint.txt"
$ca_certificate = (Get-ChildItem -Path cert:\CurrentUser\My\$ca_thumbprint)

# Prompt user for DNS names to include in certificate
$dnsNames = Read-Host 'DNS names for management server certificate (comma delimited - 1st entry is also subject of certificate)'
$dnsNamesArray = @($dnsNames -Split ',' | foreach { $_.Trim() } | where { $_ })

if ($dnsNamesArray.Length -eq 0) {
    Write-Host -ForegroundColor Red 'At least one dns name should be specified'
    exit
}

$dnsEntries = ($dnsNamesArray | foreach { "DNS=$_" }) -Join '&'

# Optionally allow the user to type in a list of IP addresses to put in the certificate
$ipAddresses = Read-Host 'IP addresses for management server certificate (comma delimited)'
$ipAddressesArray = @($ipAddresses -Split ',' | foreach { $_.Trim() } | where { $_ })
if ($ipAddressesArray.Length -gt 0) {
    $ipEntries = ($ipAddressesArray | foreach { "IPAddress=$_" }) -Join '&'
    $dnsEntries = "$dnsEntries&$ipEntries"
}
$subjectName = $ipAddressesArray[0]

# Build final dns entries string (e.g. "2.5.29.17={text}DNS=myhost&DNS=myhost.domain.com&IPAddress=10.0.0.103")
$dnsEntries = "2.5.29.17={text}$dnsEntries"

# The only required purpose of the sertificate is "Server Authentication"
$serverAuthentication = '2.5.29.37={critical}{text}1.3.6.1.5.5.7.3.1'

# Now - create the management server certificate
$certificate = New-SelfSignedCertificate -CertStoreLocation Cert:\CurrentUser\My -Subject $subjectName -Signer $ca_certificate `
                                         -FriendlyName 'VMS Server Certificate' -TextExtension @($dnsEntries, $serverAuthentication)

# Export certificate to disk - protect with a password
$password = Read-Host -AsSecureString "Management server certificate password"
Export-PfxCertificate -Cert "Cert:\CurrentUser\My\$($certificate.Thumbprint)" -FilePath "$PSScriptRoot\$subjectName.pfx" -Password $password

# Delete the management server certificate from the local certificate store
$certificate | Remove-Item
```

helpfeedback@milestone.dk

About Milestone

Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone Systems enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone Systems is a stand-alone company in the Canon Group. For more information, visit https://www.milestonesys.com/.