MAKE THE WORLD SEE

Milestone Systems

XProtect® VMS 2020 R3

Certificates guide

milestone

Contents

Copyright, trademarks, and disclaimer

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. In a Windows domain, it is recommended to establish a PKI using the Active Directory Certificate Services (AD CS).
>
> If you are unable to build such a PKI, either due to having different domains without trust between them or due to not using domains at all - it is possible to manually create and distribute certificates.
>
> WARNING: 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.

XProtect systems support secure communication:

From	To	For more information
Recording server	Management server	Management server encryption (explained) on page 9
Management server	Recording server	Encryption from the management server to the recording server (explained) on page 11
Management server	Remote servers via Data Collector: • Recording server • Event server • Log server • LPR server	Encryption between the management server and the Data Collector Server (explained) on page 12

From	To	For more information
	• Mobile server	
Clients, servers, and integrations that retrieve data streams from the recording server	Recording server	Encryption to clients and servers that retrieve data from the recording server (explained) on page 13
Mobile devices	Mobile server	Mobile server data encryption (explained) on page 15

When do I need to install 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

In the following sections, read about:

- Introduction to certificates on page 6

- Create CA certificate on page 17

- Install certificates on the clients on page 19

- Create SSL certificate on page 26

- Import SSL certificate on page 28

- Enable encryption on page 37

- View encryption status to clients on page 45

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

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

A certificate authority (CA) can issue certificates to web services on servers using a CA certificate. This certificate contains two keys, a private key and 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 certificate to exchange a secret key and thereby establish a secure SSL/TLS connection.

For more information about TLS: https://en.wikipedia.org/wiki/Transport_Layer_Security

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

- In the communication between the management server and the recording servers

- On the recording server in the communication with clients, servers and integrations that retrieve data streams from the recording server

- In the communication from clients to 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

- Some third-party MIP SDK integrations

> ⚠ 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.

Certificate distribution

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS.
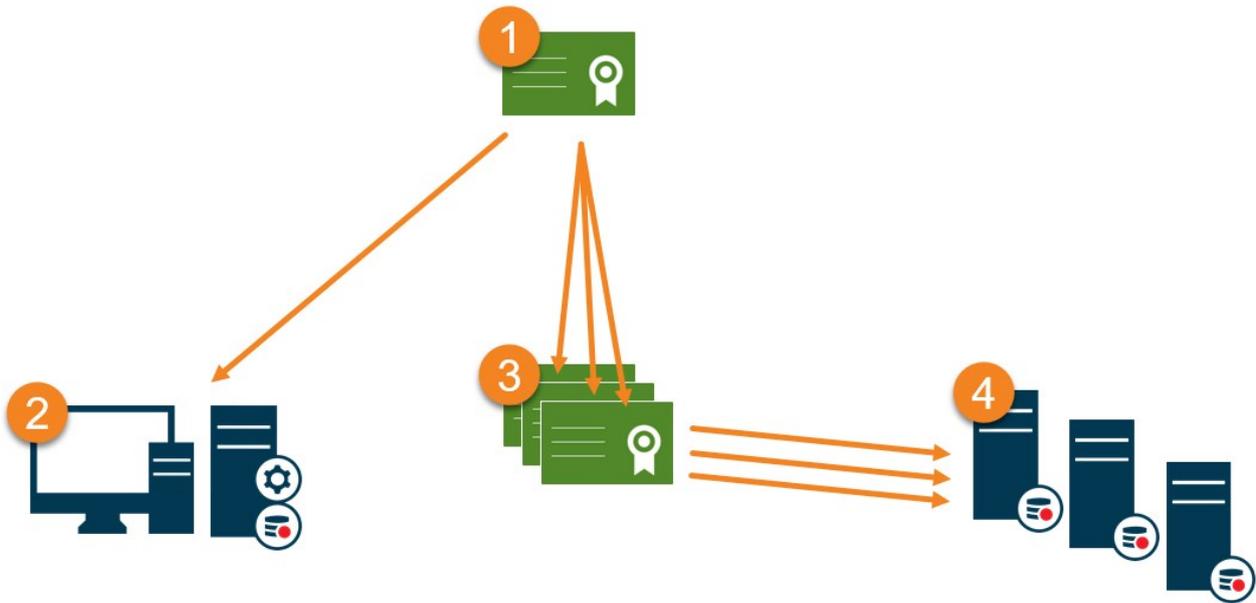
❶ A CA certificate acts as a trusted third-party, trusted by both the Subject/owner (server) and by the party that verifies the certificate (clients) (see Create CA certificate on page 17).

❷ The public CA 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).

❸ The CA certificate is used to issue private server authentication certificates to the servers (see Create SSL certificate on page 26).

❹ The created private SSL certificates must be imported to the Windows Certificate Store on all servers (see Import SSL certificate on page 28).

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. XProtect VMS will not warn you 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.

For more information, see the certificates guide about how to secure your XProtect VMS installations.

Secure communication (explained)

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

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

A certificate authority (CA) can issue certificates to web services on servers using a CA certificate. This certificate contains two keys, a private key and 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 certificate to exchange a secret key and thereby establish a secure SSL/TLS connection.

For more information about TLS: https://en.wikipedia.org/wiki/Transport_Layer_Security

> ⚠ Certificates have an expiry date. XProtect VMS will not warn you when a certificate is about to expire. If a certificate expires:
> • The clients will no longer trust the recording server with the expired certificate and thus cannot communicate with it
> • The recording servers will no longer trust the management server with the expired certificate and thus cannot communicate with it
> • The mobile devices will no longer trust the mobile 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.

When you renew a certificate with the same subject name and add it to the Windows Certificate Store, the servers will automatically pick up the new certificate. This makes it easier to renew certificates for many servers without having to re-select the certificate for each server and without restarting the services.

Management server encryption (explained)

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.

Certificate distribution for management servers

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication to the management server.
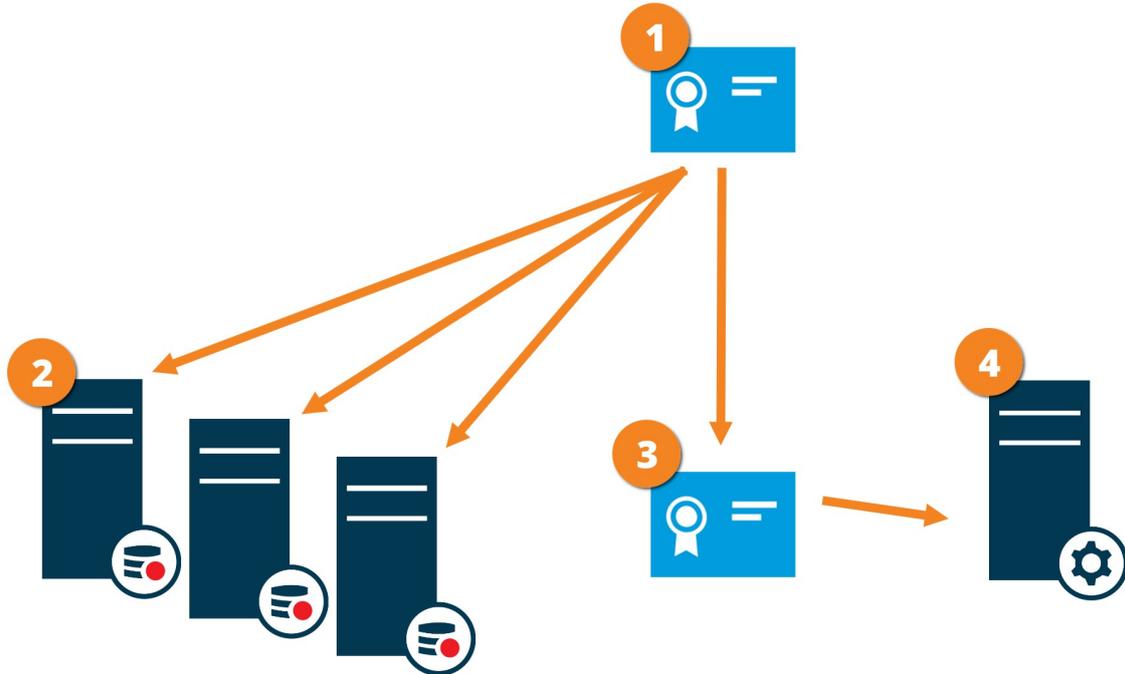
❶ A CA certificate acts as a trusted third party, trusted by both the subject/owner (management server) and by the party that verifies the certificate (recording servers)

❷ The CA certificate must be trusted on all recording servers. In this way the recording servers can verify the validity of the certificates issued by the CA

❸ The CA certificate is used to establish secure connection between the management server and the recording servers

❹ The CA certificate must be installed on the computer on which the management server is running

Requirements for the private management server certificate:

- Issued to the management server so that the management 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 the management server itself, by trusting the CA certificate that was used to issue the management server certificate

- Trusted on all recording servers connected to the management server, by trusting the CA certificate that was used to issue the management server certificate

Encryption from the management server to the recording server (explained)

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. Encryption of this communication must follow the encryption setting on the management server. So, if management server encryption is enabled, this must also be enabled on the recording servers, and vice-versa. Before you enable encryption, you must install security certificates on the management server and all recording servers, including failover recording servers.

Certificate distribution

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication from the management server.

❶ A CA certificate acts as a trusted third party, trusted by both the subject/owner (recording server) and by the party that verifies the certificate (management server)

❷ The CA certificate must be trusted on the management server. In this way the management server can verify the validity of the certificates issued by the CA

❸ The CA certificate is used to establish secure connection between the recording servers and the management server

❹ The CA certificate must be installed on the computers on which the recording servers are running

Requirements for the private recording server certificate:

- Issued to the recording server so that the recording 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 the management server, by trusting the CA certificate that was used to issue the recording server certificate

# Encryption between the management server and the Data Collector Server (explained)

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

When you enable encryption on the management server, it applies to connections from all the Data Collector servers that connect to the management server. Encryption of this communication must follow the encryption setting on the management server. So, if management server encryption is enabled, this must also be enabled on the Data Collector servers affiliated with each remote server, and vice-versa. Before you enable encryption, you must install security certificates on the management server and all Data Collector servers affiliated with the remote servers.

Certificate distribution

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication from the management server.
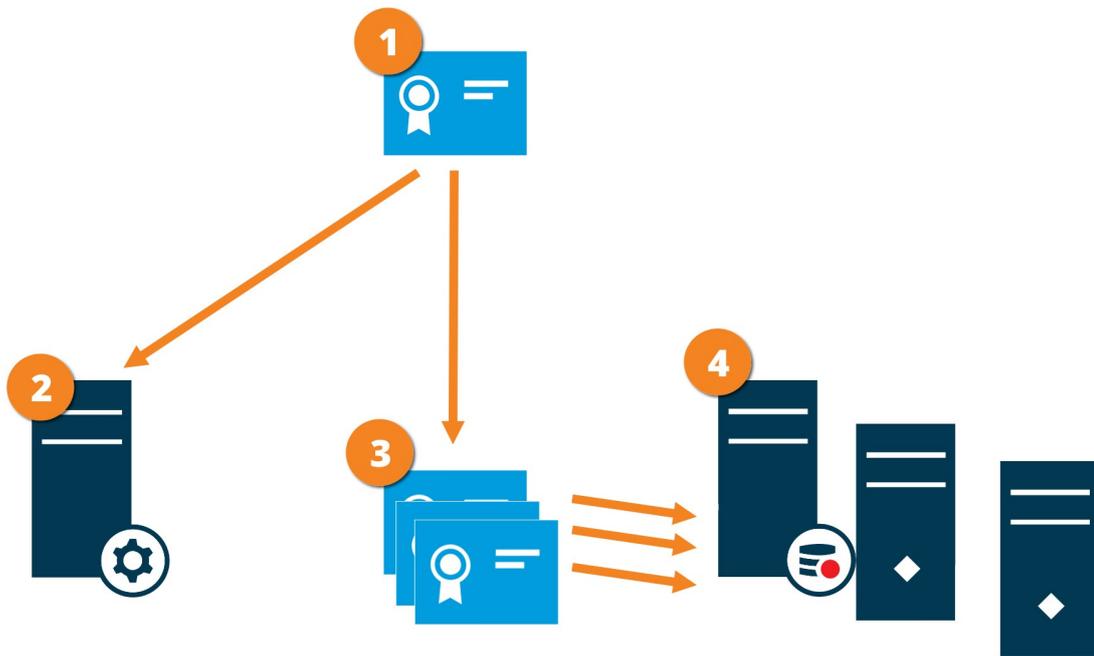
❶ A CA certificate acts as a trusted third party, trusted by both the subject/owner (data collector server) and by the party that verifies the certificate (management server)

❷ The CA certificate must be trusted on the management server. In this way the management server can verify the validity of the certificates issued by the CA

❸ The CA certificate is used to establish secure connection between the data collector servers and the management server

❹ The CA certificate must be installed on the computers on which the data collector servers are running

Requirements for the private data collector server certificate:

- Issued to the data collector server so that the data collector 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 the management server, by trusting the CA certificate that was used to issue the data collector server certificate

Encryption to clients and servers that retrieve data from the recording server (explained)

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 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

- 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.

Certificate distribution

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication to the recording server.
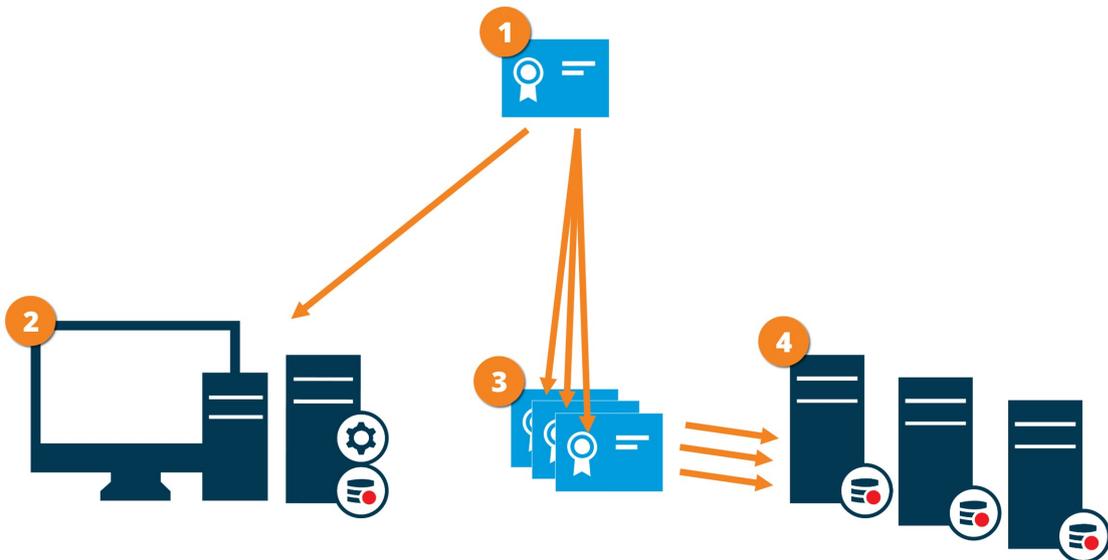
❶ A CA certificate acts as a trusted third-party, trusted by both the subject/owner (recording server) and by the party that verifies the certificate (all clients)

❷ The CA certificate must be trusted on all clients. In this way the clients can verify the validity of the certificates issued by the CA

❸ The CA certificate is used to establish secure connection between the recording servers and all clients and services

❹ The CA certificate must be installed on the computers on which the recording servers are running

Requirements for the private recording server certificate:

- Issued to the recording server so that the recording 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 that retrieve data streams from the recording servers, by trusting the CA certificate that was used to issue the recording server certificate

- The service account that runs the recording server must have access to the private key of the certificate on the recording server.

> If you enable encryption on the recording servers and your system applies failover recording servers, Milestone recommends that you also prepare the failover recording servers for encryption.

Mobile server data encryption (explained)

In XProtect VMS, encryption is enabled or disabled per mobile server. When you enable encryption on a mobile server, you will have the option to use encrypted communication with all clients, services, and integrations that retrieve data streams.

Certificate distribution for mobile servers

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication with the mobile server.
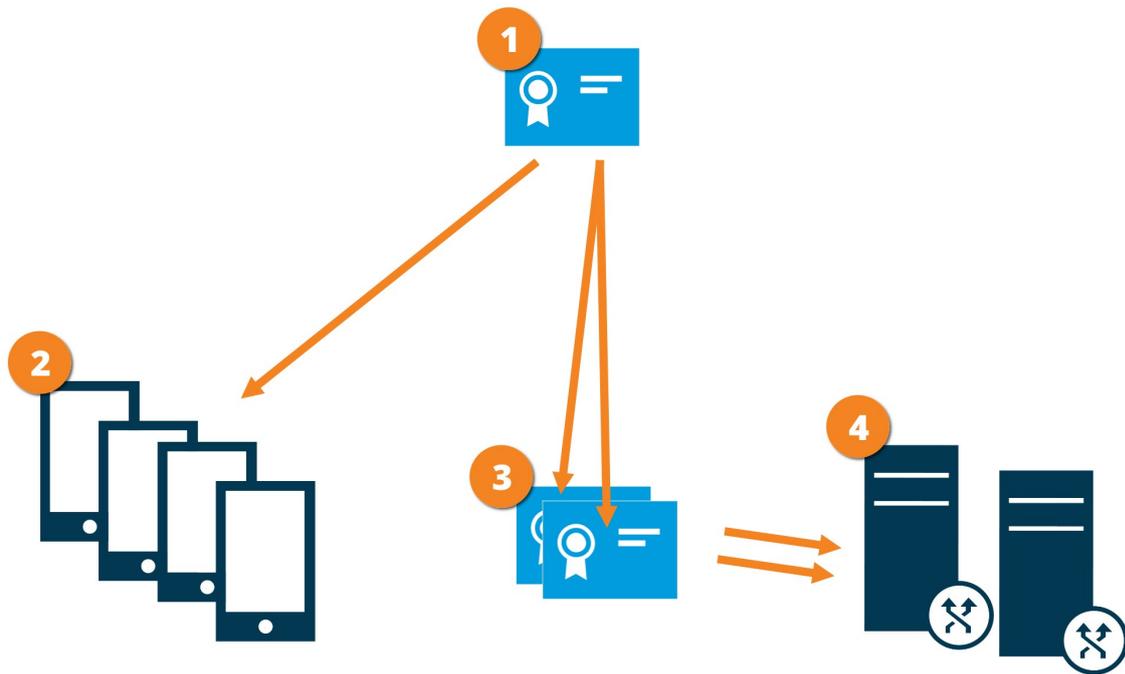
❶ A CA certificate acts as a trusted third party, trusted by both the subject/owner (mobile server) and by the party that verifies the certificate (all clients)

❷ The CA certificate must be trusted on all clients. In this way clients can verify the validity of the certificates issued by the CA

❸ The CA certificate is used to establish secure connection between the mobile server and clients and services

❹ The CA certificate must be installed on the computer on which the mobile server is running

Requirements for the CA certificate:

- The mobile server's host name must be included in the certificate, either as subject/owner or in the list of DNS names that the certificate is issued to

- The certificate must be trusted on all devices that are running services that retrieve data streams from the mobile server

- The service account that runs the mobile server must have access to the private key of the CA certificate

Mobile server encryption requirements for clients

If you do not enable encryption and use an HTTP connection, the push-to-talk feature in XProtect Web Client will not be available.

Creating and distributing certificates manually

⚠️ 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.

This script creates two certificates:

- A private certificate - only exists in the Personal Certificates store for the current user after the script is run and 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.
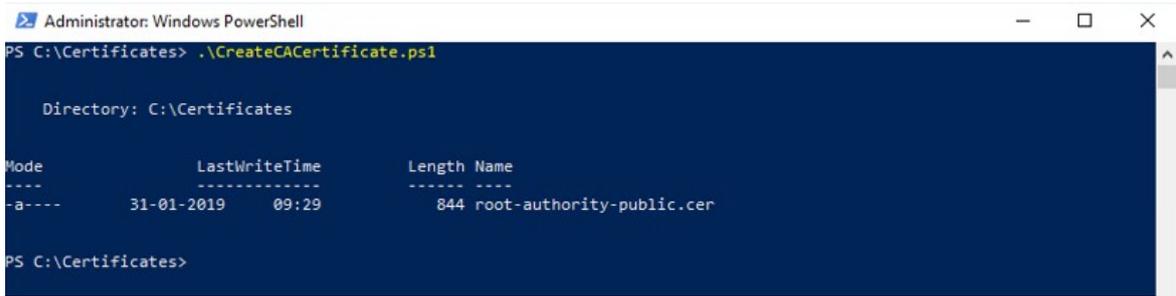

3. In Notepad, click **File** -> **Save as**, name the file **CreateCACertificate.ps1** and save it locally, like this: C:\Certificates\CreateCACertificate.ps1.

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 and graphics in the section on Secure communication (explained). Here referred to as 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 client is installed.

> ⚠️ For information about which client and server services, and integrations that require the certificate, see Introduction to certificates on page 6.

2. Right-click on the certificate and select **Install Certificate**.
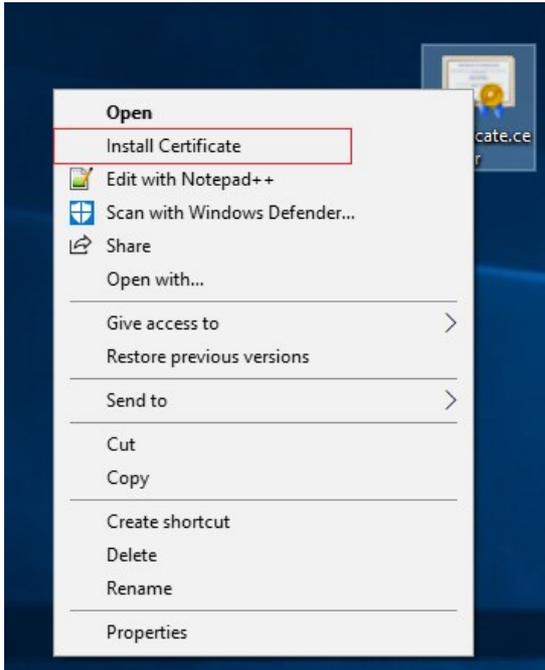
3. In the **Certificate Import Wizard**, select to install the certificate in the store of the **Local Machine** and click **Next**.
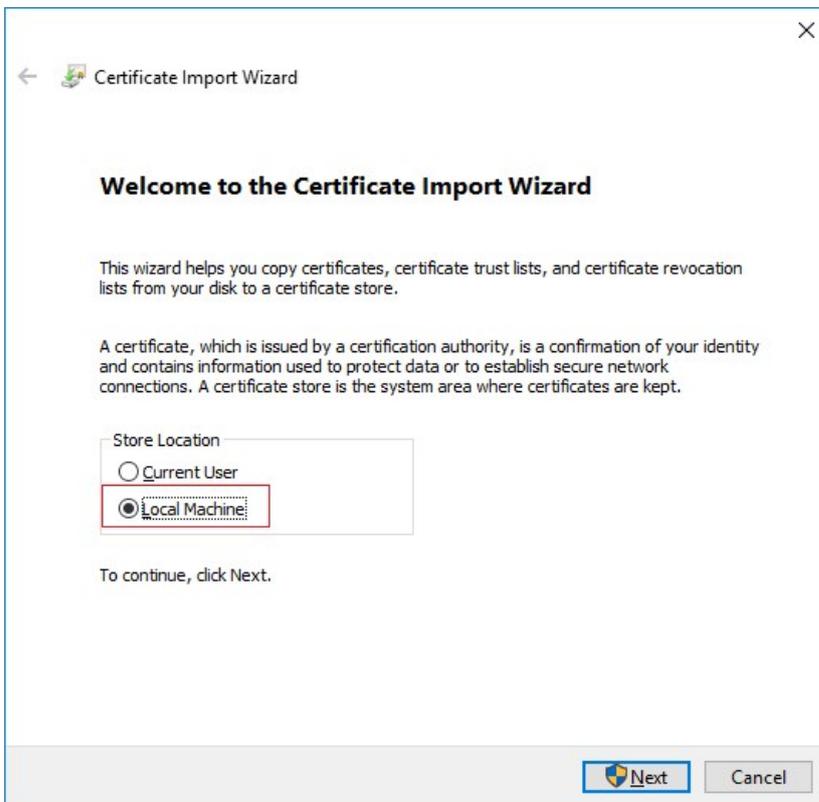
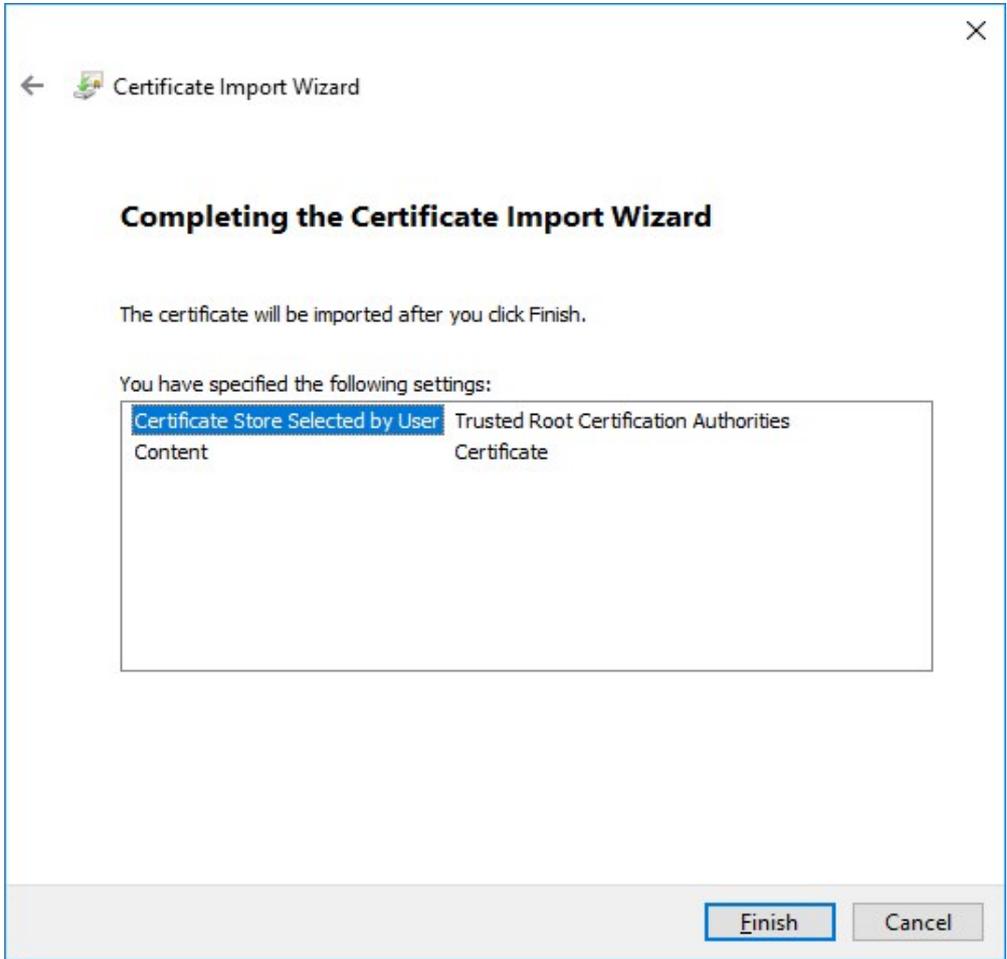4. Select to manually locate the store in which the certificate will be installed.
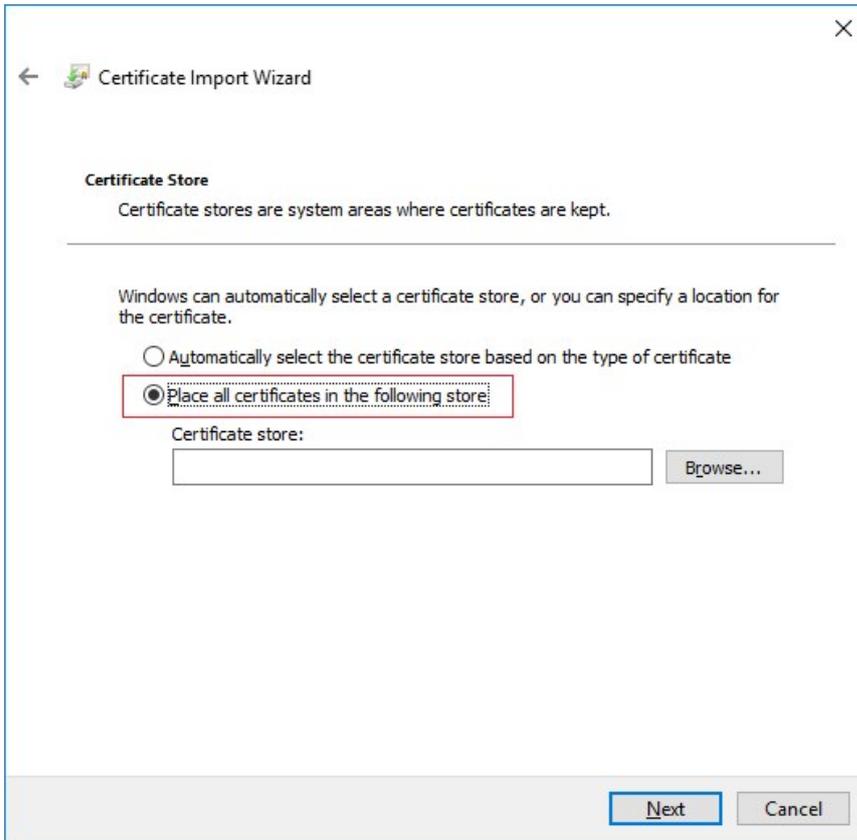
5. Click **Browse**, select **Trusted Root Certification Authorities** and click **OK**. Then click **Next**.
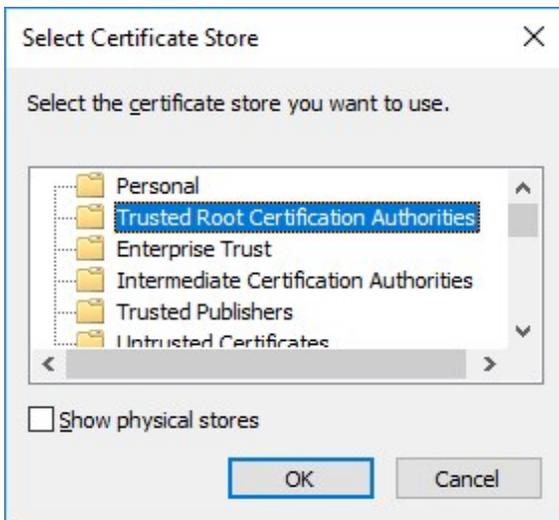
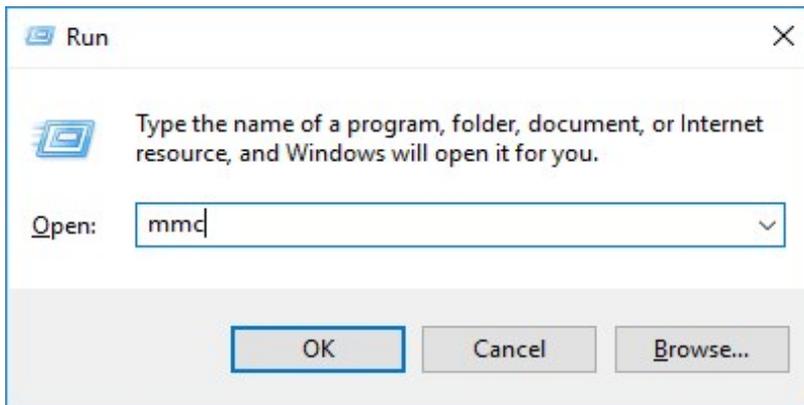6. On the **Completing the Certificate Import Wizard** dialog, click **Finish**.

> ✏️ 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.

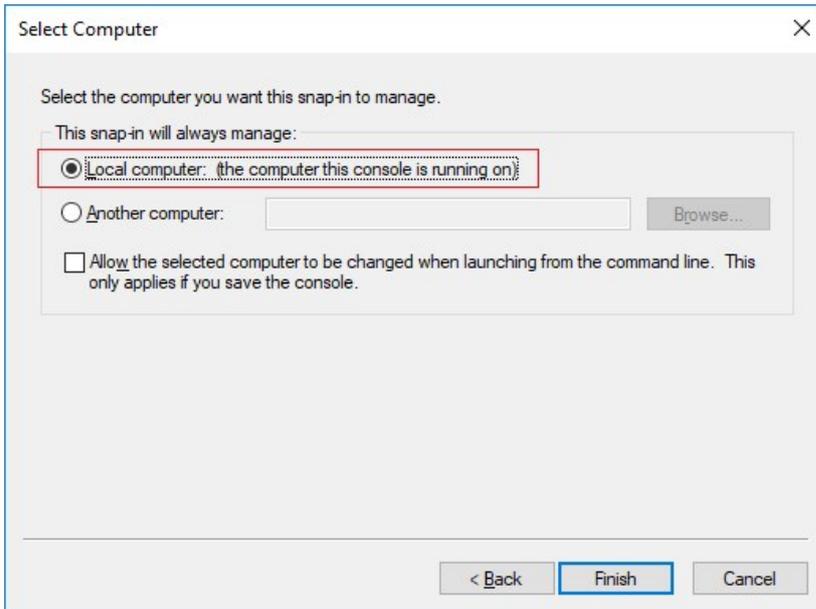9. In the Microsoft Management Console, from the **File** menu select **Add/Remove Snap-in...**.
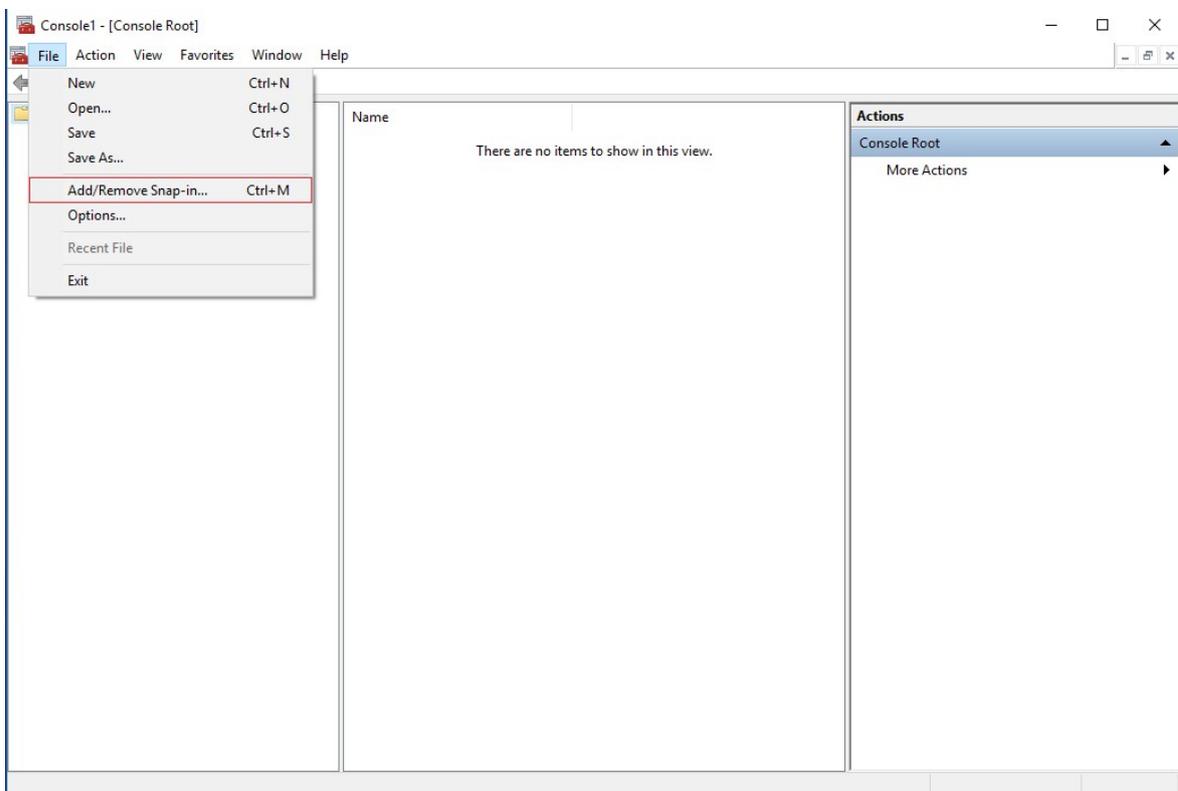
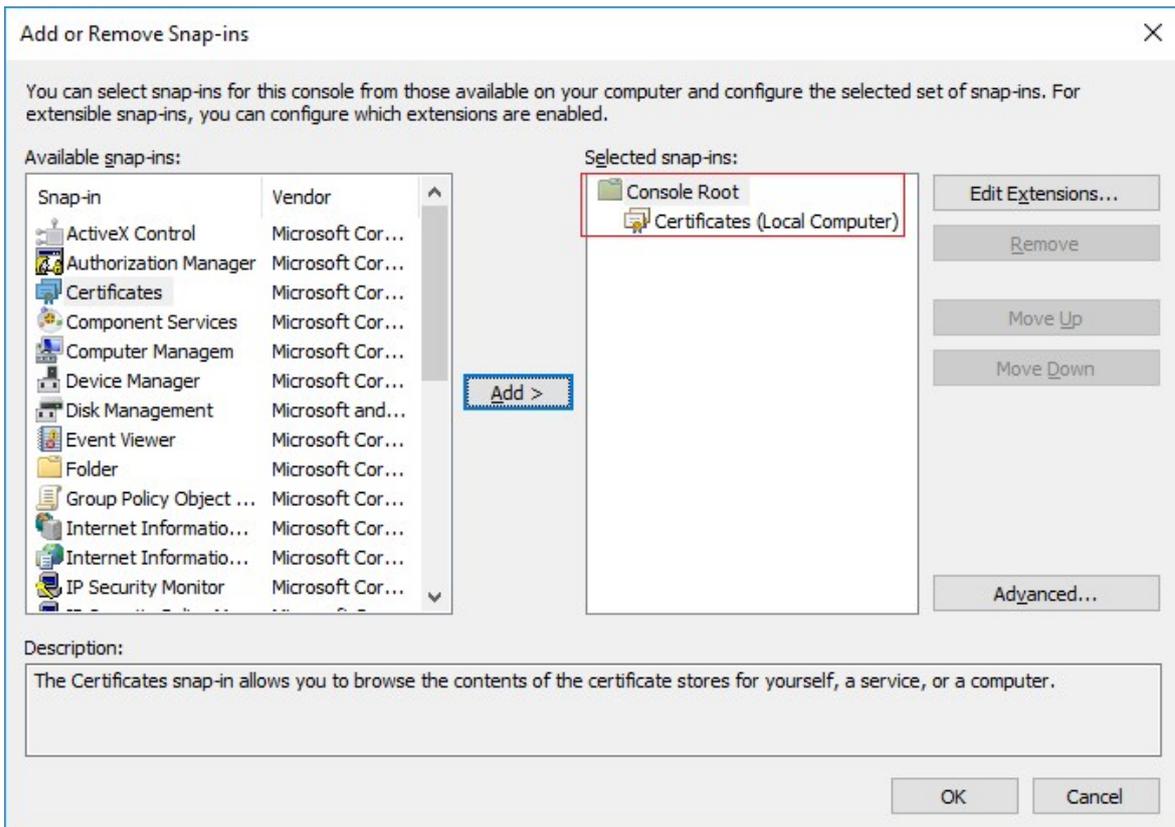10. Select the **Certificates** snap-in and click **Add**.
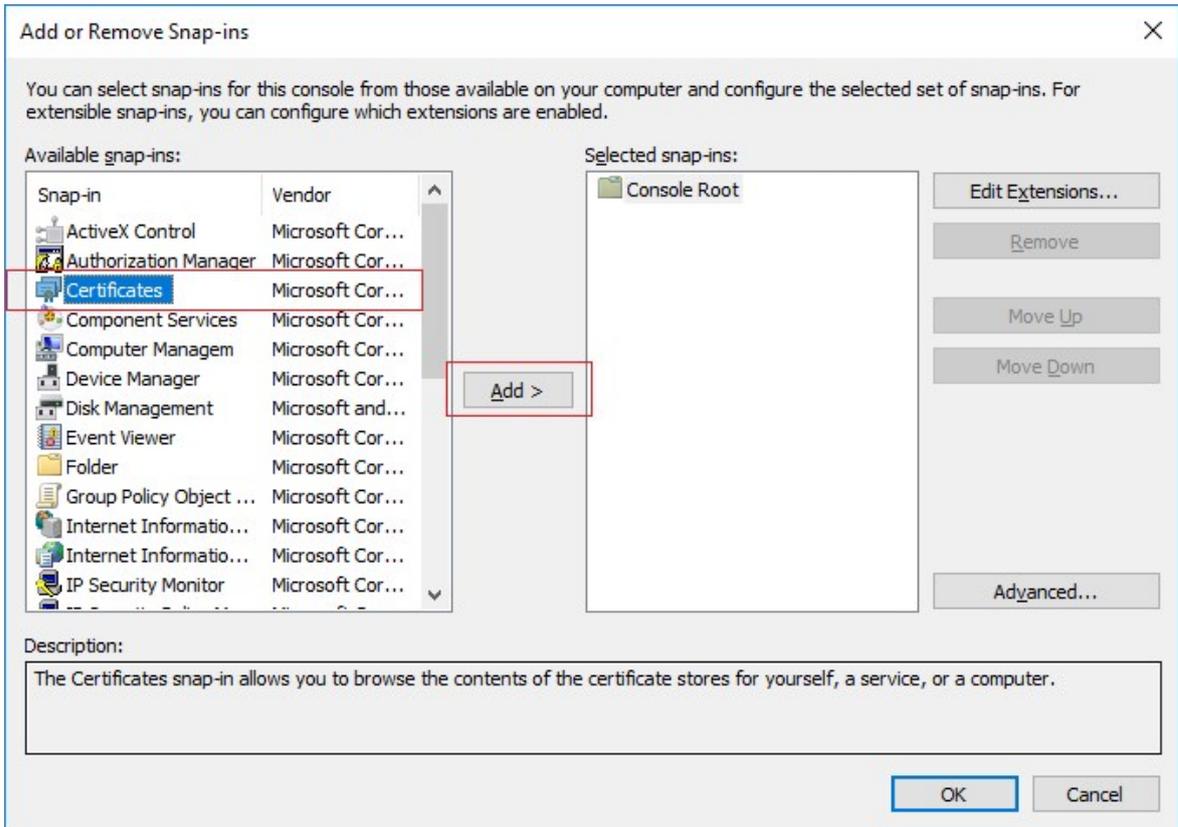
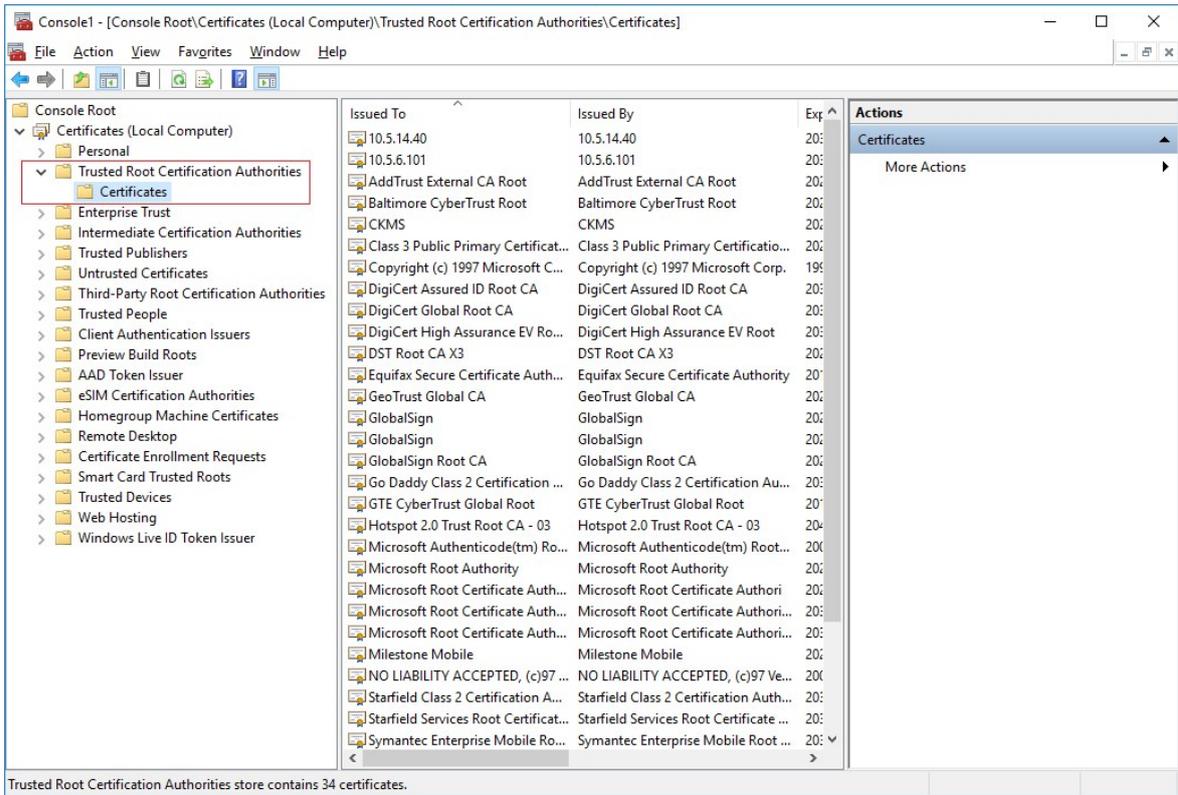11. Select that the snap-in must manage certificates for the **Computer account**.
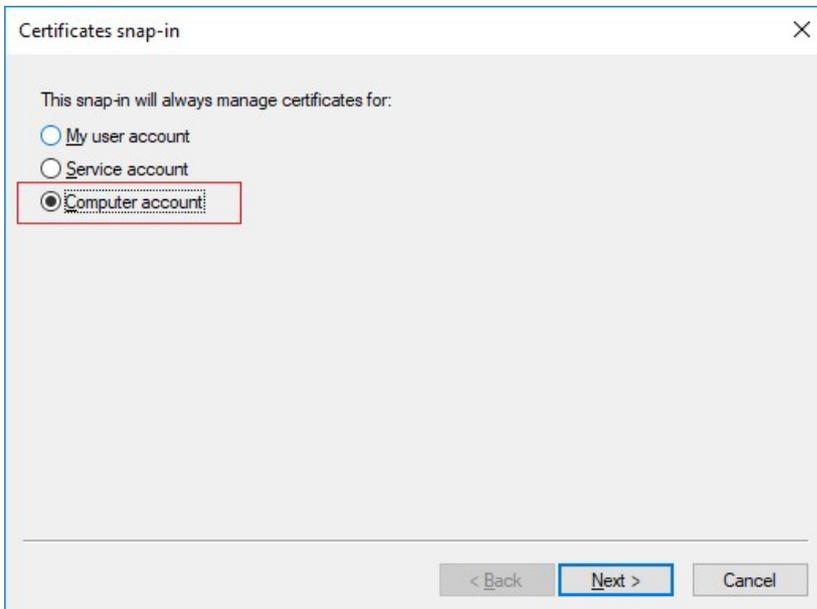
12. Select **Local computer** as the computer that you want the snap-in to manage and click **Finish**.

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).

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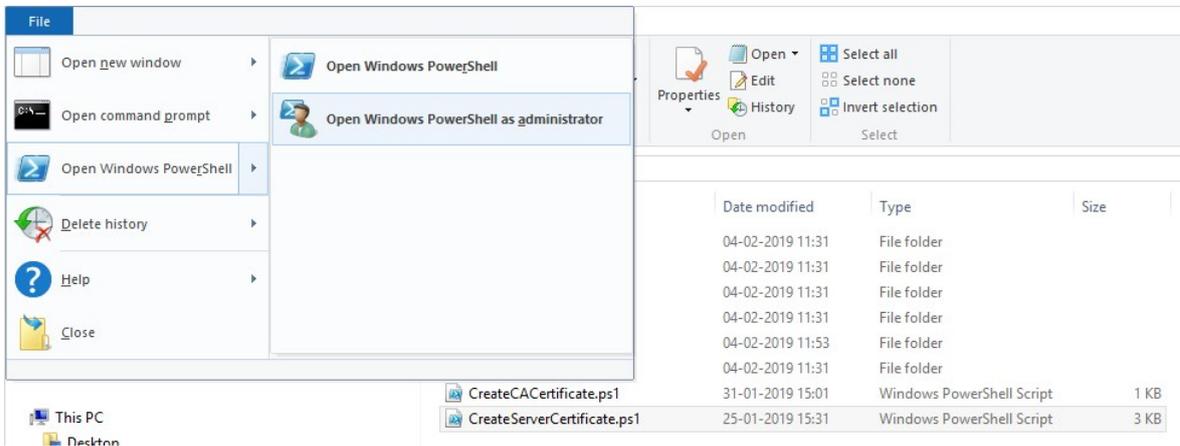
6. In PowerShell at the prompt, enter **.\CreateServerCertificate.ps1** and press **Enter**.

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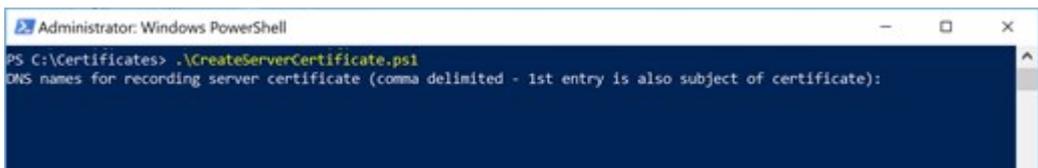
8. Enter the IP address of the server. If the server has multiple IP addresses, for example for internal and external use, add them here, separated by a space. Press **Enter**.

> ✅ 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.
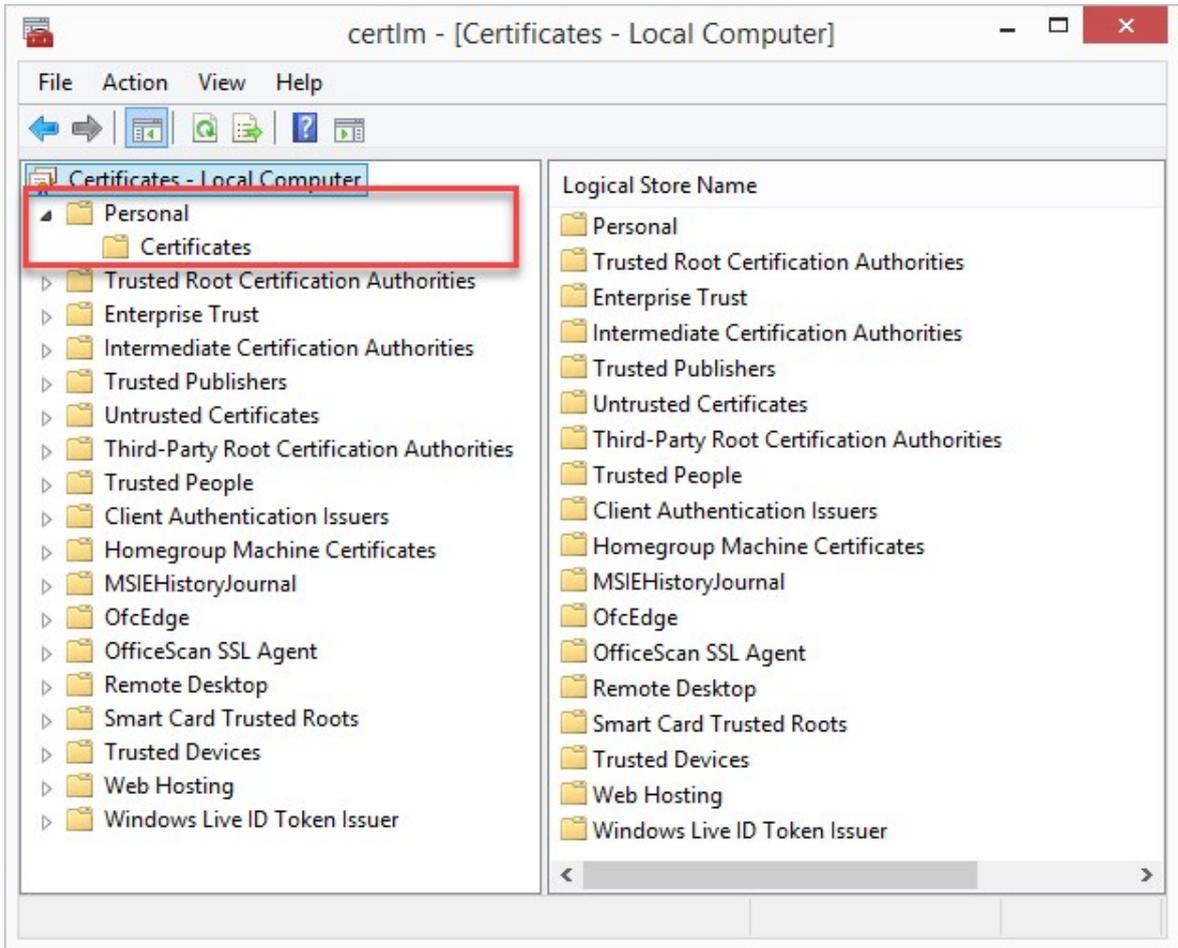
Import SSL certificate

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.
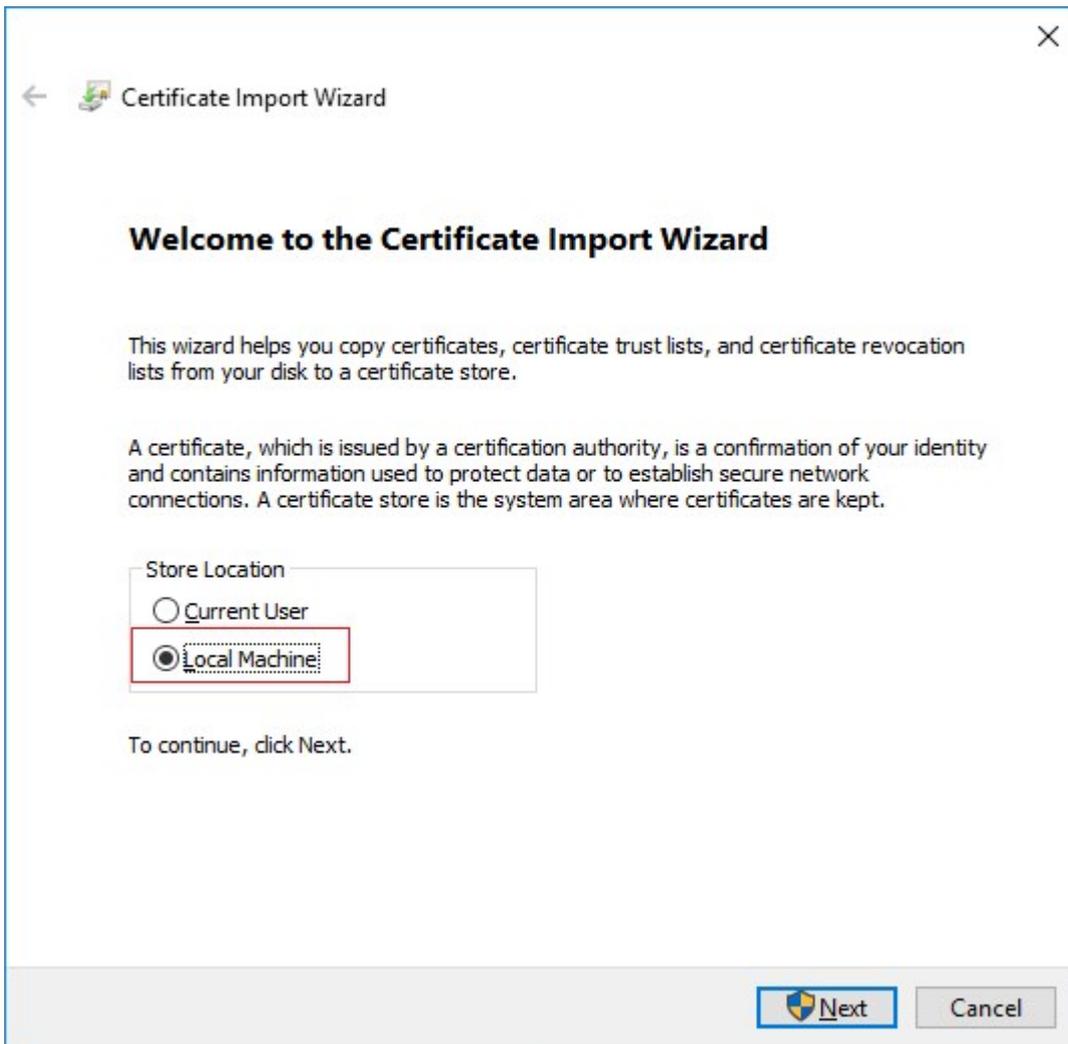
> ✏️ Remember that each certificate is created to a specific server.
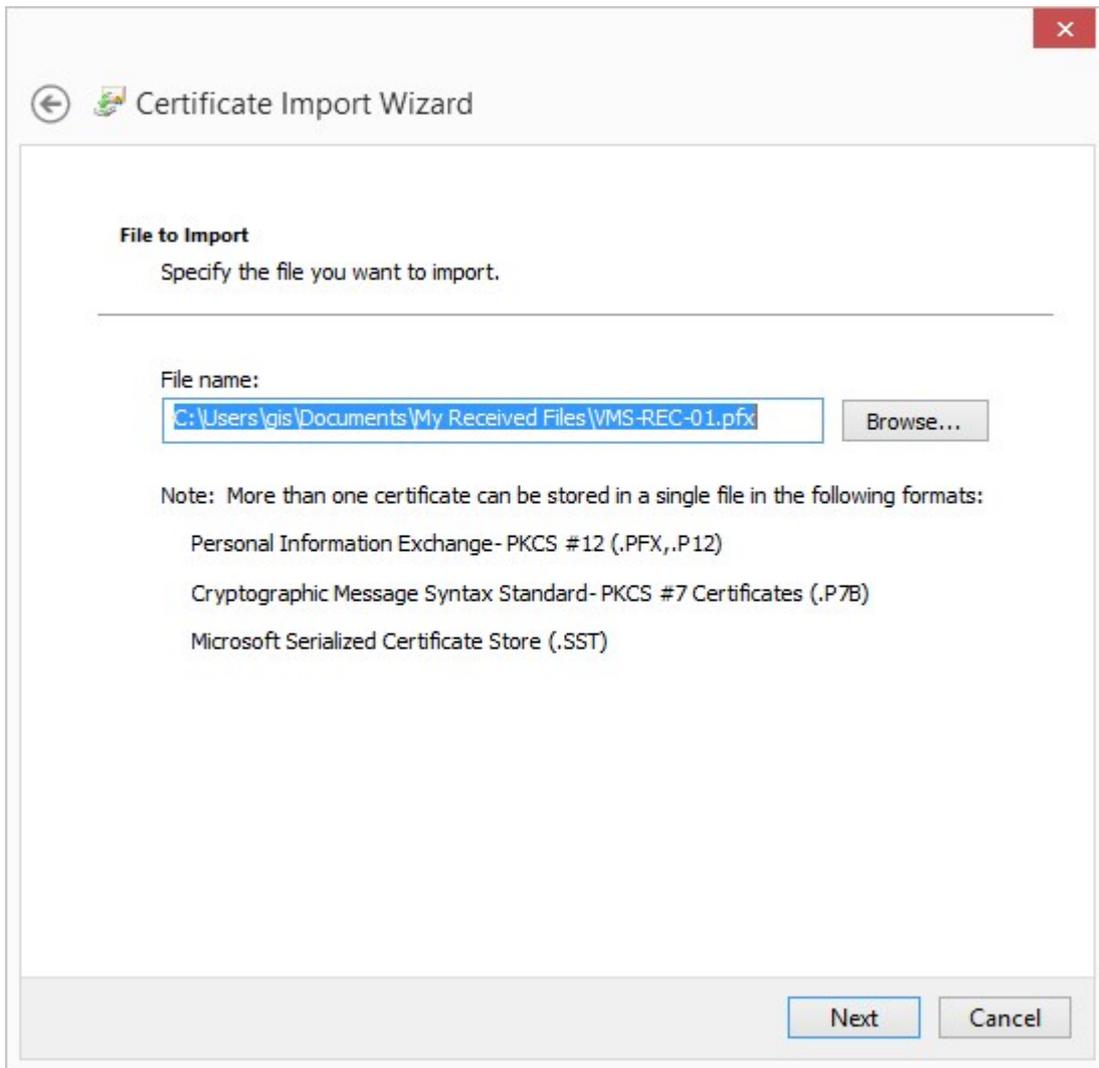
2. On the server service computer, start **Manage computer certificates**.

3. Click on **Personal**, right-click **Certificates** and select **All Tasks** > **Import**.
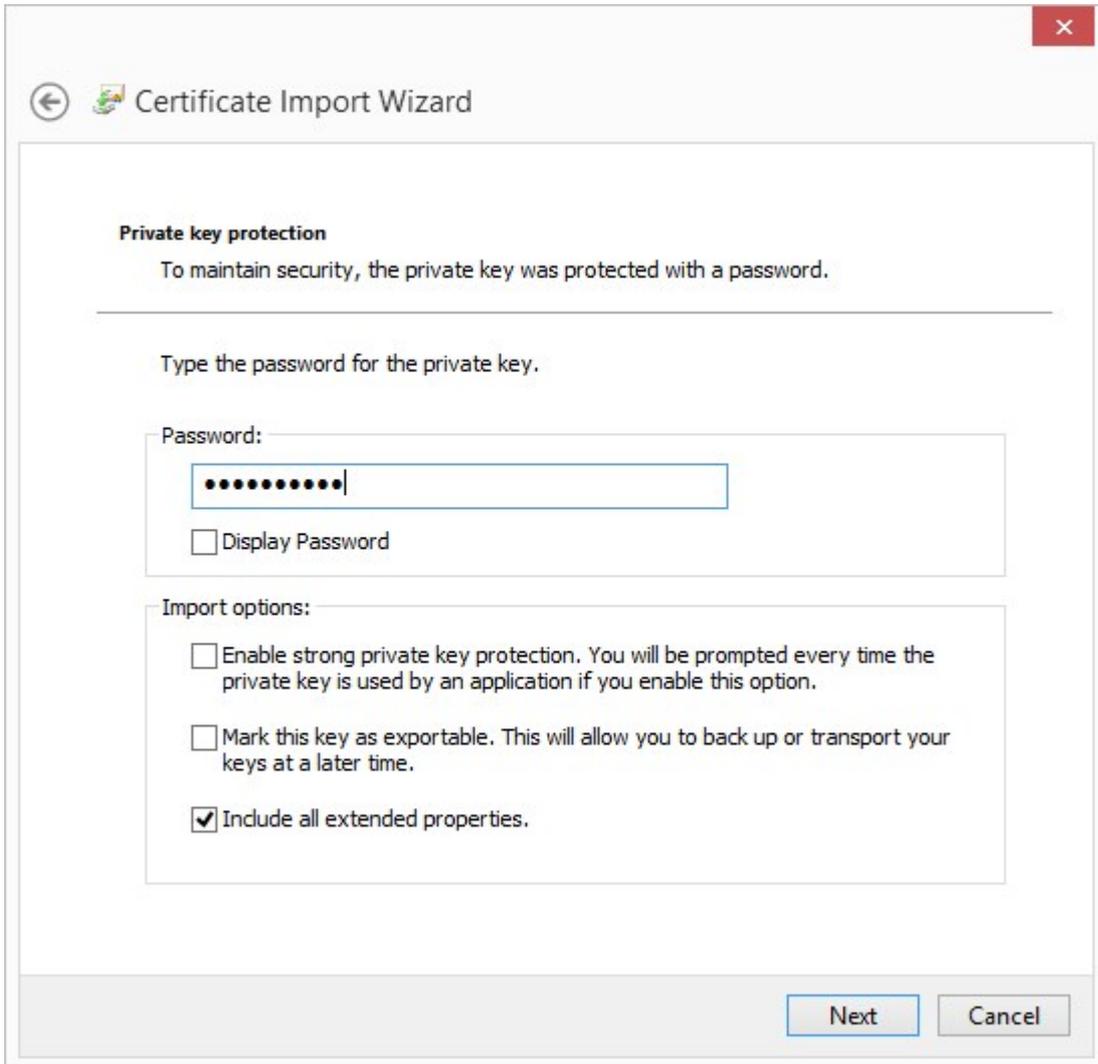
4. Select to import the certificate in the store of the **Local Machine** and click **Next**.

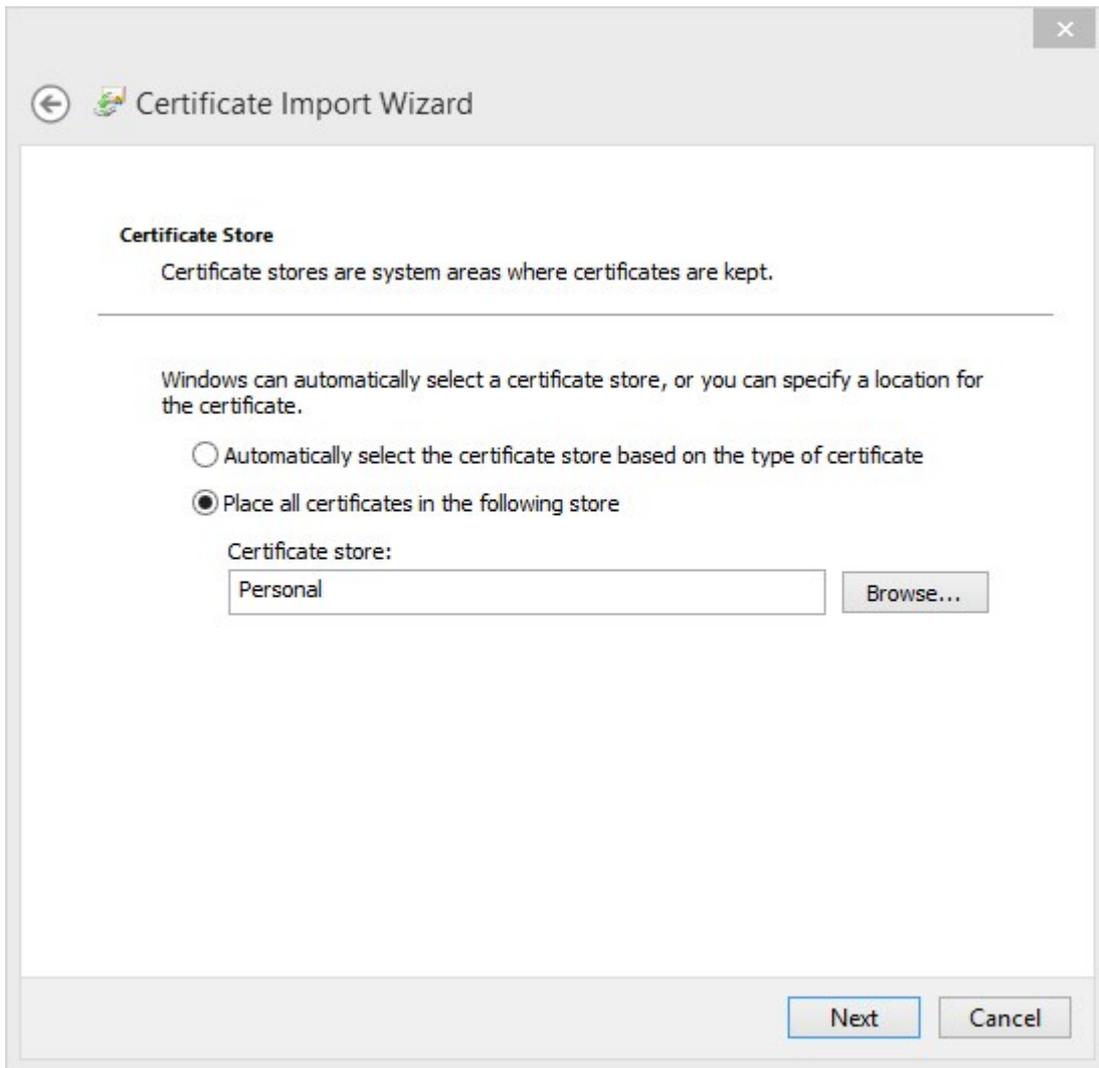5. Browse to the certificate file and click **Next**.

6. Enter the password for the private key that you specified when you created the server certificate, and click **Next**.
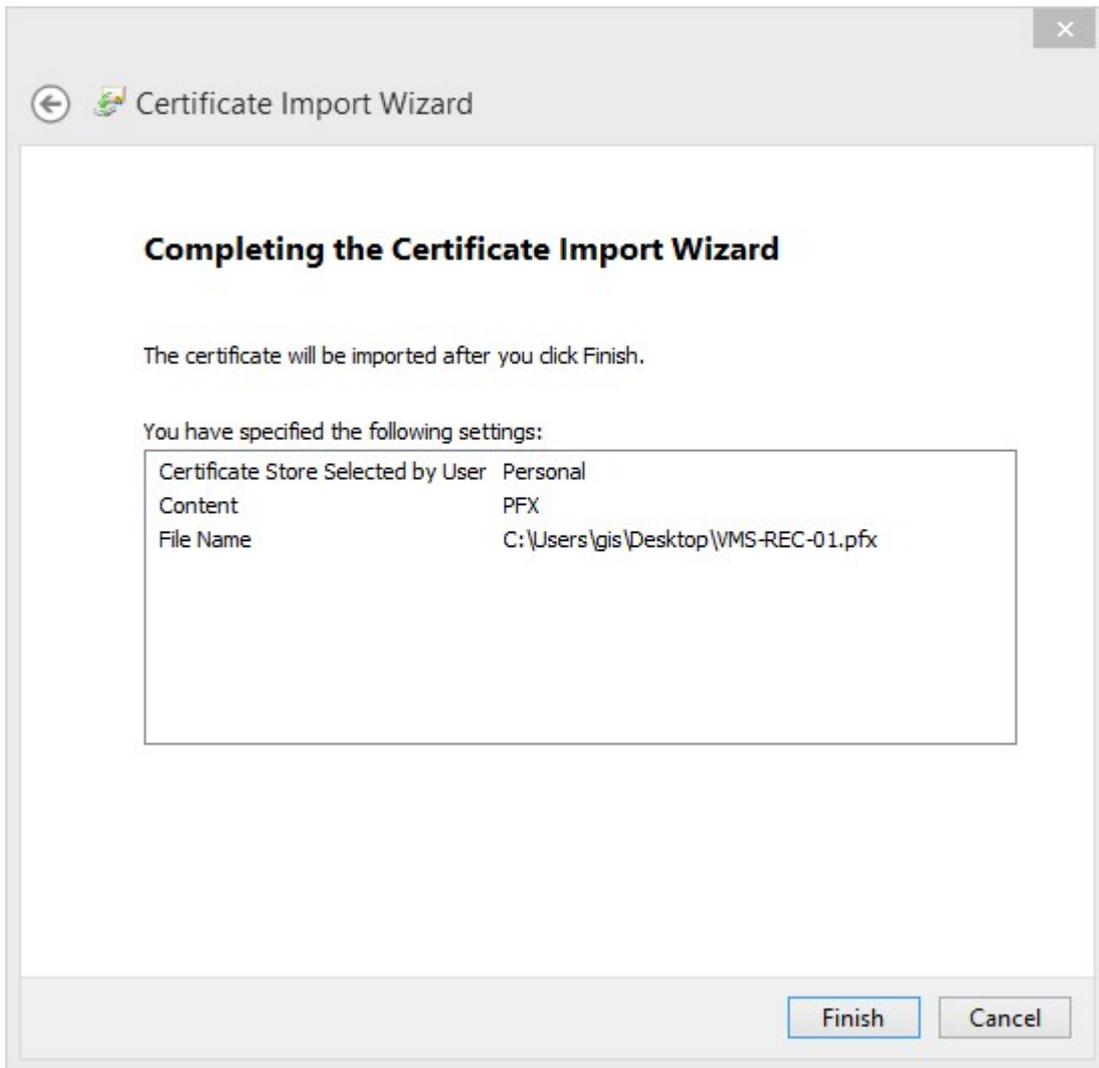
7. Place the file in the **Certificate Store**: **Personal** and click **Next**.

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

9. The imported certificate appears in the list.
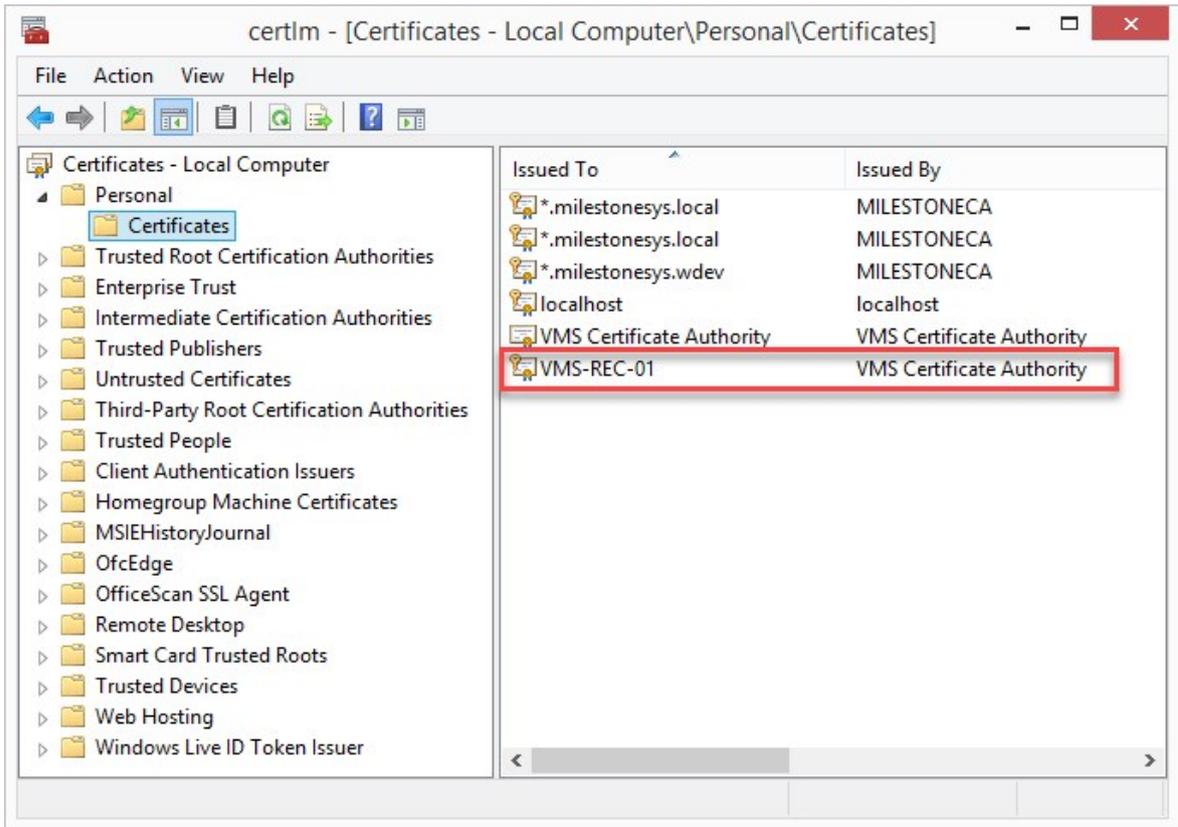
10. To allow a service to use the private key of the certificate, right click the certificate and select **All Tasks** > **Manage Private Keys**.
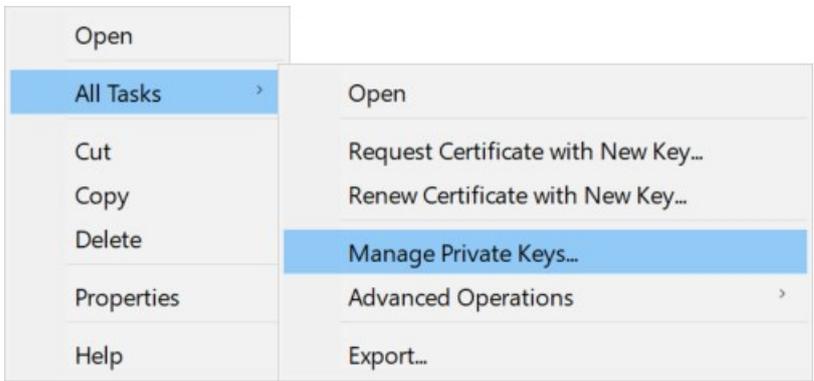
11. Add read permission for the service user for the service that needs to use the server certificate.

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

Enable encryption

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

Enable encryption to and from the management server

You can encrypt the two-way connection between the management server and the recording server or other remote servers with the data collector (Event Server, Log Server, LPR Server, and Mobile Server).

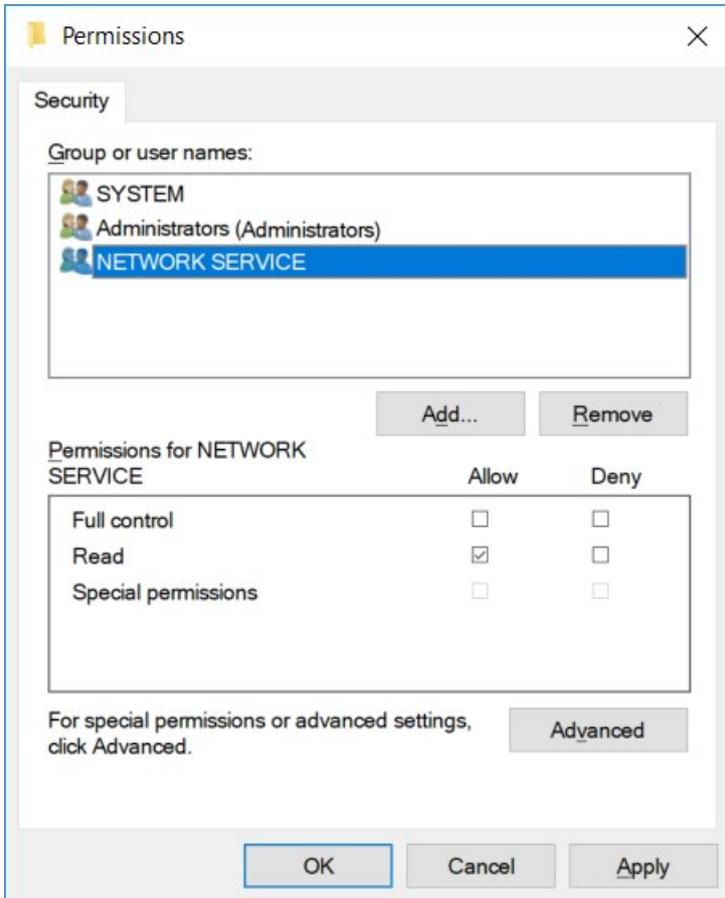If your system contains multiple recording servers or remote servers, you must enable encryption on all of them. For more information, see Management server encryption (explained) on page 9.

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.
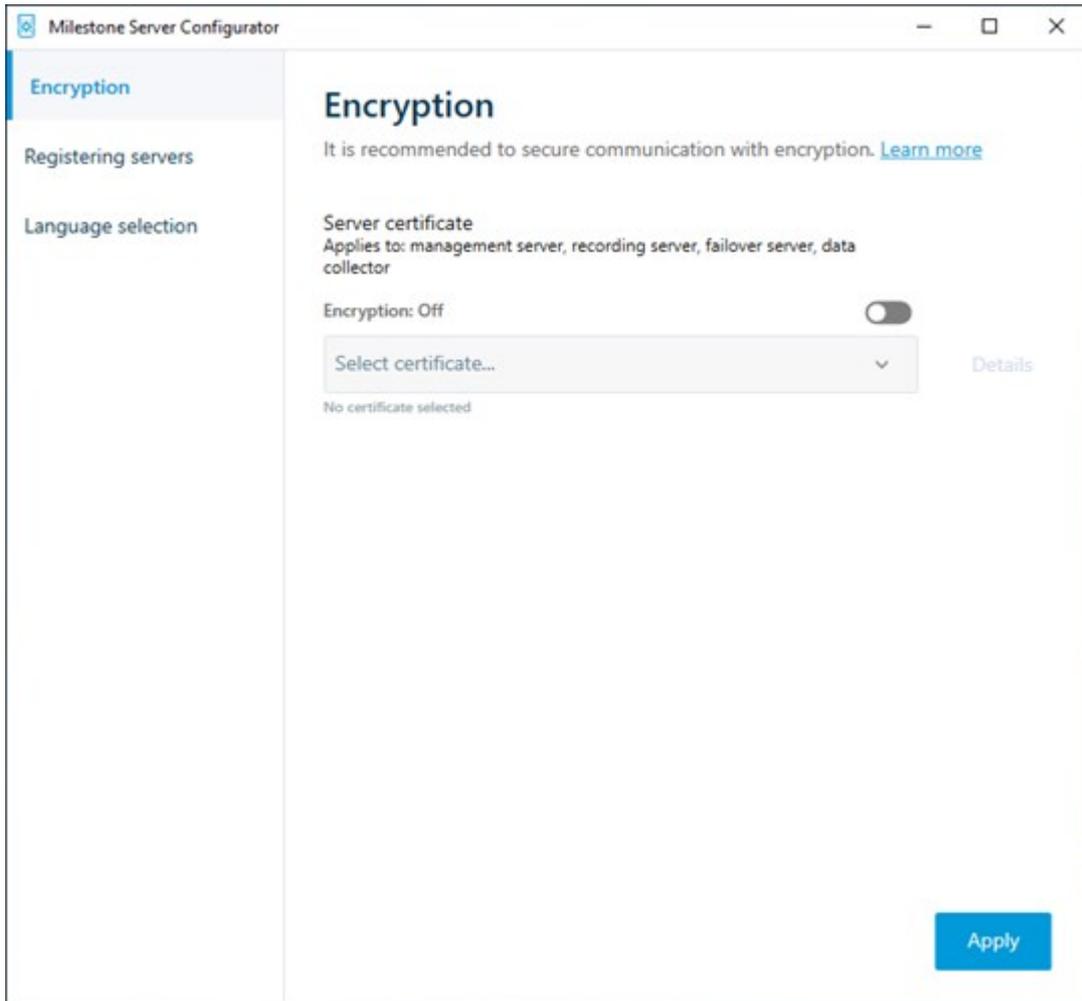
5. Click **Apply**.

To complete the enabling of encryption, the next step is to update the encryption settings on each recording server and each server with a data collector (Event Server, Log Server, LPR Server, and Mobile Server).

For more information, see Enable server encryption for recording servers or remote servers on page 38.

Enable server encryption for recording servers or remote servers

You can encrypt the two-way connection between the management server and the recording server or other remote servers with the data collector (Event Server, Log Server, LPR Server, and Mobile Server).

If your system contains multiple recording servers or remote servers, you must enable encryption on all of them. For more information, see Encryption from the management server to the recording server (explained) on page 11 and Encryption between the management server and the Data Collector Server (explained) on page 12.

Prerequisites:

- You have enabled encryption on the management server, see Enable encryption on page 37

Steps:

1. On a computer with a recording server installed, open the **Server Configurator** from:

    - The Windows Start menu

    or

    - The Recording Server Manager by right-clicking the Recording 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.

2. 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.

Enable encryption to clients and servers

You can encrypt connections from the recording server to clients and servers that stream data from the recording server. For more information, see Encryption to clients and servers that retrieve data from the recording server (explained) on page 13.

Prerequisites:

- The server authentication certificate to be used is trusted on all computers running services that retrieve

data streams from the recording server

- XProtect Smart Client and all services that retrieve data streams from the recording server must be version 2019 R1 or later

- Some third-party solutions created using MIP SDK versions earlier than 2019 R1 may need to be updated

Steps:

1. On a computer with a recording server installed, open the **Server Configurator** from:

    - The Windows Start menu

    or

    - The Recording Server Manager by right-clicking the Recording Server Manager icon on the computer task bar

2. In the **Server Configurator**, under **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 communication between the clients and servers that retrieve data streams from the recording 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.
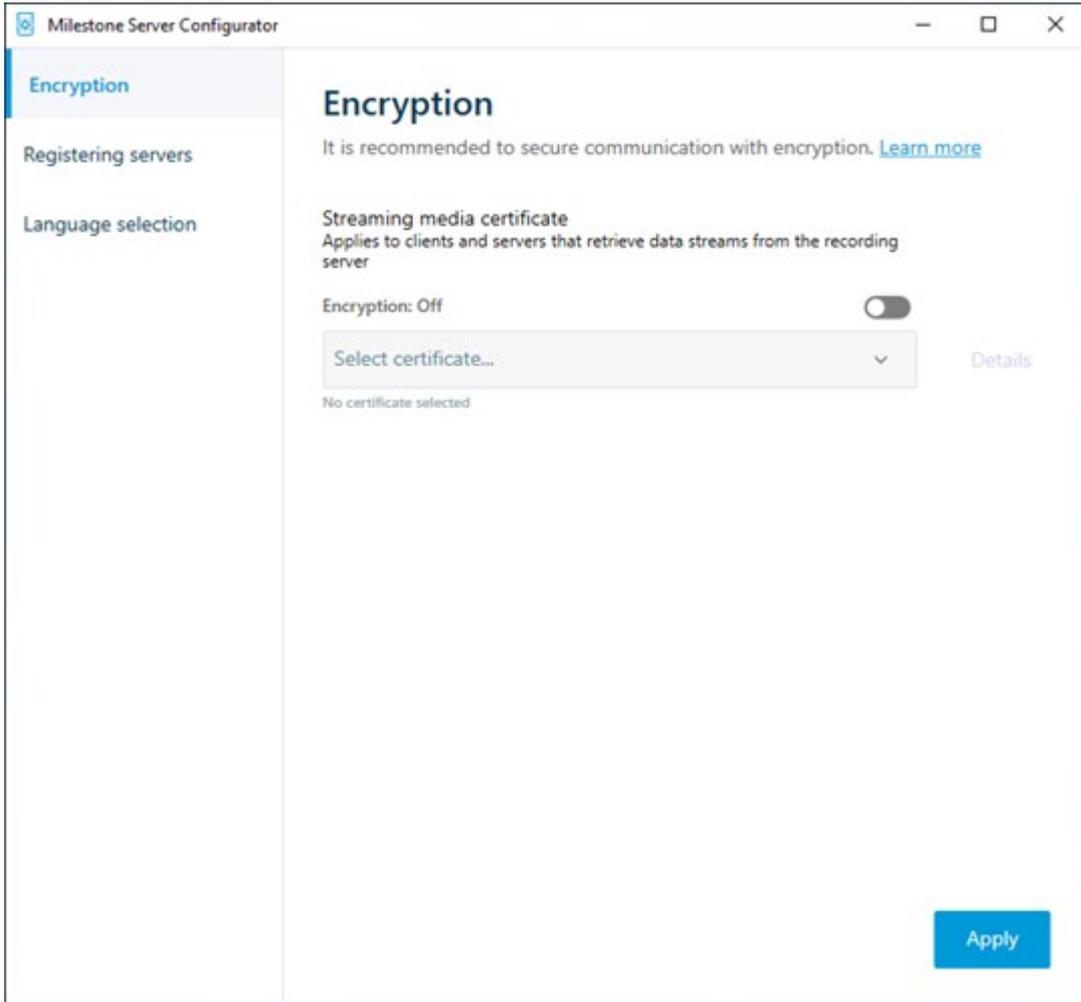
2. Click **Apply**.

> ⚠️ 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.

To verify if the recording server uses encryption, see View encryption status to clients.

Enable encryption on the mobile server

To use an HTTPS protocol for establishing 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. For more information, see Mobile server data encryption (explained) on page 15 and Mobile server encryption requirements for clients on page 16.

> 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.

Steps:

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.
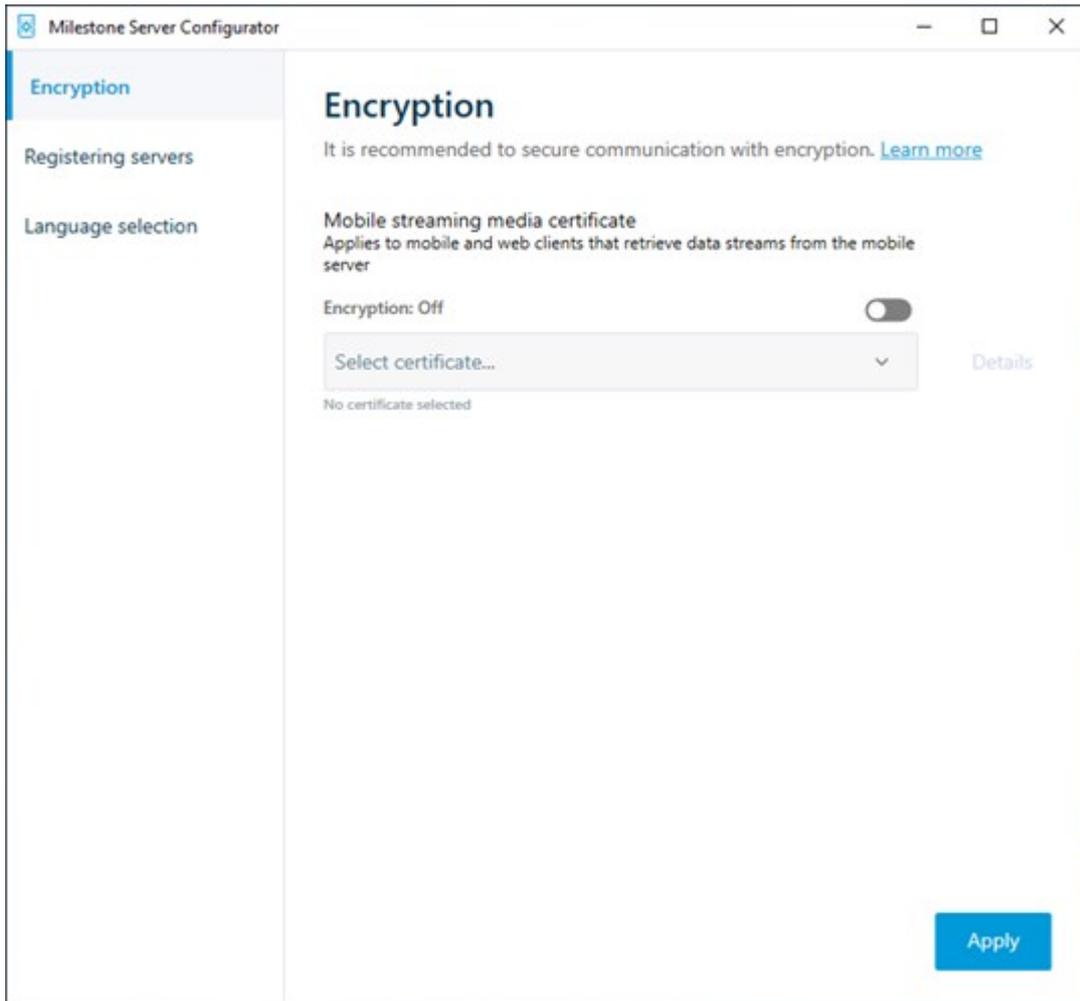
2. Click **Apply**.

> ⚠ When you apply certificates, the Mobile Server service restarts.

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.
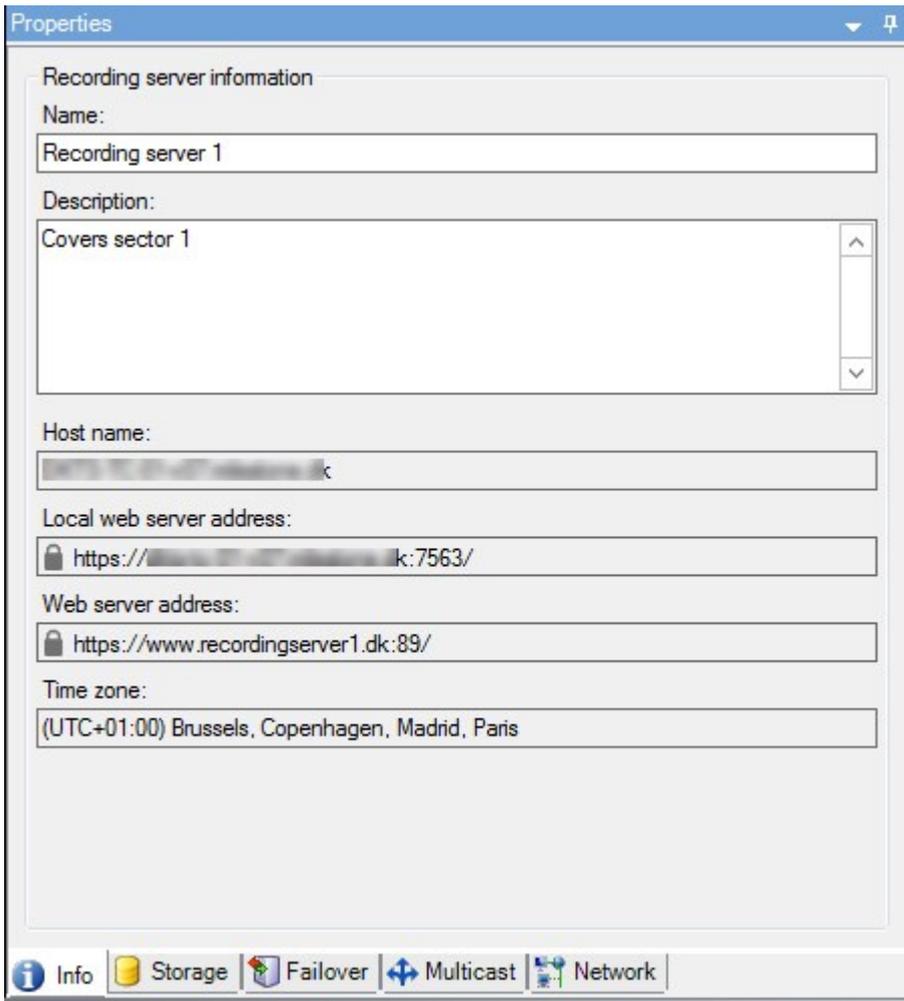
View encryption status on a failover recording server

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.

```powershell
# 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'

# 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"
```

```powershell
# 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
```

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/.