

MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS 2019 R1

Certificates guide



Contents

Copyright, trademarks, and disclaimer	3
About this guide	4
Introduction to certificates	5
Creating and distributing certificates manually	8
Create CA certificate	8
Install certificates on the clients	9
Create recording server certificate	16
Import recording server certificate	18
Enable encryption	25
View encryption status	28
Appendix A Create CA Certificate script	29
Appendix B Create Recording Server Certificate script	30

Copyright, trademarks, and disclaimer

Copyright © 2019 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

XProtect systems support secure communication from the recording server to all clients, servers, and integrations that retrieve data streams from the recording server.

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.

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 5
- Create CA certificate on page 8
- Install certificates on the clients on page 9
- Create recording server certificate on page 16
- Import recording server certificate on page 18
- Enable encryption on page 25
- View encryption status on page 28

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 from the recording server is encrypted 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 recording servers using a CA certificate. This certificate contains two keys, a private key and public key. The public key is installed on the clients by installing a public certificate. The private key is used for signing recording server certificates that must be installed on the recording server. Whenever a client calls the recording server, the server sends the recording server certificate including the public key to the client. The client can validate the recording server certificate using the already installed public CA certificate. The client and the recording server can now use the public and private recording 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, encryption is enabled or disabled per recording server. When you enable encryption on a recording server, communication to all clients, servers, and integrations that retrieve data streams are encrypted. In this guide referred to as clients:

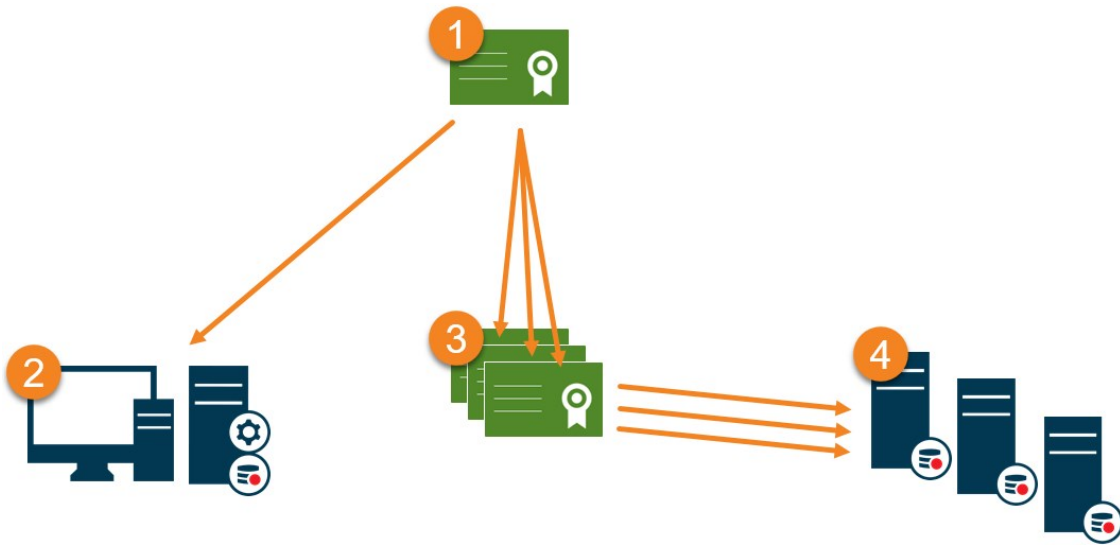
- XProtect Smart Client
- Management Client
- Management Server (for System Monitor and for images and AVI video clips in email notifications)
- Milestone Mobile Server
- XProtect Event Server
- XProtect LPR
- ONVIF Bridge
- XProtect DLNA Server
- Sites that retrieve data streams from the recording server 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 have to add HTTPS support themselves.

Certificate distribution

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



- 1 A CA certificate acts as a trusted third-party, trusted by both the Subject/owner (recording server) and by the party that verify the certificate (clients) (see Create CA certificate on page 8).
- 2 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 9
- 3 The CA certificate is used to issue private server authentication certificates to the recording servers (see Create recording server certificate on page 16).
- 4 The created private recording server certificates must be imported to the Windows Certificate Store on all recording servers (see Import recording server certificate on page 18).

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.



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. 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 recording server will automatically pick up the new certificate. This makes it easier to renew certificates for many recording servers without having to re-select the certificate for each recording server and without restarting the Recording Server service.

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.

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 Windows 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.



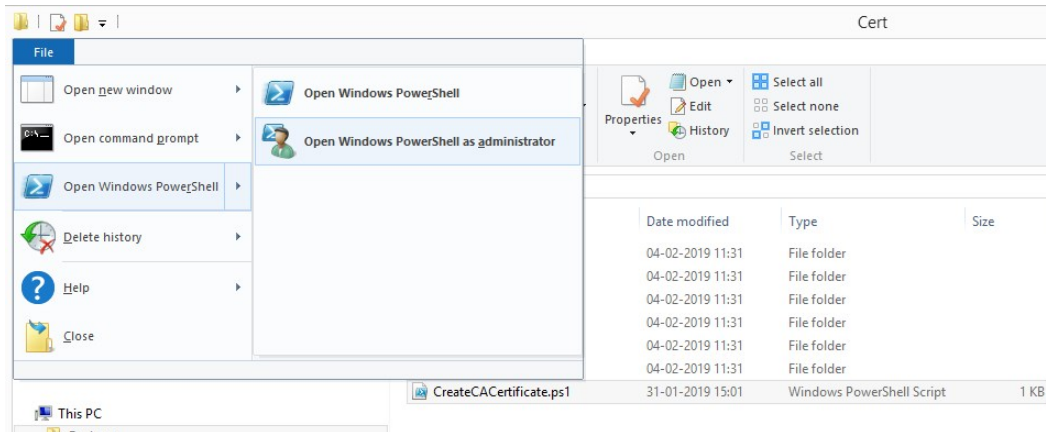
It is very important that the lines break in the same places as in Appendix A. You can add the line breaks in Notepad or alternatively, reopen this PDF with Google Chrome, copy the content again and paste it into Notepad.

```

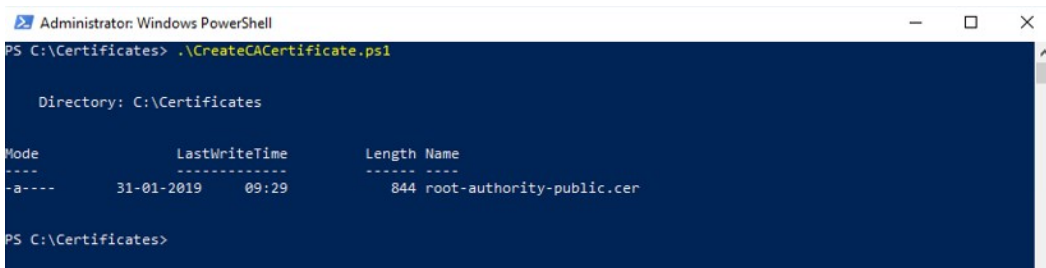
# Run this script once, to create a certificate that can sign multiple recording server certificates
# Private certificate for signing other certificates (in certificate store)
$ca_certificate = New-SelfSignedCertificate -CertStoreLocation cert:\CurrentUser\My -DnsName 'VMS Certificate Authority' -KeyUsageProperty All `
-KeyUsage CertSign, CRLSign, DigitalSignature -FriendlyName 'VMS CA Certificate'
# Thumbprint of private certificate used for signing other certificates
Set-Content -Path "$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"
    
```

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 the **CreateCACertificate.ps1** file.


- In the **File** menu, select **Open Windows Powershell** and then **Open Windows PowerShell as administrator**.



- In PowerShell at the prompt, type `.\CreateCACertificate.ps1` and press **Enter**.




- 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, type **Set-ExecutionPolicy RemoteSigned**. Press **Enter** and select **A**.

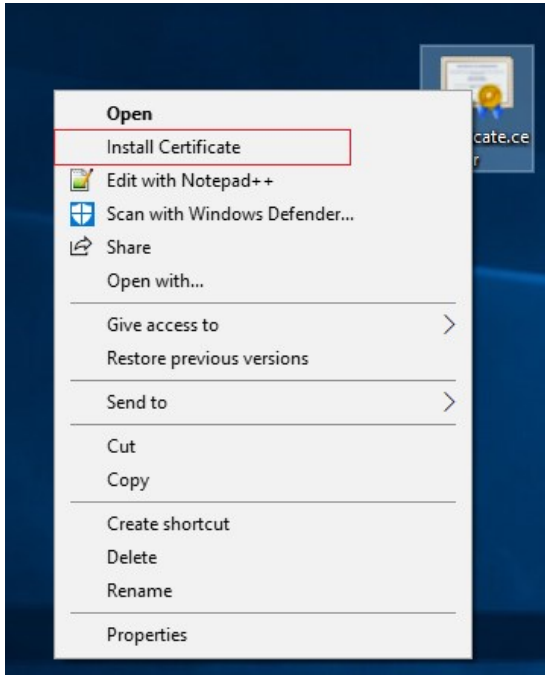
Install certificates on the clients

After you created the CA certificate, you must install and trust the certificate on all the computers that run clients or server services, and integrations that retrieve data streams from the recording server. In this section referred to as clients.

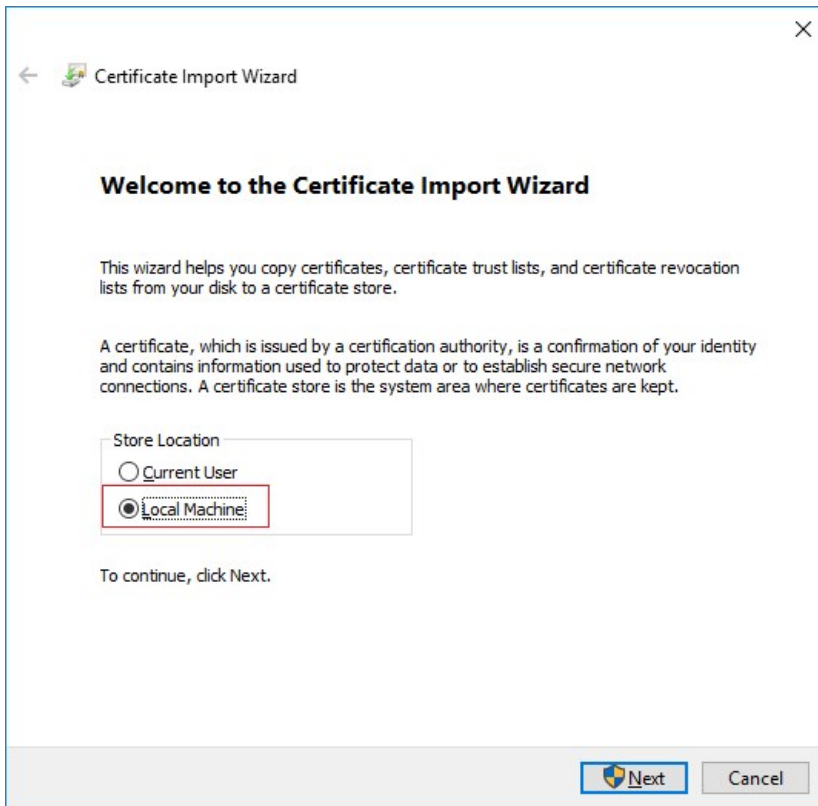
- Copy the `root-authority-public.cer` file from the computer where you created the CA certificate (`C:\Certificates\root-authority-public.cer`) to the computer where the client is installed.

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

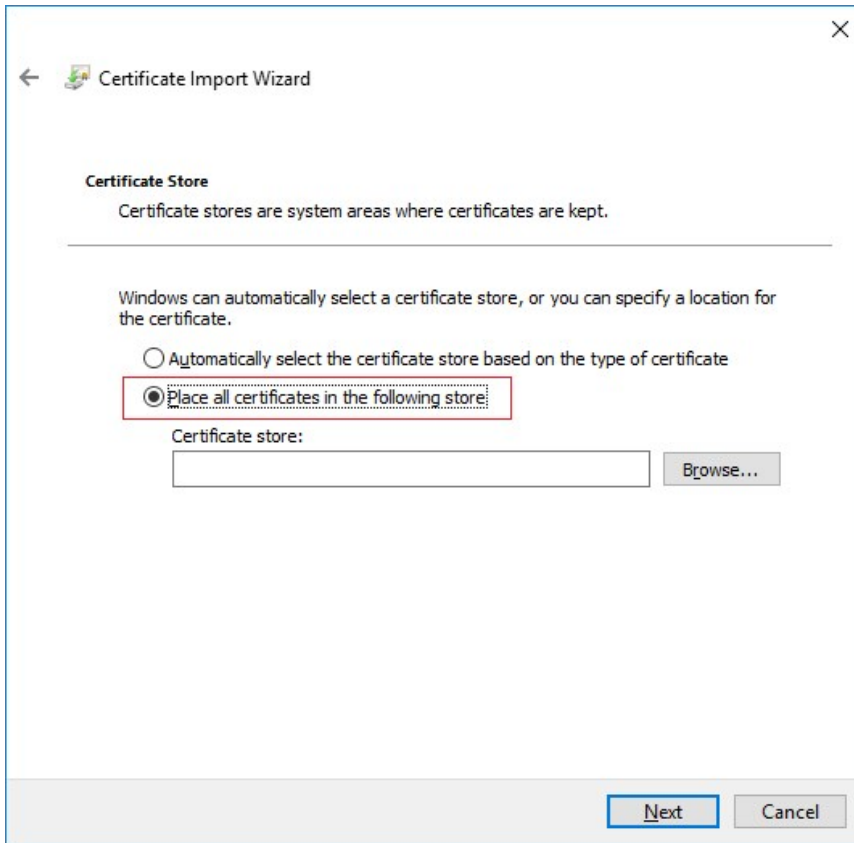
2. Right-click on the certificate and select **Install Certificate**.



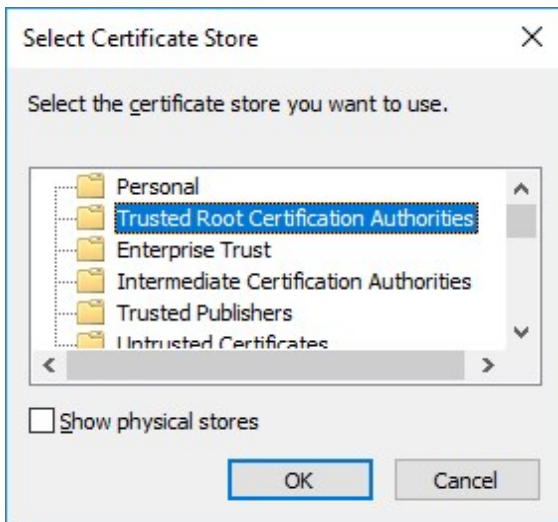
3. In the **Certificate Import Wizard**, select to install the certificate in the store of the **Local Machine** and click **Next**.




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

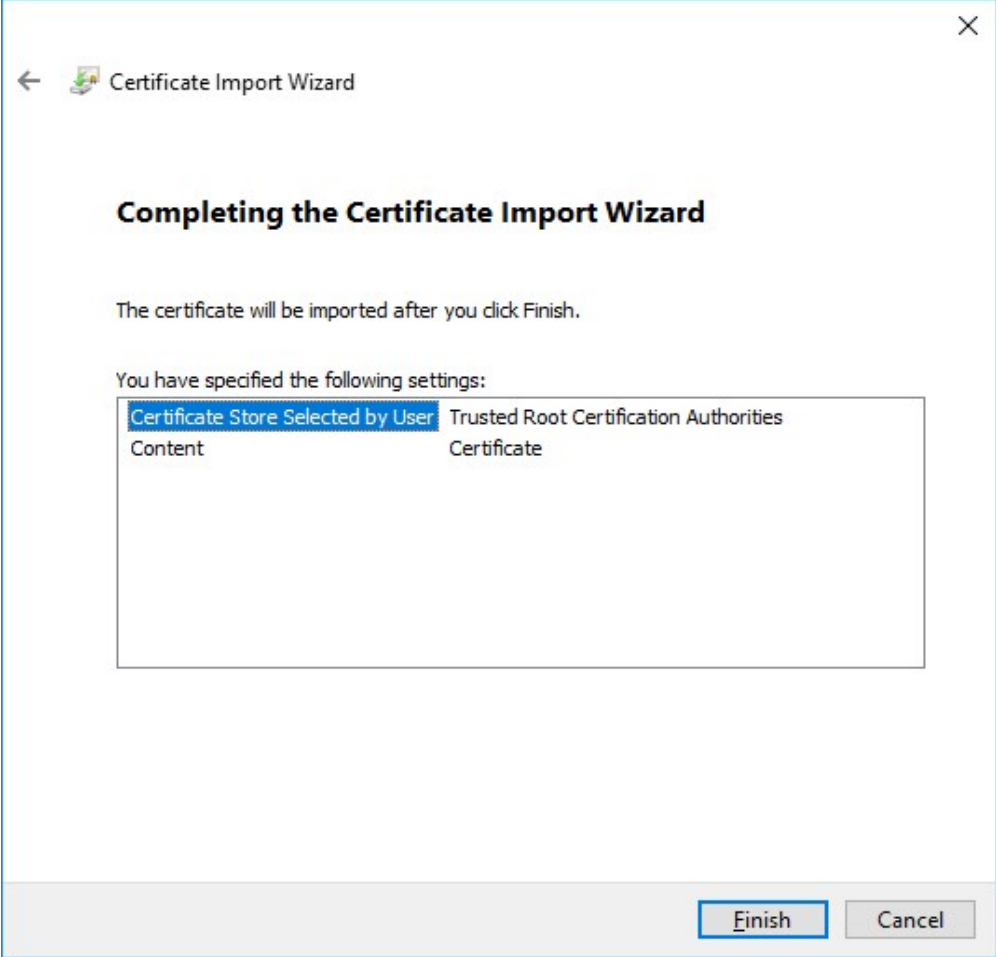


5. Click **Browse**, select **Trusted Root Certification Authorities** and click **OK**. Then click **Next**.

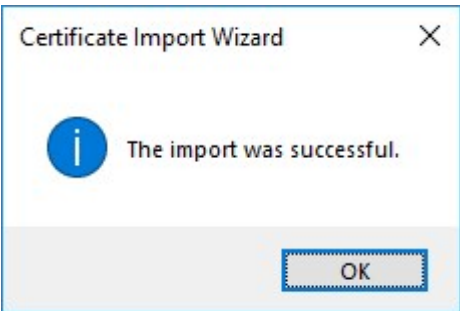


6. On the **Completing the Certificate Import Wizard** dialog, click **Finish**.

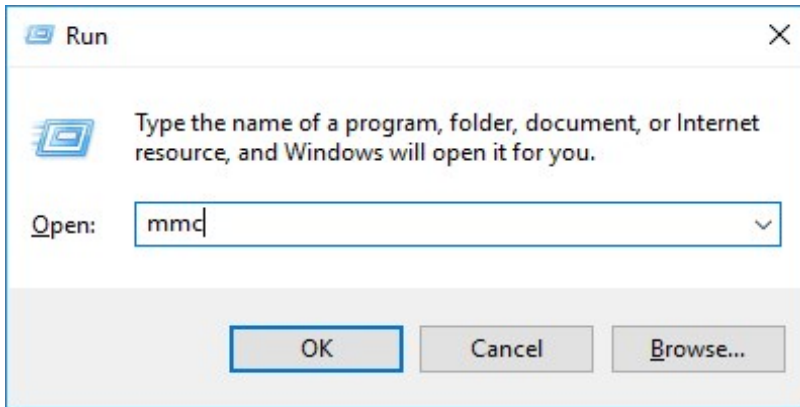
 If you receive a security warning that you are about to install a root certificate, click **Yes** to continue.



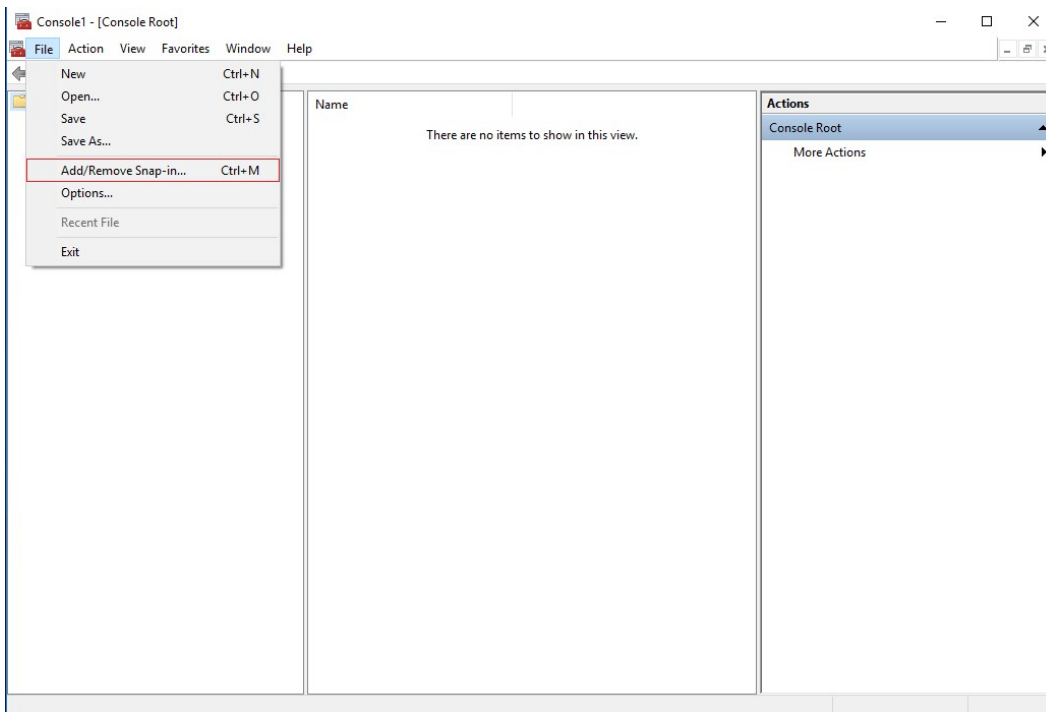
7. You will receive a confirmation dialog of successful import.



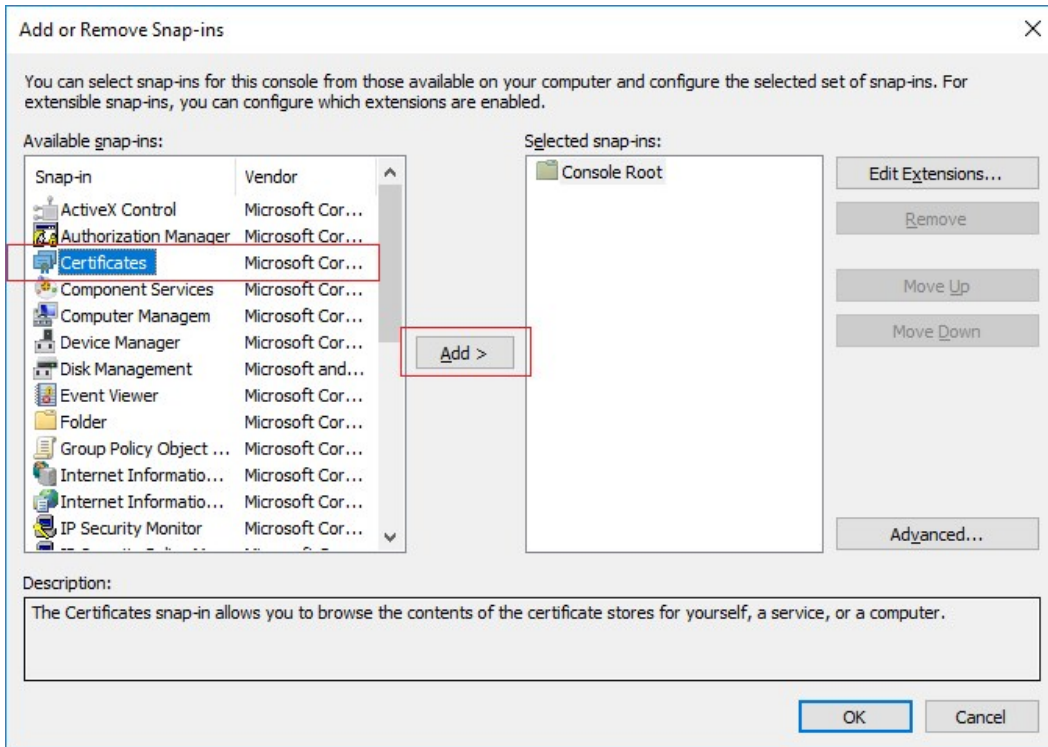
- To verify that the certificate is imported, start the Microsoft Management Console.



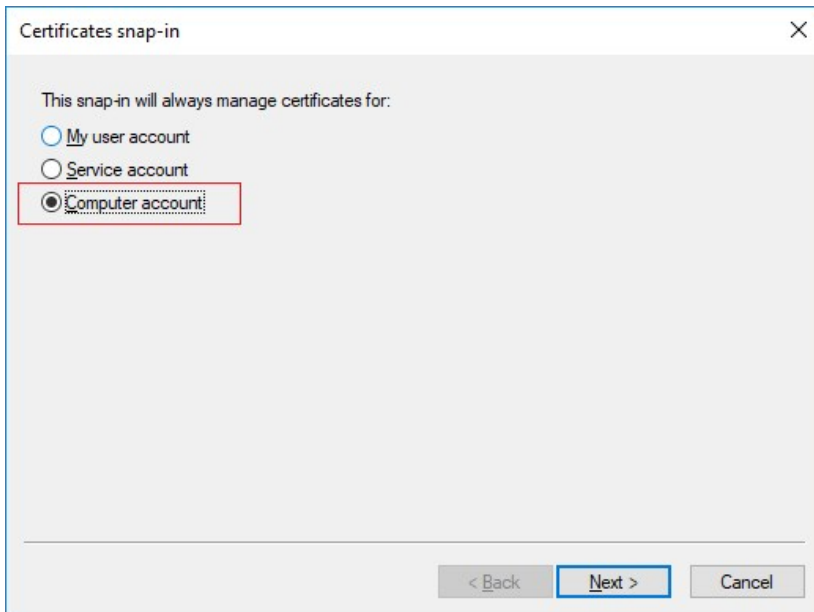
- In the Microsoft Management Console, from the **File** menu select **Add/Remove Snap-in...**



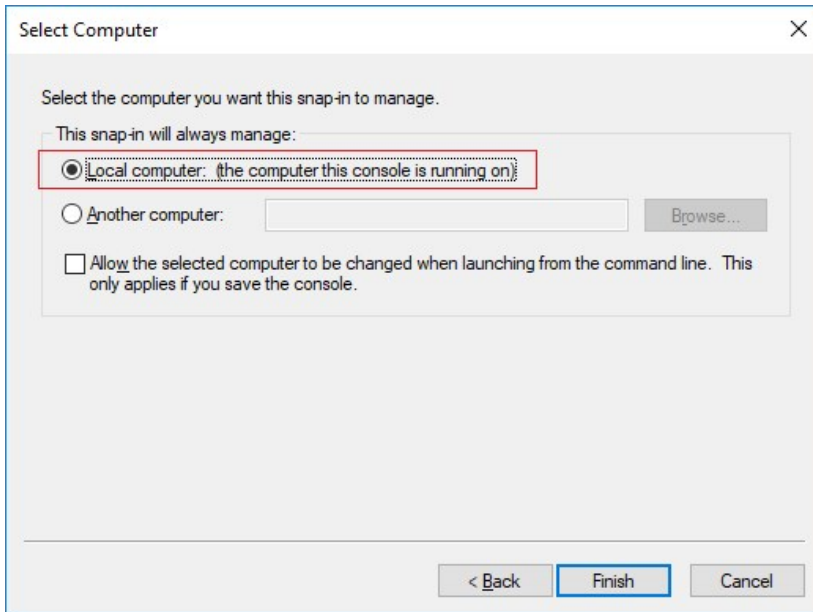
10. Select the **Certificates** snap-in and click **Add**.



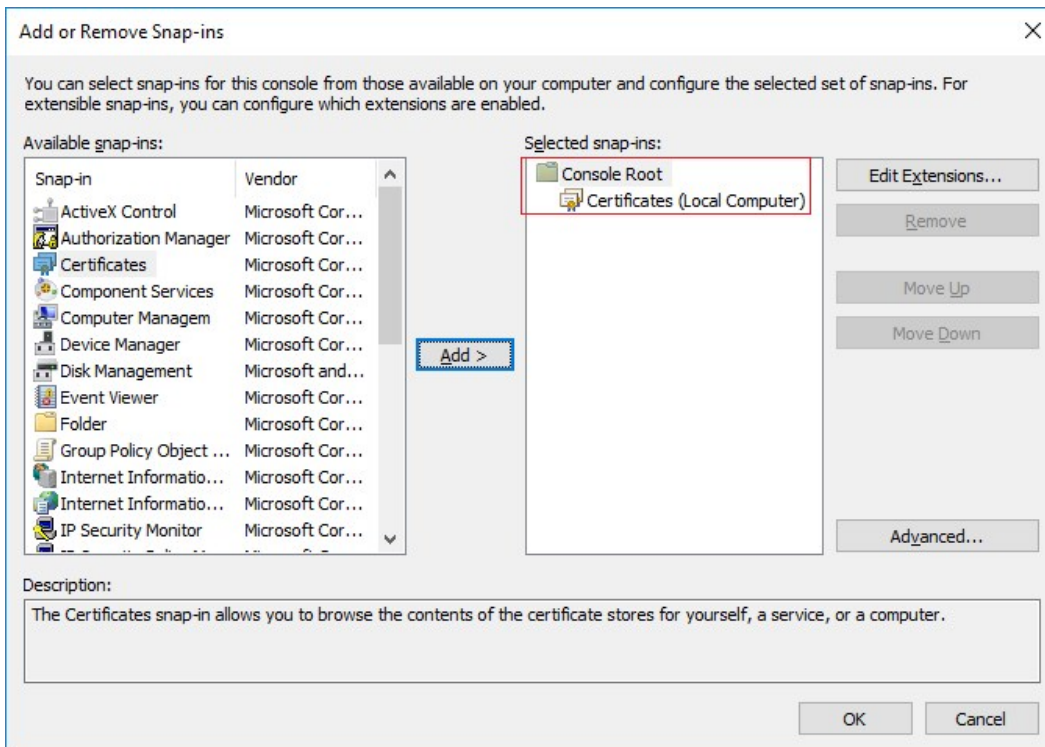
11. Select that the snap-in must manage certificates for the **Computer account**.



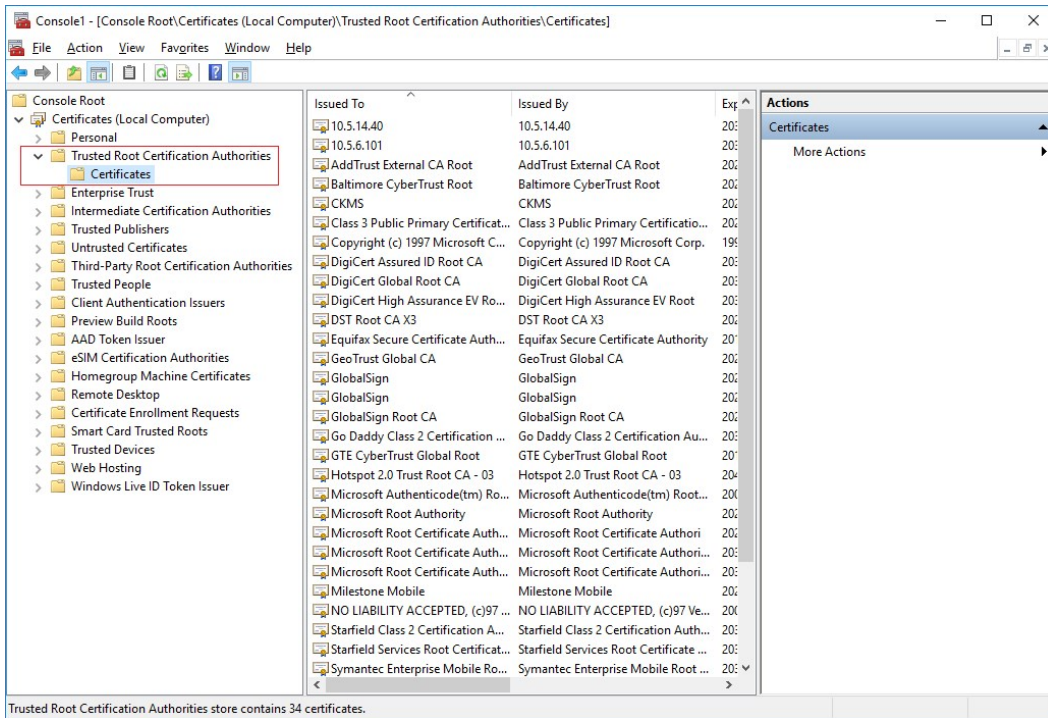
- 12. Select **Local computer** as the computer that you want the snap-in to manage and click **Finish**.



- 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 a client or server service, or an integration that retrieves data streams from the recording server, until you have installed the certificate on all relevant computers.

Create recording server 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 recording servers or failover recording servers.

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



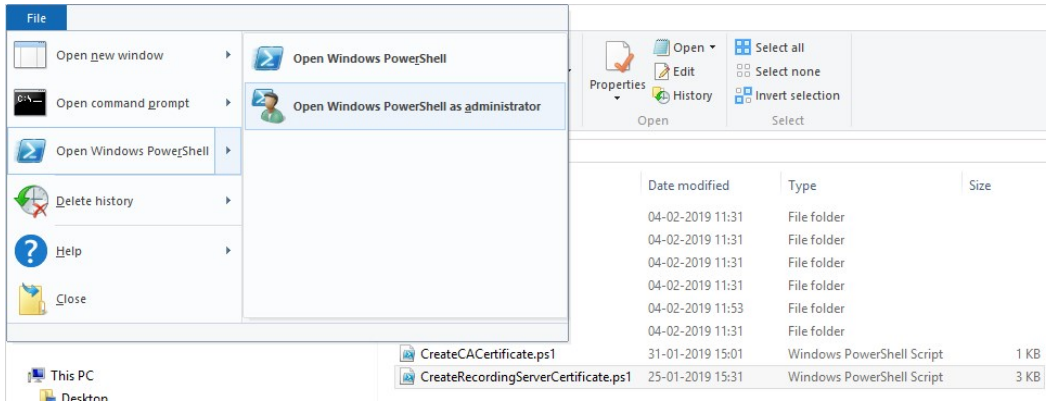
The computer that you use for creating certificates must run Windows 10 or Windows Server 2016 or newer.

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



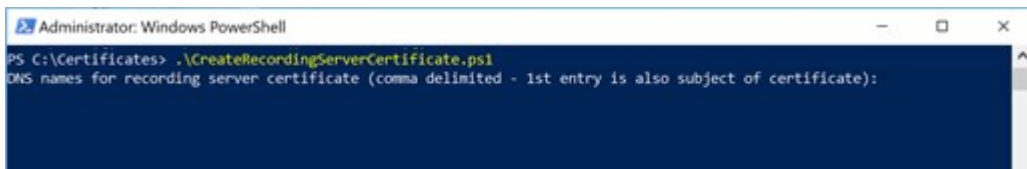
It is very important that the lines break in the same places as in Appendix B. You can add the line breaks in Notepad or alternatively, reopen this PDF with Google Chrome, copy the content again and paste it into Notepad.

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



- In PowerShell at the prompt, type **.\CreateRecordingServerCertificate.ps1** and press **Enter**.
- Enter the DNS name for the recording server. If the server has multiple names, for example for internal and external use, add them here, separated by commas. 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**.



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

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

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



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

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

11. Run the script until you have certificates for all your recording servers.

Import recording server certificate

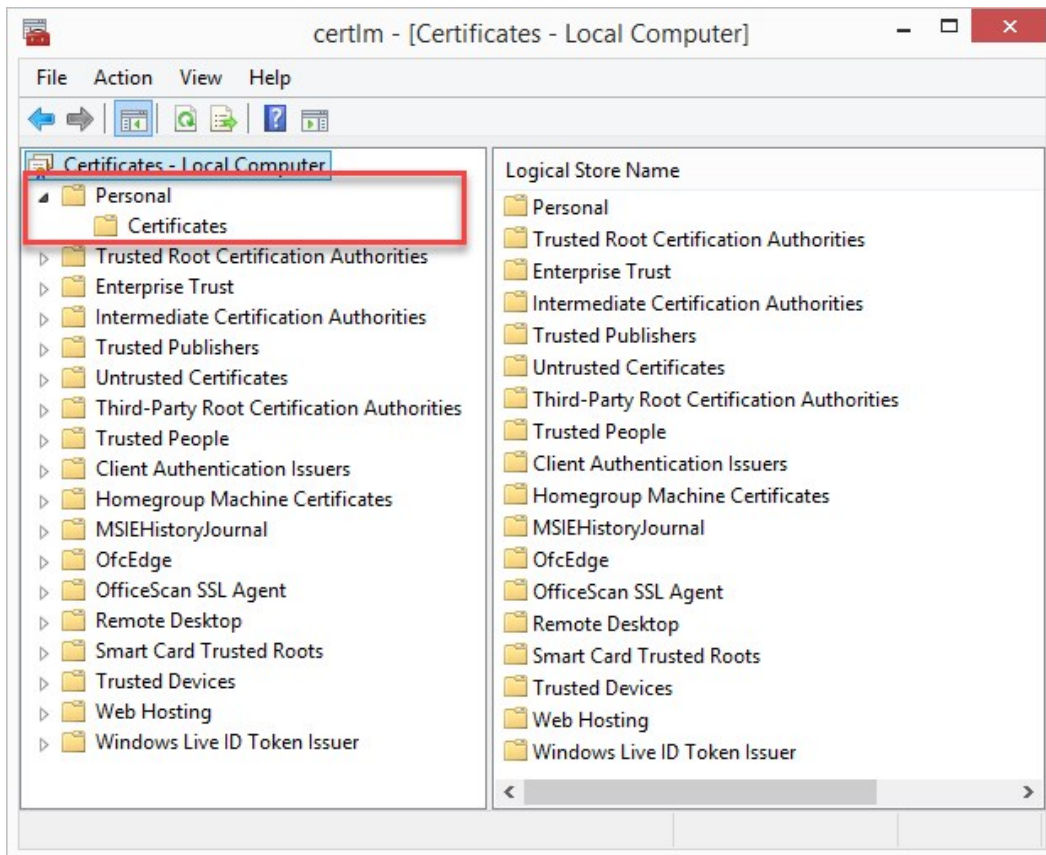
After you created the recording server certificates, install them on the computers that run the Recording Server service and the Failover Recording Server service.

1. Copy the relevant Subjectname.pfx file from the computer where you created the certificate to the corresponding recording server/failover recording server computer.

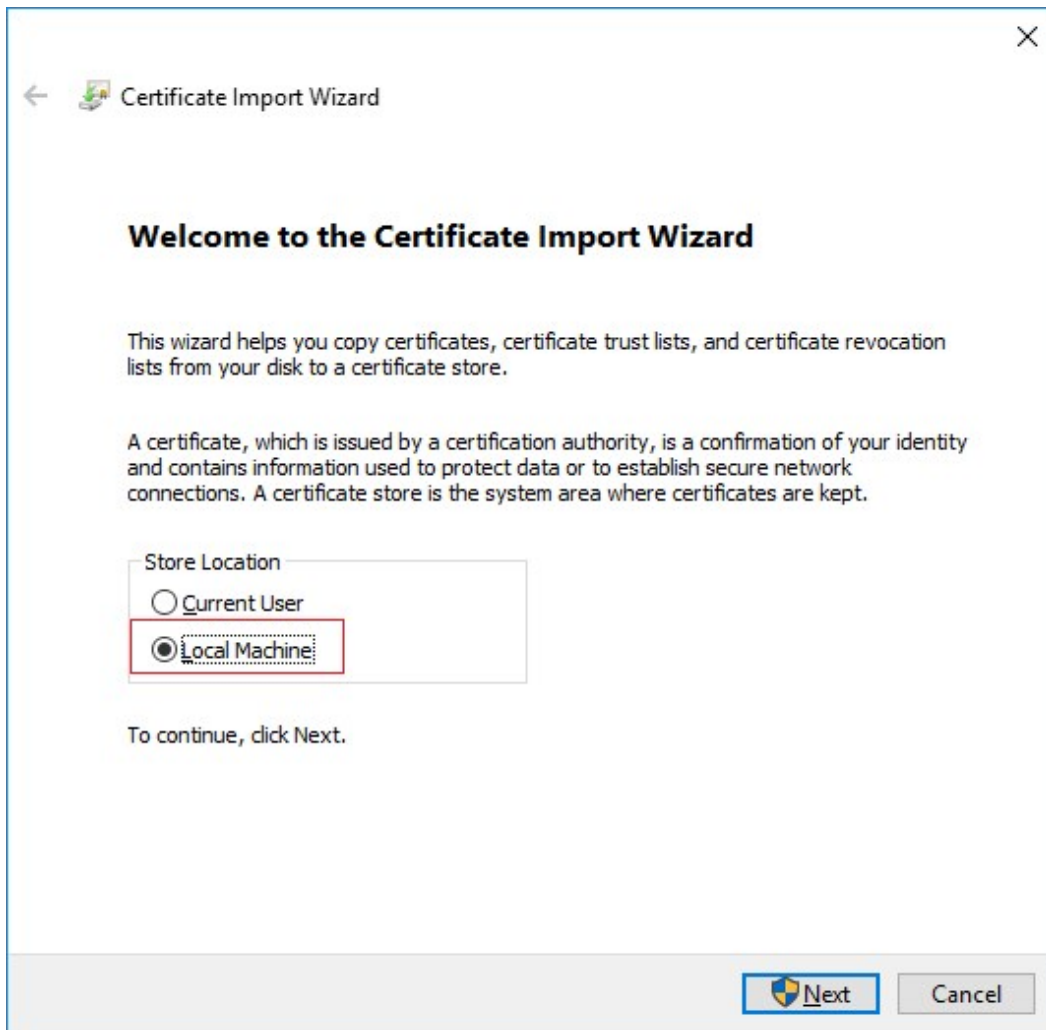


Remember that each certificate is created to a specific recording server/failover recording server.

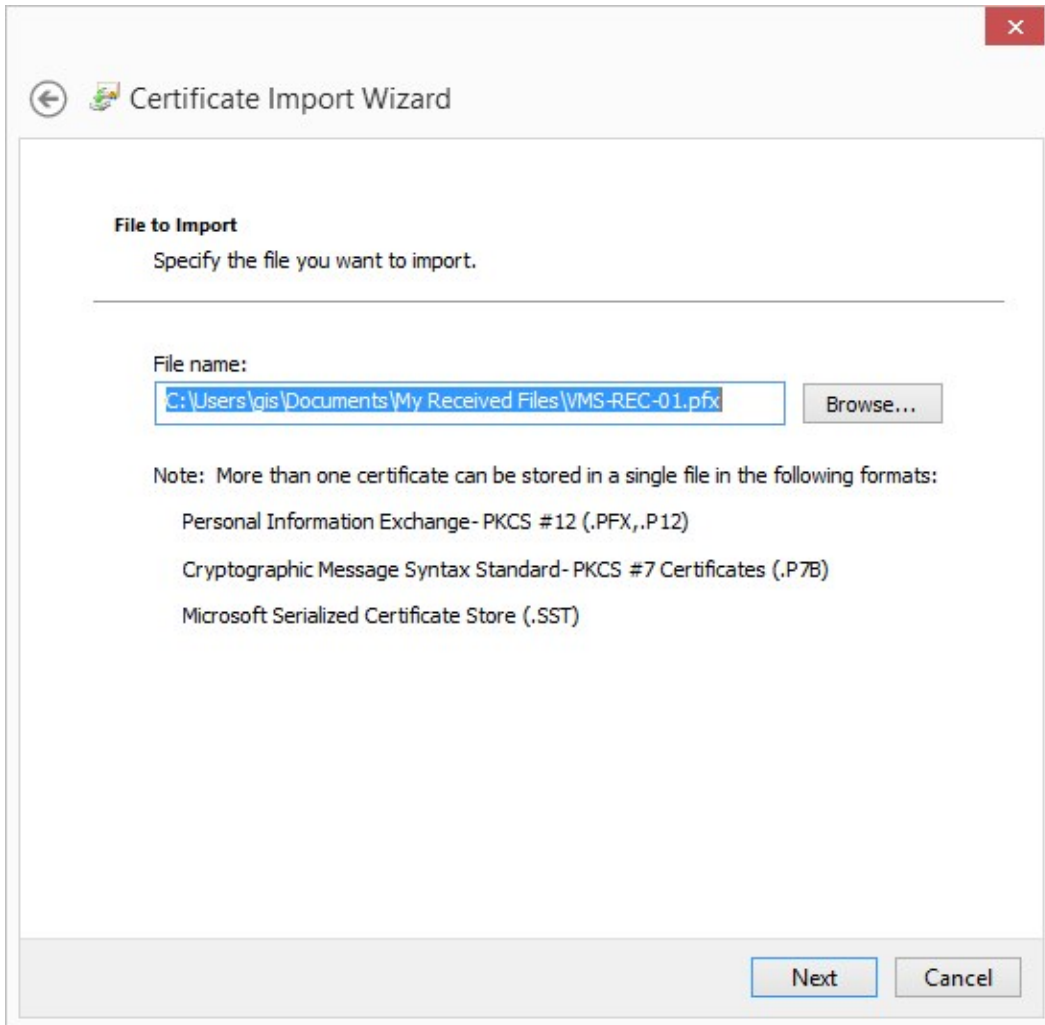
2. On the recording server/failover recording server computer, start **Manage computer certificates**.
3. Click on **Personal**, right-click **Certificates** and select **All Tasks > Import**.



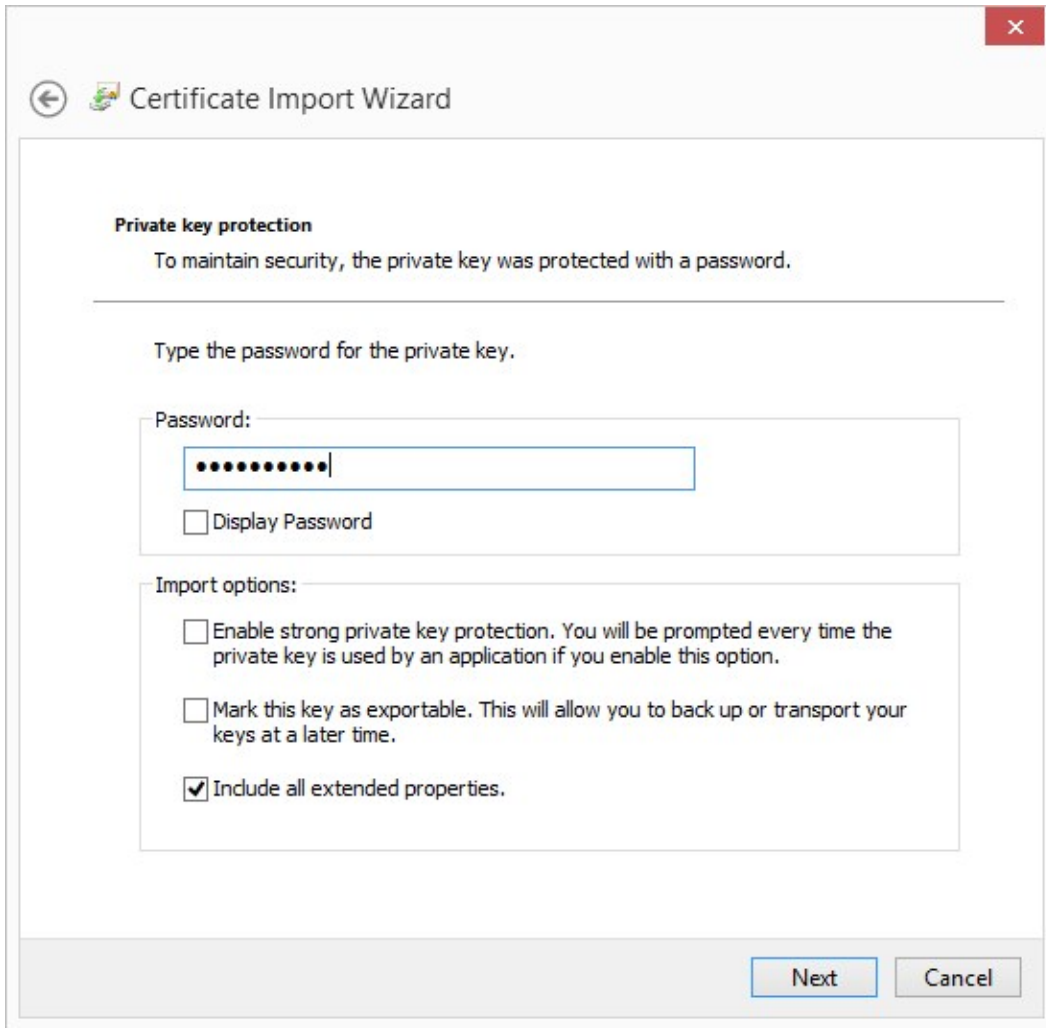
4. Select to import the certificate in the store of the **Local Machine** and click **Next**.



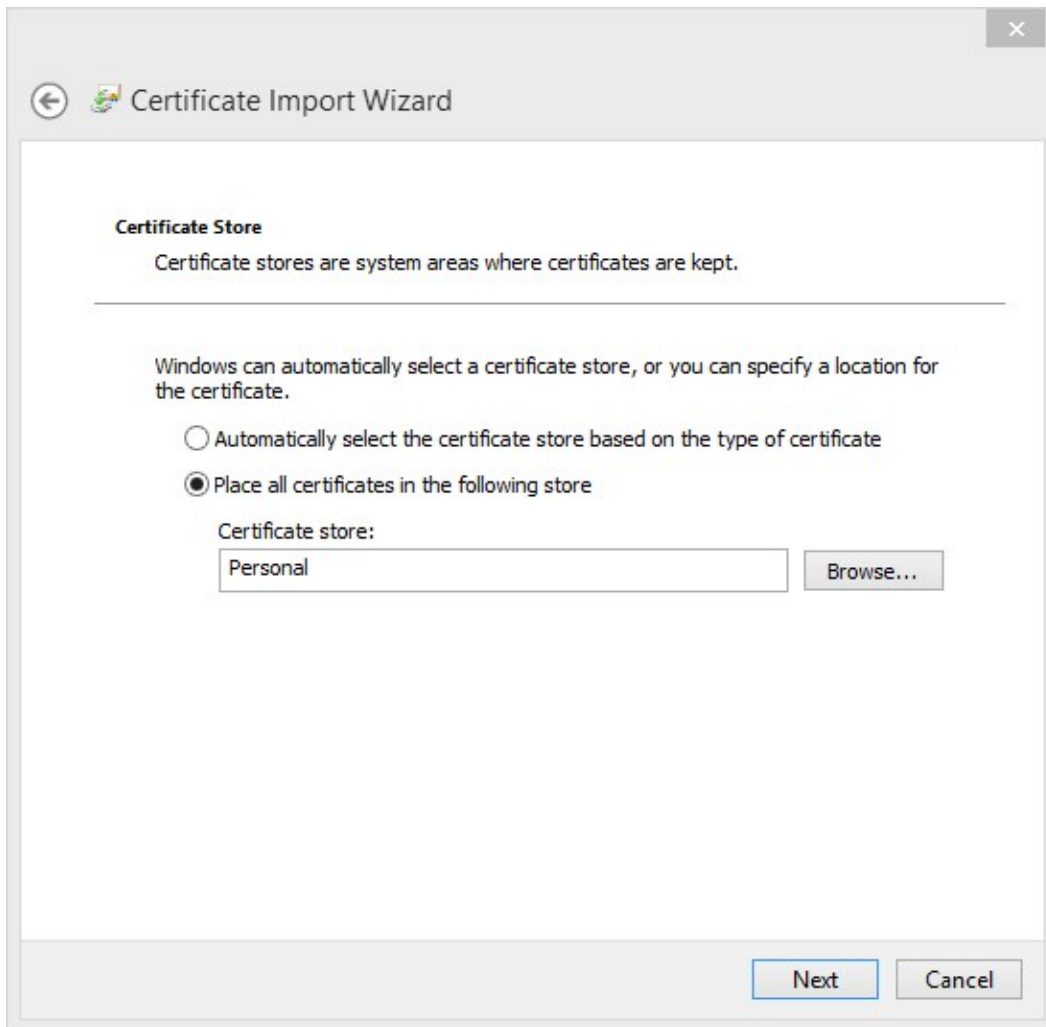
5. Browse to the certificate file and click **Next**.



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



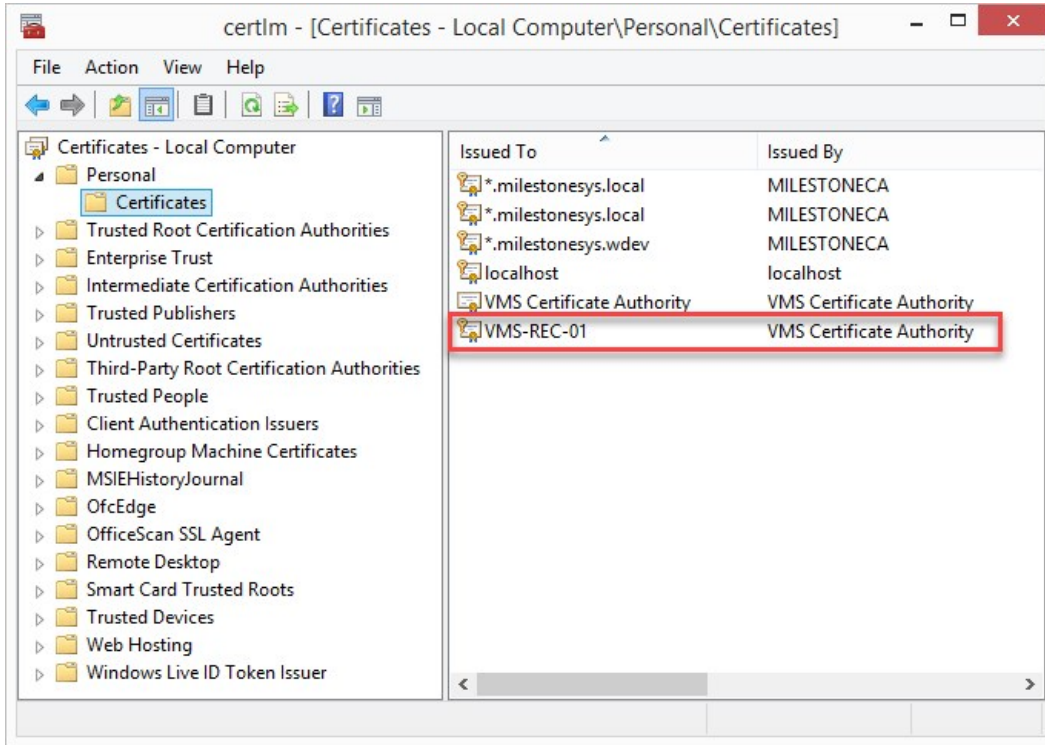
7. Place the file in the **Certificate Store: Personal** and click **Next**.



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



9. The imported certificate appears in the list.



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

Enable encryption

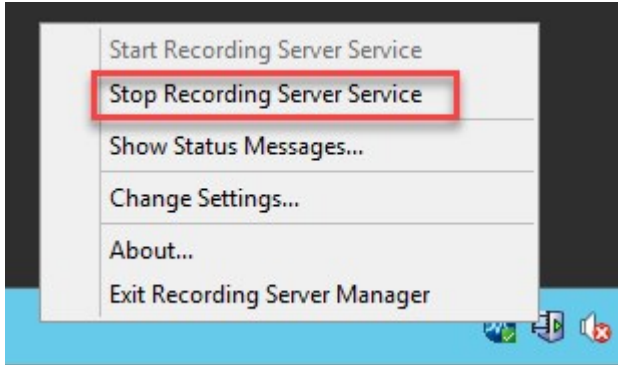
You are ready to apply encryption in your system either during installation of XProtect VMS or by enabling encryption via the Recording Server Manager icon in the tray controller on each recording server.



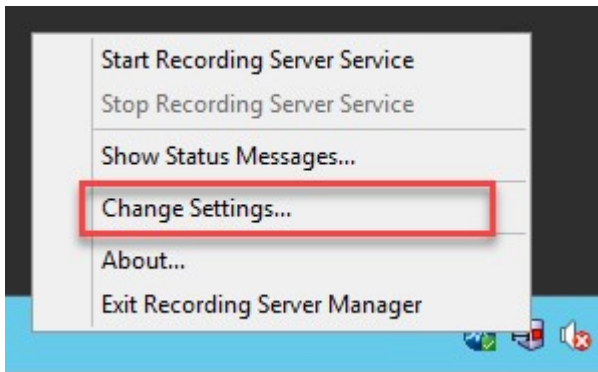
The computers that retrieve data streams from the recording server and where you installed the CA certificate do not require any enabling.

To enable encryption:

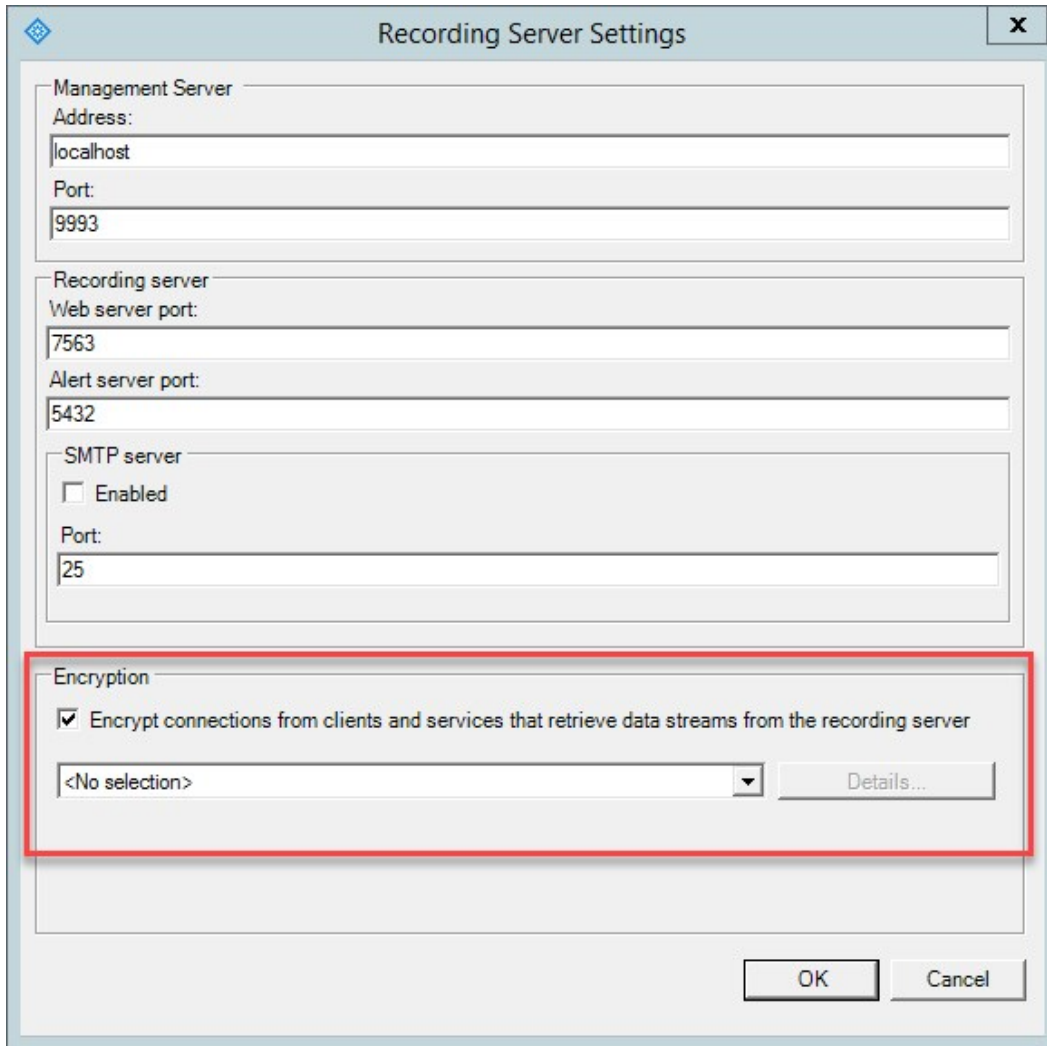
1. On the recording server, right-click the Recording Server Manager icon in the tray controller and stop the Recording Server service.



2. When the recording server is not running, right-click the Recording Server Manager icon and select **Change settings**.



3. Select the **Encrypt connections from clients and services that retrieve data streams from the recording server** check box.



4. In the drop-down list, select the certificate you created for this recording server and click **OK**.
5. Start the Recording Server service.
6. If your system contains multiple recording servers, continue the steps above until you have enabled encryption on all of them.

For information about installing XProtect VMS, see the Administrator manual (<https://www.milestonesys.com/support/help-yourself/manuals-and-guides/>).



If you enable encryption, and the selected certificate is not trusted on all computers running clients and services that retrieve data streams from the recording server, they are not able to communicate with the recording server.

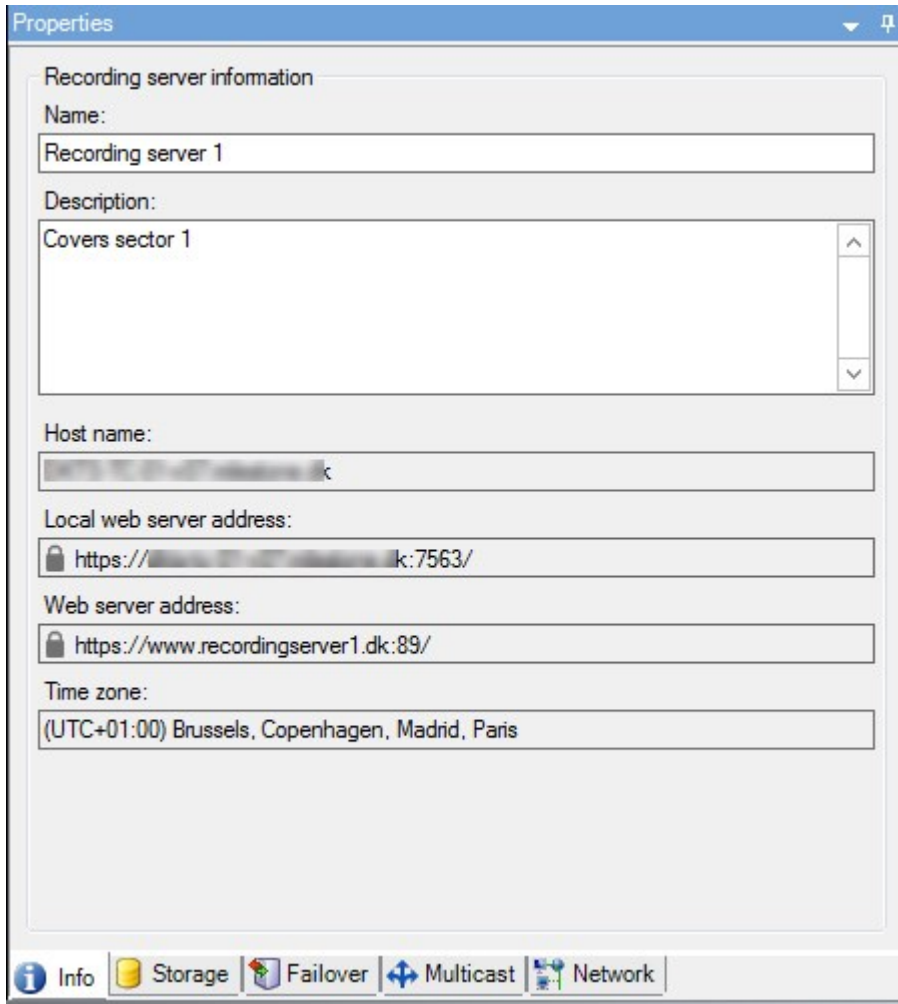


Enabling encryption requires that all clients, servers, and integrations that retrieve data streams from the recording server are upgraded to version 2019 R1 or later.

View encryption status

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, 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 recording server 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"
```

```

# Run this script once for each recording server for which a certificate is needed.
# Certificate should be executed on the single computer where the CA certificate is located.
# The created recording server certificate should then be moved to the recording server 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 recording 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
}
$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 recording server certificate (comma delimited)'
$ipAddressesArray = @($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 certificate is "Server Authentication"
$serverAuthentication = '2.5.29.37={critical}{text}1.3.6.1.5.5.7.3.1'

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

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

# Delete the recording server 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/>.

