MAKE THE WORLD SEE

Milestone Systems

XProtect® VMS 2022 R1

Certificates guide



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	73
Install certificates in a domain for communication with the Management Server or Recording Server &	85
Install certificates in a Workgroup environment for communication with the Management Server	
or Recording Server10	
Install certificates for communication with the Event Server	
Import client certificates 12	28
View encryption status to clients	34
View encryption status on a failover recording server13	35
Appendix A Create CA Certificate script	36
Appendix B Create Server SSL Certificate script	37
Appendix C Create Failover Management Server Certificate script	38

Copyright, trademarks, and disclaimer

Copyright © 2022 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

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.

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

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

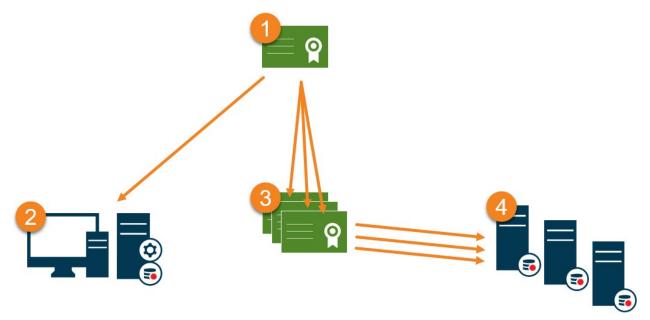
- XProtect DLNA Server
- Sites that retrieve data streams from the recording server through Milestone Interconnect
- Third-party MIP SDK integrations that support HTTPS

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.



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

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).

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

• 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 85

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 103

• 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 125

• 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 128

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.

Third Party CA/ Domain	Self Signed CA / Domain
Third Party CA/ Non-Domain	Self Signed CA/ Non-Domain

) No Public Key Distribution Needed

Public Key Distribution Needed

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 128.

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

Milestone Server Configurator		<u> </u>	
Encryption	Encryption		
Registering servers	It is recommended to secure communication with encryption	n. <u>Learn m</u>	ore
Language selection	Server certificate Applies to: management server, recording server, failover server, data collector		
	Encryption: On		
	DocCert1	~	Details
	Certificate issued by mjt-MJT-DC-CA, DC=mjt, DC=local. Expires 4/27/2022		
	Mobile streaming media certificate Applies to mobile and web clients that retrieve data streams from the server Encryption: On	mobile	
	DocCert1	~	Details
	Certificate issued by mjt-MJT-DC-CA, DC=mjt, DC=local. Expires 4/27/2022		Apply

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 thirdparty 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.



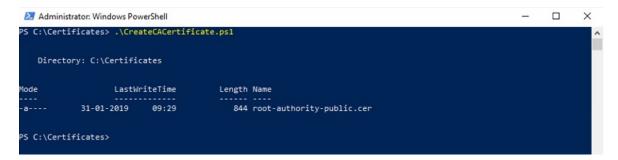
It is very important that the lines break in the same places as in Appendix A. You can add the line breaks in Notepad or alternatively, reopen this PDF with Google Chrome, copy the content again and paste it into Notepad.

	CreateCACertificate.ps1 - Notepad	
File Edit Format View Help		
<pre># Private certificate for signin \$ca_certificate = New-SelfSigned KeyUsage CertSign, CRLSign, Dig # Thumbprint of private certific Set-Content -Path "\$PSScriptRoot # Public CA certificate to trust</pre>	e a certificate that can sign multiple recording server certificates g other certificates (in certificate store) Certificate -CertStoreLocation cert:\CurrentUser\My -DnsName 'VMS Certificate Auth italSignature -FriendlyName 'VMS CA Certificate' ate used for signing other certificates \ca_thumbprint.txt" -Value \$ca_certificate.Thumbprint (Third-Party Root Certification Authorities) CurrentUser\My\\$(\$ca_certificate.Thumbprint)" -FilePath "\$PSScriptRoot\root-author	
		8, Col 130

- 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.

Open <u>n</u> ew window	Þ	Dpen Window	s Powe <u>r</u> Shell	☐ Open ▼ ☐ Edit	Select all		
Open command <u>p</u> rompt	Þ	Open Window	s PowerShell as <u>a</u> dministrator	Properties History Open	Select		
Open Windows Powe <u>r</u> S	hell 🕨						
Delete history	Þ			Date modified 04-02-2019 11:31	Type File folder	Size	
3				04-02-2019 11:31	File folder		
Help				04-02-2019 11:31	File folder		
V				04-02-2019 11:31	File folder		
Close				04-02-2019 11:31	File folder		
				04-02-2019 11:31	File folder		
			CreateCACertificate.ps1	31-01-2019 15:01	Windows PowerShell Scri	ipt	1 k

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 128 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**.

	Open		
	Install Certificate		
7	Edit with Notepad++		
•	Scan with Windows Defender		
2	Share		
	Open with		
	Give access to	2	>
	Restore previous versions		
	Send to	1	>
	Cut		_
	Сору		
	Create shortcut		
	Delete		
	Rename		

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

÷	🖉 Certificate Import Wizard	×
	Welcome to the Certificate Import Wizard	
	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
	Store Location	
	To continue, dick Next.	
	<u>∳N</u> ext Cancel	

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

Certificate Store		
Certificate stor	es are system areas where certificat	es are kept.
the certificate.	utomatically select a certificate store	
Place all	certificates in the following store	
Certifica	te store:	
		Browse

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.

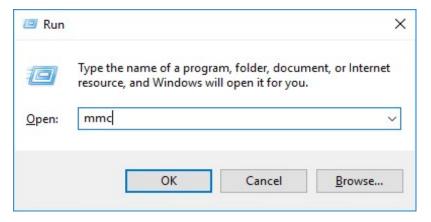
If you receive a security warning that you are about to install a root certificate, click **Yes** to continue.

-	Certificate Import Wizard)
	Completing the Certificate Import Wizard	
	The certificate will be imported after you click Finish.	
	You have specified the following settings:	
	Certificate Store Selected by User Trusted Root Certification Authorities Content Certificate	
	<u> </u>	ancel

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....

	onsole1 - [Console Root]							– 🗆 ×
Fil	e Action View Favorite New Open	s Window	Help					_ & ×
-	New	Ctrl+N						
	Open	Ctrl+0	Name				Actions	
	Save Save As	Ctrl+S		There are no ite	ms to show in this view.		Console Root	
							More Actions	•
	Add/Remove Snap-in	Ctrl+M						
	Options							
	Recent File							
	Exit							
_			·					

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

ilable <u>s</u> nap-ins:			Selected snap-ins:	Edit Extensions
ap-in	Vendor		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor			Remove
Authorization Manager		-		
Certificates	Microsoft Cor			E
Component Services	Microsoft Cor			Move Up
Computer Managem	Microsoft Cor			Move Down
Device Manager	Microsoft Cor		Add >	Hove Down
Disk Management	Microsoft and	Ļ		
Event Viewer	Microsoft Cor			
Folder	Microsoft Cor			
Group Policy Object				
Internet Informatio	Microsoft Cor			
Internet Informatio	Microsoft Cor			
IP Security Monitor	Microsoft Cor	~		Advanced
cription:				

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

Certificates snap-in			×
This snap-in will always manage certificates for: My user account Service account © <u>Computer account</u>			
·	< <u>B</u> ack	<u>N</u> ext >	Cancel

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

Local computer: (th)	e computer this console is running on)	
Another computer:		Browse

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

ActiveX Control ActiveX Control Authorization Manager Certificates Component Services Computer Managem Device Manager Disk Management Event Viewer Folder Group Policy Object Internet Informatio Internet Informatio	Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft and Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor		Add >	Certificates (Local Comput	Remove Move Up Move Down
IP Security Monitor	Microsoft Cor	~			Advanced

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

File Action View Favorites Window He	lp				-	
🔿 🖄 📰 🗋 🗟 🕞 🖉 🗊						
Console Root	Issued To	Issued By	Exp ^	Actions		
Certificates (Local Computer)	[10.5.14.40	10.5.14.40	20:	Certificates		
	Ito.5.6.101 Ido.5.6.101 Ido.5.101 Ido.5.6.101 Ido.5.101 Ido.5.101	10.5.6.101 AddTrust External CA Root Baltimore CyberTrust Root CKMS Class 3 Public Primary Certificatio Copyright (c) 1997 Microsoft Corp. DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert High Assurance EV Root DST Root CA X3 Equifax Secure Certificate Authority GeoTrust Global CA GlobalSign GlobalSign GlobalSign Root CA Go Daddy Class 2 Certification Au	20: 202 202 202 202 202 202 203 203 204 204 204 204 204 204 204 204 204 204	More Actions		
 Trusted Devices Web Hosting Windows Live ID Token Issuer 	G Daddy Class 2 Certification G TE CyberTrust Global Root Hotspot 2.0 Trust Root CA - 03 Microsoft Authenticode(tm) Ro Microsoft Root Authority Microsoft Root Certificate Auth Microsoft Root Certificate Auth Starfield Class 2 Certification A Starfield Class 2 Certification A Starfield Services Root Certificat Symantec Enterprise Mobile Ro C	GTE CyberTrust Global Root Hotspot 2.0 Trust Root CA - 03 Microsoft Authenticode(tm) Root Microsoft Root Authority Microsoft Root Certificate Authori Microsoft Root Certificate Authori NO LIABILITY ACCEPTED, (c)97 Ve Starfield Class 2 Certification Auth Starfield Services Root Certificate	20° 204 200 202 202 202 203 203 203			

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.



Ì

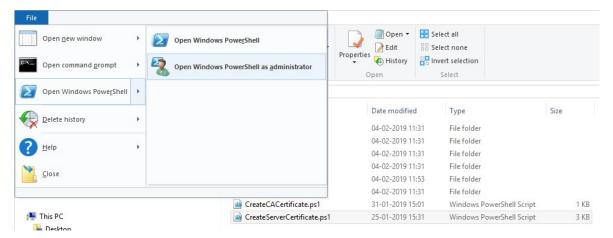
The computer that you use for creating certificates must run Window 10 or Windows Server 2016 or newer.

- 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.



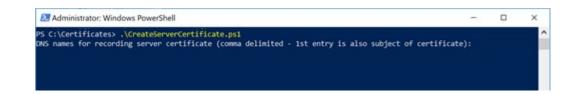
It is very important that the lines break in the same places as in Appendix B. You can add the line breaks in Notepad or alternatively, reopen this PDF with Google Chrome, copy the contents again and paste it into Notepad.

- 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

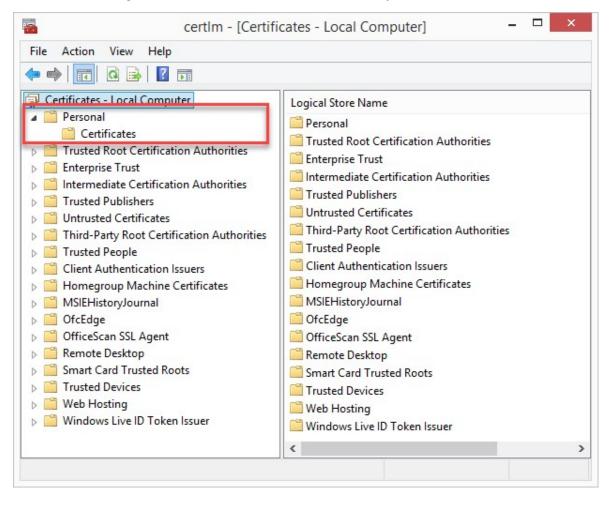
After you created the SSL certificates, install them on the computers that run the server service.

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.

Welcome to the	Certificate Import	t Wizard
This wizard helps you cop lists from your disk to a ce		st lists, and certificate revocation
and contains information connections. A certificate	ed by a certification authori used to protect data or to ex store is the system area wh	
Store Location		
To continue, dick Next.		
To continue, click Next.		

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

File to Import				
Specify the file	e you want to import.			
File name:				
	Documents\My Receive	ed Files\VMS-REC-01.	Browse.	
Note: More th	an one certificate can l	pe stored in a single f	ile in the following form	ater
	formation Exchange- P			urus.
Cryptograp	hic Message Syntax St	andard- PKCS #7 Cer	tificates (.P7B)	
Microsoft S	erialized Certificate Sto	re (.SST)		

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

F	Private key protection
	To maintain security, the private key was protected with a password.
	Type the password for the private key.
	Type the password for the private key.
	Password:
	••••••
	Display Password
	Import options:
	Enable strong private key protection. You will be prompted every time the
	private key is used by an application if you enable this option.
	Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
	✓ Include all extended properties.

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

Certificat				
Certi	ficate stores are system	areas where certificate	es are kept.	
Wind	ows can automatically s	elect a certificate store,	, or you can specif	y a location for
the c	ertificate.			1
C	Automatically select th	e certificate store base	d on the type of c	ertificate
0	Place all certificates in	the following store		
	Certificate store:			
	Personal			Browse

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

The ce	rtificate will be imported after	you click Finish.
You ha	ve specified the following set	tings:
Certi Conte File N		Personal PFX C: \Users \gis \Desktop \VMS-REC-01.pfx

9. The imported certificate appears in the list.

certlm - [Certificates	- Local Computer\Personal\(Certificates] – 🗆 🚬
File Action View Help		
🗢 🔿 🚈 📊 📋 🙆 📑 🛛 🖬		
 Certificates - Local Computer Personal Certificates Certificates Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Third-Party Root Certification Authorities Trusted People Client Authentication Issuers Homegroup Machine Certificates MSIEHistoryJournal OfcEdge OfficeScan SSL Agent Smart Card Trusted Roots 	Issued To	Issued By Iocalhost VMS Certificate Authority VMS Certificate Authority

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

Open	
All Tasks	Open
Cut Copy	Request Certificate with New Key Renew Certificate with New Key
Delete	Manage Private Keys
Properties	Advanced Operations
Help	Export

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

group or user names:		
SYSTEM		
Administrators (Administrat	tors)	
NETWORK SERVICE		
	Add	Remove
Permissions for NETWORK	Allow	Deny
Full control		
Read	\checkmark	
Special permissions		
or special permissions or adva	nced settings	
lick Advanced.	liood sotaligs,	Advanced

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 active 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.

 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:\Certificate\CreateFailoverCertificate.ps1

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.

Open <u>n</u> ew window	۲	Open Wind	lows Powe <u>r</u> Shell		🗐 Open 👻 📝 Edit	Selec			
Open command prom	pt ▶	Open Wind	dows PowerShell as <u>a</u> dministrator	Properties	History		t selection lect		
Open Windows Powe	<u>r</u> Shell								
Delete history		1			Date modified	Ы	Туре	Size	
					04-02-2019 11	1:31	File folder		
2 Help					04-02-2019 11	:31	File folder		
					04-02-2019 11	1:31	File folder		
×					04-02-2019 11	:31	File folder		
Close					04-02-2019 11	1:53	File folder		
					04-02-2019 11	1:31	File folder		
			CreateCACertificate.ps1		31-01-2019 15	5:01	Windows PowerShell Script		1 K
📜 This PC			CreateServerCertificate.p	s1	25-01-2019 15	5:31	Windows PowerShell Script		3 K

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.

You are now ready to install the certificate on the primary and the secondary computer.

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.

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.

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

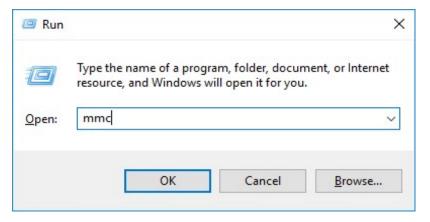
Add the CA certificate to the Mobile Server by doing the following.



Ì

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....

	onsole1 - [Console Root] Action View Favorite	s Window	Help					×
4	e Action View Favorite New Open	Ctrl+N	1100					
	Open	Ctrl+O				Actio	10	
	Save	Ctrl+S	Name				ole Root	•
	Save As			There are no ite	ms to show in this view.		More Actions	-
	Add/Remove Snap-in	Ctrl+M					viore Actions	
	Options							
	Recent File							
	Exit							

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

Click OK.

ActiveX Control Microsoft Cor ActiveX Control Microsoft Cor Authorization Manager Microsoft Cor Certificate Templates Microsoft Cor Certificates Microsoft Cor Certificates Microsoft Cor Certificates Microsoft Cor Certificates Microsoft Cor Certification Authority Microsoft Cor Component Services Microsoft Cor Computer Managem Microsoft Cor	Certificates - Current User Remove Move Up Move Down	ActiveX Control Microsoft Cor Authorization Manager Microsoft Cor Authorization Manager Microsoft Cor Certificates Microsoft Cor Certificates Microsoft Cor Certificates Microsoft Cor Certificates Microsoft Cor Component Services Microsoft Cor Computer Managem Microsoft Cor Device Manager Microsoft Cor Disk Management Microsoft Cor Enterprise PKI Microsoft Cor	Remove Move Up
ActiveX Control Microsoft Cor ActiveX Control Microsoft Cor Certificates Microsoft Cor Certification Authority Microsoft Cor Certification Authority Microsoft Cor Certification Authority Microsoft Cor Component Services Microsoft Cor	Move Up Move Down	ActiveX control Microsoft Coll Removing Authorization Manager Microsoft Coll Microsoft Coll Certificate Templates Microsoft Coll Move I Certificates Microsoft Coll Move I Certificates Microsoft Coll Move I Certification Authority Microsoft Coll Move I Component Services Microsoft Coll Move I Computer Managem Microsoft Coll Move I Device Manager Microsoft Coll Move I Disk Management Microsoft Coll Microsoft Coll Enterprise PKI Microsoft Coll Microsoft Coll	Move Up
Certificate Templates Microsoft Cor Certificates Microsoft Cor Certification Authority Microsoft Cor Component Services Microsoft Cor	Move Down	Certificate Templates Microsoft Cor Certificates Microsoft Cor Certification Authority Microsoft Cor Component Services Microsoft Cor Computer Managem Microsoft Cor Device Manager Microsoft Cor Disk Management Microsoft Cor Enterprise PKI Microsoft Cor	
Certificates Microsoft Cor Certification Authority Microsoft Cor Component Services Microsoft Cor	Move Down	Certificates Microsoft Cor Certification Authority Microsoft Cor Component Services Microsoft Cor Computer Managem Microsoft Cor Device Manager Microsoft Cor Disk Management Microsoft Cor Enterprise PKI Microsoft Cor	
Certification Authority Microsoft Cor Component Services Microsoft Cor Add >	Move Down	Certification Authority Microsoft Cor Component Services Microsoft Cor Computer Managem Microsoft Cor Device Manager Microsoft Cor Disk Management Microsoft Cor Enterprise PKI Microsoft Cor	
Component Services Microsoft Cor Add >		Component Services Microsoft Cor Computer Managem Microsoft Cor Device Manager Microsoft Cor Disk Management Microsoft Cor Enterprise PKI Microsoft Cor	Move Down
Add >		Component Services Microsoft Cor Computer Managem Microsoft Cor Device Manager Microsoft Cor Disk Management Microsoft and Enterprise PKI Microsoft Cor	11070.007
Computer Managem Microsoft Cor		Device Manager Microsoft Cor Disk Management Microsoft and Enterprise PKI Microsoft Cor	1
		Disk Management Microsoft and Enterprise PKI Microsoft Cor	
		Enterprise PKI Microsoft Cor	
Group Policy Object Microsoft Cor		📓 Group Policy Object Microsoft Cor 🗸 🛛 🗛 Advance	
	Advanced		Advanced
scription:	Advanced		Advanced
Event Viewer Microsoft Cor		Event Viewer Microsoft Cor	
Folder Microsoft Cor			
Group Policy Object Microsoft Cor 🗸		Group Policy Object Microsoft Cor 🗸 Advance	
Group Policy Object Microsoft Cor 🗸		Group Policy Object Microsoft Cor	
Group Policy Object Microsoft Cor 🗸		Group Policy Object Microsoft Cor	

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

Action		Help	
nsole Root Certificates	- Current User	ject Type Certificates	
🛅 Tri	Find Certificates		
🧾 En 🧊 Int	All Tasks	> Find Certificates	
Ac	View New Window from Here	> Request New Certificate Import	
📔 Ur 🎬 Th	New Taskpad View	Advanced Operations >	Create Custom Request
Tri Cli Ce	Refresh Export List		Enroll On Behalf Of Manage Enrollment Policies
📔 Sn	Help		

42 | Install certificates for communication with the Mobile Server

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

Click Next.

– 🗆 🗆

🔄 Certificate Enrollment

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

onfigured by you ustom Request	Add Nev
Proceed without enrollment policy	

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

			_		×
C	Certificate Enrollment				
	Custom request				
	Chose an option fror	n the list below and configure the certificate options as required.			
	Template:	(No template) CNG key		~	
		Suppress default extensions			
	Request format:	○ <u>P</u> KCS #10			
		<u> </u>			
		not available for certificates based on a custom certificate reque the certificate template.	st, even w	/hen this	
			<u>N</u> ext	Cano	el :
	issue an erro	ormat depends on the CA. If the wrong format is chosen r when the certificate signing request (CSR) is submitted. ke 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.

General	Subject	Extensions	Private Key	Signature		
A friend	ly name	and descript	ion will make	e it easier to iden	tify and use a certi	ficate.
Friendly	y name:					
TestLa	bDomain.	.com				
Descrip	tion:					
TestLa	bDomain.	.com				

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:

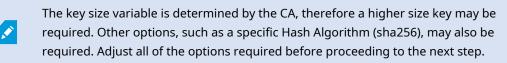
	ubject	-	D			
eneral S	subject	Extensions	Private Key	Signature		
an enter	inform				hich the certificate is is and alternative name v	
Subject of	f certifie	cate				
			receiving the	certificate		
Subject na						
	annea				CN=Test for Docs	
Туре:				A Julia	O=MJT	
Country		~		Add >	OU=MJT Lab	
Value:				Remove	L=Maple Grove	
			ר ור	Remove	S=MN C=USA	
	20200402				C-05A	
Alternativ	e name	3	_		10	
Туре:			_			
Directory	y name	~				
Value:						
				Add >		
			<	Remove		

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.

General Subject Extensions Private Key Signature The following are the certificate extensions for this certificate type. Key usage Key usage extension describes the purpose of a certificate. Available options: CRL signing Data encipherment Decipher only Encipher only Key agreement Non repudiation Add > Make these key usages critical Extended Key Usage (application policies) V OK Cancel Apply			Esteraione					
Key usage The key usage extension describes the purpose of a certificate. Available options: CRL signing Data encipherment Decipher only Encipher only Key agreement Non repudiation Add > Remove Make these key usages critical Extended Key Usage (application policies) v	ieneral	Subject	Extensions	Private Key	Signature			
The key usage extension describes the purpose of a certificate. Available options: CRL signing Data encipherment Decipher only Encipher only Key agreement Non repudiation Make these key usages critical Extended Key Usage (application policies) Basic constraints		-	e the certific	ate extension	s for this cer	tificate type.		^
Available options: CRL signing Data encipherment Decipher only Encipher only Key agreement Non repudiation < Remove							<u></u>	
CRL signing Data encipherment Decipher only Encipher only Key agreement Non repudiation < Remove	The ke	y usage e	extension des	cribes the pu	irpose of a co	ertificate.		
Data encipherment Decipher only Encipher only Key agreement Non repudiation < Remove	Availal	ole option	ns:			Selected options:		
Decipher only Encipher only Key agreement Non repudiation Make these key usages critical Extended Key Usage (application policies) Sasic constraints								
Encipher only Key agreement Non repudiation < Remove			ient					
Key agreement Non repudiation < Remove				Δ	dd >	Key encipherment		
Non repudiation Remove Make these key usages critical Extended Key Usage (application policies) Basic constraints								
Make these key usages critical Extended Key Usage (application policies) Basic constraints			n	Z P	amova			
Extended Key Usage (application policies) Basic constraints								
Basic constraints	✓ Mak	these k	ey usages cr	itical				
	Extend	ded Key U	lsage (applic	ation policies	s)		*	I
	Basic	constrain	ts				*	
								~

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.



Certificate Properties				×
General Subject Exter	nsions Private Key	Signature		
Cryptographic Servic	e Provider			~
Key options				~
Set the key length and	export options for	the private key.		
Key size: 2048		~		
Make private key ex	portable			
Allow private key to	be archived			
Strong private key p	protection			
Select Hash Algorithr	n			^
Select Hash Algorithm	n to be used for this	s request		
Hash Algorithm: sha2	256		~	
Select Signature Form	nat			~
		ОК	Cancel	Apply

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.

- 🗆 X

Certificate Enrollment

Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

Custom request	i) STATUS: Available	Details 🔺
The following options	describe the uses and validity period that apply to this t	ype of certificate:
Key usage:	Digital signature Key certificate signing Key encipherment	
Application polici		
Validity period (da	ys):	
		Properties
	Γ	Next Canc

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.

- 🗆 X

Finish

Cancel

📮 Certificate Enrollment

Where do you want to save the offline request?

If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish.

File Name:	
C:\Users\Administrator\Desktop\CSR6.1.21	Browse
File format:	
Base 64	
Binary	

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.

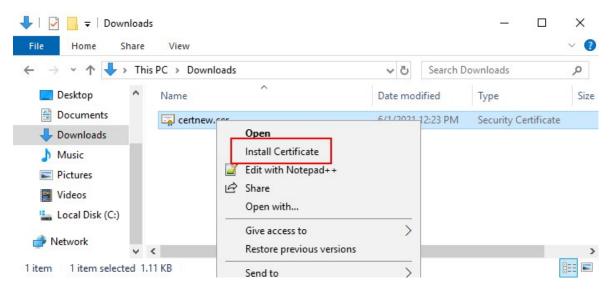
The following steps use a .CER file from an internal CA.

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.

CSR6.1.21 - Notepad	1 <u></u>		×
File Edit Format View Help			
BEGIN NEW CERTIFICATE REQUEST			~
MIIGBAYJKoZIhvcNAQcCoIIF9TCCBfECAQMxDzANBglghkgBZQMEA	gEFAD	CCBEoG	
CCsGAQUFBwwCoIIEPASCBDgwggQ0MGQwYgIBAgYKKwYBBAGCNwoKA	-		
AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QLTBBMDAwNDY3D		-	
MDQ2N1xBZG1pbm1zdHJhdG9yDAdNTUMuRVhFMIIDxqCCA8ICAQEwg		-	
ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAgMAk10MRQwEgYDVQQHD	-		
cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UECgwDTUpUMRYwF			
ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC	-	-	
5z1YrUGOo4dW1/b3o35rpcQQbyOUE0K1NWjaIy4YrRPM9HjhKReTh			
Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ//Zi08bEPobL		-	
lkaJWWRx3mbl/Yz0f1bwZrKFT3nkrXYOFYmZOR19W0J+Iin0Btziw			
nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9qC47RP9yMjyu			
qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs18zBATRXkk/k			
Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEAYI3DQIDMQ4WD			
NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/wQEAwICpDAdB	-		
vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCNxUUMTYwNAIBB			
MDA0NjcMGUIQLTBBMDAwNDY3XEFkbWluaXN0cmF0b3IMB01NQy5FW			
BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFMAb	-		
AHIAZQAgAEsAZQB5ACAAUwB0AG8AcgBhAGcAZQAgAFAAcgBvAHYAa		•	
ADANBgkghkiG9w0BAQsFAAOCAQEAgtKb5HCh2a1BD2QcKdFuhVQbN	-	-	
7bXdwVuzoAxd9BFd+uVy4D3TmvXtineT3GVWQbKJCcxRZeTKPBFnH	-		
cX4ySsKR1xGSuOhsfIVa/5NXiIYgYxMhlz3nt2CDw+RNqAp/1gLV2			
088po4/b9eiXV7A1DWFy7ecw/7Z20a07Sa0OaRbwzGJ8HelIiVEjf		-	
LkeSaJtjokkJuGPdr+ykjfuCmIF4hSbc0xzVkPCQbiHOwSxDGlkqY	-	-	
0L7QgBXCc7tcecDieqbYmp50LJPpqEQDQiYjzg57j3eYIFNYYjAAM		-	
hwIBA4AUvruQxeU1yku5Cem3anpu1cbMEDAwDQYJYIZIAWUDBAIBB			
hkiG9w0BCQMxCgYIKwYBBQUHDAIwLwYJKoZIhvcNAQkEMSIEICk1S			
DU1UXU+V05r1F8bNdM0mDgYfmjCiMA0GCSqGSIb3DQEBAQUABIIBA		-	
oZQj0vbWrAP0Ab2u8epFm7ZIMZzsJSzR0z98m+R+1R2mCogWC0SSa			
A3eqzDYxAu9p9drJft317sGAERE/i1D3BFvKZZQH0sz0JNRwDp3qB	-	-	
JSOpYvI1s3S23ZYEedQLp35Xy87378zLLGLpgGKTK4teav1IitUJw	-		
uOY4XLagwI1WWALsPF1+5ZcVNZMvsgzsbuMEXvjBkFKyhMv49oisg			
7Mbq8K6ckbKkVpuvmWThkVTp1W3hIS/i/J0X7c2unA25LxAC/P/Ly			
06jNaHC/zBQ=	-/	, 54,	
END NEW CERTIFICATE REQUEST			
the senter server hegelst			
<			>
Windows (CRLF Ln 1, C	ol 1	100%	

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.

🔶 🍠 Certificate Import Wizard

Welcome to the Certificate Import Wizard

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

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

Store Location

Local Machine

To continue, dick Next.

Next	Cancel
------	--------

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

← 🖉 Certificate Import Wizard	×
Certificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate.	
 Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Browse 	Select Certificate Store × Select the certificate store you want to use.
Next Can	cel

5. Finish the Install Certificate wizard.

Enable encryption on the Mobile Server

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

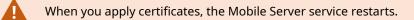
- 1. On a computer with a Mobile Server installed, open the Server Configurator from:
 - The Windows Start menu
 - or
- The Mobile Server Manager by right-clicking the Mobile Server Manager icon on the computer task bar
- 2. In the Server Configurator, under Mobile streaming media certificate, turn on 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.

_	
with encryption. <u>Learn</u>	more
over server, data	
~	Details
ires 5/8/2021	
treams from the mobile	
~	Details
/3/2121	
	Apply

5. Click Apply.



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.

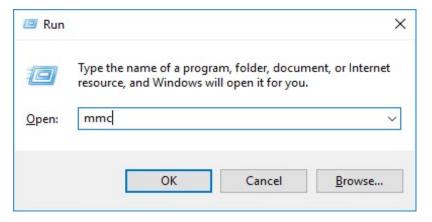
Add a CA certificate to the server

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....

	onsole1 - [Console Root]					– 🗆 X
Fi	e Action View Favorites New Open	Window	Help			_ 8 ×
	New	Ctrl+N				
	Open	Ctrl+0	Name		Actions	
	Save Save As	Ctrl+S	There are no	o items to show in this view.	Console Root	•
					More Actions	•
	Add/Remove Snap-in Options	Ctrl+M				
	Recent File					
	Exit					
-						
]]	

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

Click OK.

nap-in V					
	Vendor	^		Console Root	Edit Extensions
ActiveX Control N	Microsoft Cor			Certificates - Current L	Remove
Authorization Manager	Microsoft Cor				
	Microsoft Cor				
	Microsoft Cor				Move Up
,	Microsoft Cor				Move Down
	Microsoft Cor		Add >		Plove Down
	Microsoft Cor				
	Microsoft Cor				
	Microsoft and				
	Microsoft Cor				
	Microsoft Cor				
	Microsoft Cor				
Group Policy Object N	Microsoft Cor	~			Advanced
cription:					

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

1 🖄 🖬	1 🗟 🗟 🔽 🖬			
onsole Root Certificates	- Current User	Object Typ		
Tru	Find Certificates			
> 📫 En	All Tasks	>	Find Certificates	
> 📫 Ac > 📫 Tri	View New Window from Here	>	Request New Certificate Import	
📔 Ur 📔 Th	New Taskpad View		Advanced Operations >	Create Custom Request
Cli	Refresh Export List			Enroll On Behalf Of Manage Enrollment Policies
> 📔 Sn	Help			

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

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

Click Next.

– 🗆 🗆

🔄 Certificate Enrollment

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

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

		_		×
Certificate Enrollment				
Custom reques	t			
Chose an option fro	m the list below and configure the certificate options as required.			
Template:	(No template) CNG key		~	
	Suppress default extensions			
Request format:	○ <u>P</u> KCS #10			
	<u> </u>			
	s not available for certificates based on a custom certificate reque in the certificate template.	st, even w	vhen this	
		<u>N</u> ext	Cano	el:
issue an erro	format depends on the CA. If the wrong format is chosen or when the certificate signing request (CSR) is submitted. ake 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.

A friendly name and description will make it easier to identify and use a certificate Friendly name: TestLabDomain.com Description: TestLabDomain.com	
TestLabDomain.com Description:	e.
Description:	
TestLabDomain.com	
OK Cancel	Apply

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:

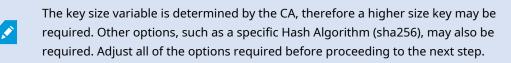
Certificat	e Propert	ies					×
General	Subject	Extensions	Private Key	Signature			
can ent	er inform						is issued. You ne values that
-	of certifie		receiving the	e certificate			
Subject	name:				10		
Type:						Test for Do	cs
Count	iry	~	-	Add >	0=N 0U=	MJT Lab	
Value:				Remove	L=N S=N C=U		
Alterna	tive name	2:					
Type:							
Direct	ory name	~					
Value:				Add >			
			<	Remove			
				O	< [Cancel	Apply

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.

General	Subject	Extensions	Private Key	Signature			
The foll			ate extension	-	tificate type.		^
Key us	age					^	
The ke	y usage e	xtension des	cribes the pu	irpose of a co	ertificate.		
Availat	ole option	IS:			Selected options:		
CRL sig]		Digital signature		
	ncipherm	ent			Key certificate signing	_	
	ner only			11.	Key encipherment		
	er only reement		A	dd >			
	pudiatio	n		emove			
✓ Mak	e these k	ey usages cr	itical				
Extend	led Key U	lsage (applic	ation policie	s)		*	
Racio	constrain	+c				~	
Dasic	constrain	6				•	

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.



	te Propert	ties				>
General	Subject	Extensions	Private Key	Signature		
Crypt	ographic	Service Prov	ider			*
Key o	ptions					^
Set the	e key leng	th and expo	rt options for	the private key.		
Key siz	e: 2048			,	~	
✓ Mal	ce private	key exportal	ble			
	w private	key to be ar	chived			
Stro	ng privat	e key protec	tion			
	ong privat	e key protec	tion			
	ong privat		tion			~
Select	Hash Alg	gorithm	tion used for this	request		^
Select Select	Hash Alg	gorithm orithm to be		; request	~	^
Select Select	Hash Alg	gorithm orithm to be		; request	~	*
Select Select Hash A	: Hash Alg Hash Alg Algorithm	gorithm orithm to be ^{I:} sha256		; request	~	^
Select Select Hash A	Hash Alg	gorithm orithm to be ^{I:} sha256		; request	~	*
Select Select Hash A	: Hash Alg Hash Alg Algorithm	gorithm orithm to be ^{I:} sha256		; request	~	^
Select Select Hash A	: Hash Alg Hash Alg Algorithm	gorithm orithm to be ^{I:} sha256		; request	~	~

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.

- 🗆 X

Certificate Enrollment

Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

Custom request	(i) STATUS: Available	Details 🔺
The following option	s describe the uses and validity period that apply to this typ	pe of certificate:
Key usage:	Digital signature Key certificate signing Key encipherment	
Application polic		
Validity period (d	ays):	
		Properties
	_	Next Cance
		Cance

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.

Ì

- 🗆 X

Finish

Cancel

Certificate Enrollment

Where do you want to save the offline request?

If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish.

File Name:	
C:\Users\Administrator\Desktop\CSR6.1.21	Browse
File format:	
Base 64	
Binary	

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.

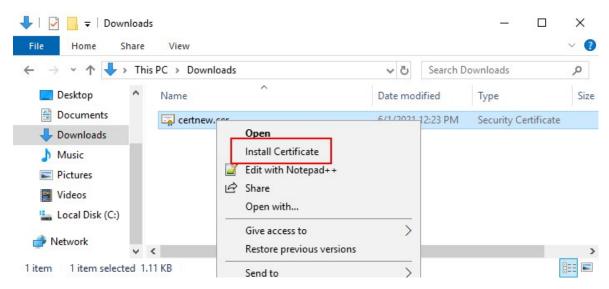
The following steps use a .CER file from an internal CA.

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.

File Edit Format View Help BEGIN NEW CERTIFICATE REQUEST MIIGBAYJKoZIhvcNAQcCoIIF9TCCBfECAQMxDzANB; CCsGAQUFBwwCoIIEPASCBDgwggQ0MGQwYgIBAgYKK AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QL MDQ2N1xBZG1pbm1zdHJhdG9yDAdNTUMuRVhFMIIDx; ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAgMAk10M cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UEC; ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFA; 5z1YrUG0o4dW1/b3o35rpcQQby0UE0K1NWjaIy4Yr; Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ; 1kaJWWRx3mb1/Yz0f1bwZrKFT3nkrXY0FYmZOR19W; nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9; qJJo0K6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs; Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEA; NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/; vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCN; MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b; BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwBvA;	WYBBAGCNWoKATFRM TBBMDAWNDY3DB1JU qCCA8ICAQEwggO7M RQwEgYDVQQHDAtNY gwDTUpUMRYwFAYDV AOCAQ8AMIIBCgKCA RPM9HjhKReThbcSn //Zi08bEPobLv8Yn DJ+Iin0BtziwiC8D qC47RP9yMjyuuEtp	NE8CAQAw JCOwQTAw NIICowIB YXBsZSBH YQQDDA1U AQEA7G1/ nxddj6eR WieNDuw DHt+bxST
MIIGBAYJKoZIhvcNAQcCoIIF9TCCBfECAQMxDzANB CCsGAQUFBwwCoIIEPASCBDgwggQ0MGQwYgIBAgYKK AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QL MDQ2N1xBZG1pbm1zdHJhdG9yDAdNTUMuRVhFMIIDx ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAgMAk10M cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UEC ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFA 5z1YrUG0o4dW1/b3o35rpcQQby0UE0K1NWjaIy4Yr Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ 1kaJWWRx3mb1/Yz0f1bwZrKFT3nkrXY0FYmZOR19W nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9 qJJo0K6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEA NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCN MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b	WYBBAGCNWoKATFRM TBBMDAWNDY3DB1JU qCCA8ICAQEwggO7M RQwEgYDVQQHDAtNY gwDTUpUMRYwFAYDV AOCAQ8AMIIBCgKCA RPM9HjhKReThbcSn //Zi08bEPobLv8Yn DJ+Iin0BtziwiC8D qC47RP9yMjyuuEtp	NE8CAQAw JCOwQTAw NIICowIB YXBsZSBH YQQDDA1U AQEA7G1/ nxddj6eR WieNDuw DHt+bxST
CCsGAQUFBwwCoIIEPASCBDgwggQ0MGQwYgIBAgYKK AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QL MDQ2N1xBZG1pbm1zdHJhdG9yDAdNTUMuRVhFMIIDx ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAgMAk10M cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UEC ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFA 5z1YrUGOo4dW1/b3o35rpcQQby0UE0K1NWjaIy4Yr Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ 1kaJWWRx3mb1/Yz0f1bwZrKFT3nkrXY0FYmZOR19W nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9 qJJo0K6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEA NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCN MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b	WYBBAGCNWoKATFRM TBBMDAWNDY3DB1JU qCCA8ICAQEwggO7M RQwEgYDVQQHDAtNY gwDTUpUMRYwFAYDV AOCAQ8AMIIBCgKCA RPM9HjhKReThbcSn //Zi08bEPobLv8Yn DJ+Iin0BtziwiC8D qC47RP9yMjyuuEtp	NE8CAQAw JCOwQTAw NIICowIB YXBsZSBH YQQDDA1U AQEA7G1/ nxddj6eR WieNDuw DHt+bxST
AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QL MDQ2N1xBZG1pbmlzdHJhdG9yDAdNTUMuRVhFMIIDx ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAgMAk10M cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UEC ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFA 5z1YrUGOo4dW1/b3o35rpcQQby0UE0K1NWjaIy4Yr Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ 1kaJWWRx3mb1/Yz0f1bwZrKFT3nkrXYOFYmZOR19W nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9 qJJo0K6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEA NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/r vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCN MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b	TBBMDAwNDY3DB1JU qCCA8ICAQEwggO7M RQwEgYDVQQHDAtNY gwDTUpUMRYwFAYDV AOCAQ8AMIIBCgKCA RPM9HjhKReThbcSn //Zi08bEPobLv8Yn DJ+Iin0BtziwiC8D qC47RP9yMjyuuEtp	JCOwQTAW MIICowIB /XBsZSBH /QQDDA1U AQEA7G1/ mxddj6eR WieNDuw DHt+bxST
MDQ2N1xBZG1pbm1zdHJhdG9yDAdNTUMuRVhFMIIDx ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAgMAk10M cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UEC ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFA 5z1YrUGOo4dW1/b3o35rpcQQbyOUE0K1NWjaIy4Yr Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ 1kaJWWRx3mb1/Yz0f1bwZrKFT3nkrXYOFYmZOR19W nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9 qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEA NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCN MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b	qCCA8ICAQEwggO7M RQwEgYDVQQHDAtNY gwDTUpUMRYwFAYDV AOCAQ8AMIIBCgKCA RPM9HjhKReThbcSn //Zi08bEPobLv8Yn DJ+Iin0BtziwiC8D qC47RP9yMjyuuEtp	MIICowIB (XBsZSBH (QQDDA1U QQEA7G1/ hxddj6eR WieNDuw OHt+bxST
ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAgMAk10M cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UEC ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFA 5z1YrUGOo4dW1/b3o35rpcQQby0UE0K1NWjaIy4Yr Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ 1kaJWWRx3mb1/Yz0f1bwZrKFT3nkrXY0FYmZ0R19W nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9 qJJo0K6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEA NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCN MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b	RQwEgYDVQQHDAtNY gwDTUpUMRYwFAYDV AOCAQ8AMIIBCgKCA RPM9HjhKReThbcSn //Zi08bEPobLv8Yn DJ+Iin0BtziwiC8D qC47RP9yMjyuuEtp	/XBsZSBH /QQDDA1U AQEA7G1/ nxddj6eR nWieNDuw)Ht+bxST
cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UEC ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFA 5z1YrUGOo4dW1/b3o35rpcQQbyOUE0K1NWjaIy4Yr Ziz50dV7tJOqtds9GuaPYX7PrGfsUs5/4AvEK8nDJ 1kaJWWRx3mb1/Yz0f1bwZrKFT3nkrXYOFYmZOR19W nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9 qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEA NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/v vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCN MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b	gwDTUpUMRYwFAYDV AOCAQ8AMIIBCgKCA RPM9HjhKReThbcSn //Zi08bEPobLv8Yn DJ+Iin0BtziwiC8D qC47RP9yMjyuuEtp	/QQDDA1U AQEA7G1/ nxddj6eR nWieNDuw DHt+bxST
ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFA 5zlYrUGOo4dW1/b3o35rpcQQby0UE0K1NWjaIy4Yr Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ 1kaJWWRx3mb1/Yz0f1bwZrKFT3nkrXY0FYmZOR19W nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9 qJJo0K6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEA NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCN MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b	AOCAQ8AMIIBCgKCA RPM9HjhKReThbcSn //Zi08bEPobLv8Yn DJ+Iin0BtziwiC8D qC47RP9yMjyuuEtp	QEA7G1/ hxddj6eR hWieNDuw DHt+bxST
5zlYrUGOo4dW1/b3o35rpcQQbyOUE0K1NWjaIy4Yr Ziz50dV7tJOqtds9GuaPYX7PrGfsUs5/4AvEK8nDJ 1kaJWWRx3mb1/Yz0f1bwZrKFT3nkrXYOFYmZOR19W nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9 qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEA NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/ vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCN MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b	RPM9HjhKReThbcSn //Zi08bEPobLv8Yn DJ+Iin0BtziwiC8D qC47RP9yMjyuuEtp	nxddj6eR WieNDuw Ht+bxST
Ziz50dV7tJOqtds9GuaPYX7PrGfsUs5/4AvEK8nDJ lkaJWWRx3mbl/Yz0f1bwZrKFT3nkrXYOFYmZOR19W nSd7C4rpx6uESaVltrVFfIYID6B/PfUCU+3uDUzs9 qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEA NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCN MDA0NjcMGU1QLTBBMDAwNDY3XEFkbWluaXN0cmF0b	//Zi08bEPobLv8Yn DJ+Iin0BtziwiC8D qC47RP9yMjyuuEtp	WieNDuw OHt+bxST
<pre>lkaJWWRx3mbl/Yz0f1bwZrKFT3nkrXYOFYmZOR19W nSd7C4rpx6uESaVltrVFfIYID6B/PfUCU+3uDUzs9 qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEA NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/ vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCN MDA0NjcMGU1QLTBBMDAwNDY3XEFkbWluaXN0cmF0b</pre>	DJ+Iin0BtziwiC8D qC47RP9yMjyuuEtp	Ht+bxST
nSd7C4rpx6uESaVltrVFfIYID6B/PfUCU+3uDUzs9 qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEA NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/ vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCN MDA0NjcMGU1QLTBBMDAwNDY3XEFkbWluaXN0cmF0b	qC47RP9yMjyuuEtp	
nSd7C4rpx6uESaVltrVFfIYID6B/PfUCU+3uDUzs9 qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEA NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/ vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCN MDA0NjcMGU1QLTBBMDAwNDY3XEFkbWluaXN0cmF0b	qC47RP9yMjyuuEtp	
qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEA NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCN MDA0NjcMGU1QLTBBMDAwNDY3XEFkbWluaXN0cmF0b		
Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEA NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/ vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCN MDA0NjcMGU1QLTBBMDAwNDY3XEFkbWluaXN0cmF0b		o6cXNJp
vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCN MDA0NjcMGU1QLTBBMDAwNDY3XEFkbWluaXN0cmF0b	YI3DQIDMQ4WDDEwL	
MDA0NjcMGU1QLTBBMDAwNDY3XEFkbWluaXN0cmF0b	VQEAwICpDAdBgNVH	Q4EFgQU
MDA0NjcMGU1QLTBBMDAwNDY3XEFkbWluaXN0cmF0b	KUUMTYWNAIBBQWLS	VAtMEEw
BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwBvAG8AcwBvA		
	GYAdAAgAFMAbwBmA	HQAdwBh
AHIAZQAgAEsAZQB5ACAAUwB0AG8AcgBhAGcAZQAgA	FAAcgBvAHYAaQBkA	GUAcgMB
ADANBgkqhkiG9w0BAQsFAAOCAQEAqtKb5HCh2a1BD	2QcKdFuhVQbNxg+G	5wcVkZt
7bXdwVuzoAxd9BFd+uVy4D3TmvXtineT3GVWQbKJC		
cX4ySsKR1xGSuOhsfIVa/5NXiIYgYxMh1z3nt2CDw		
088po4/b9eiXV7A1DWFy7ecw/7Z20a07Sa0OaRbwz		
LkeSaJtjokkJuGPdr+ykjfuCmIF4hSbcOxzVkPCQb	iHOwSxDG1kqYHZ8X	ru665Q6
0L7QgBXCc7tcecDieqbYmp50LJPpqEQDQiYjzg57j	BeYIFNYYjAAMAAxg	gGLMIIB
hwIBA4AUvruQxeU1yku5Cem3anpu1cbMEDAwDQYJY	IZIAWUDBAIBBQCgS	jAXBgkq
hkiG9w0BCQMxCgYIKwYBBQUHDAIwLwYJKoZIhvcNA	kEMSIEICk1SKp5M	WjMa+vr
DU1UXU+V05r1F8bNdM0mDgYfmjCiMA0GCSqGSIb3D	DEBAQUABIIBAEjqq	e4GSGE4
oZQj0vbWrAP0Ab2u8epFm7ZIMZzsJSzR0z98m+R+1		
A3eqzDYxAu9p9drJft317sGAERE/i1D3BFvKZZQH0		
JSOpYvI1s3S23ZYEedQLp35Xy87378zLLGLpgGKTK		
uOY4XLagwI1WWALsPF1+5ZcVNZMvsgzsbuMEXvjBk		
7Mbq8K6ckbKkVpuvmWThkVTp1W3hIS/i/J0X7c2un	-	
06jNaHC/zBQ=		.,,
END NEW CERTIFICATE REQUEST		
THE REAL TONIC REPORT		
<		>
Window	vs (CRLF Ln 1, Col 1	100%

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.

🔶 🍠 Certificate Import Wizard

Welcome to the Certificate Import Wizard

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

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

Store Location

Local Machine

To continue, dick Next.

Next	Cancel
------	--------

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

← 🛿 🖉 Certificate Import Wizard	×
Certificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate.	
 Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Browse	Select Certificate Store × Select the certificate store you want to use. Interview of the certification Authorities Intermediate Certification Authorities Intermediate Certification Authorities Trusted Publishers × Show physical stores OK
Next Can	cel

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.

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

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.

Encryption Registering servers Language selection Server certificate Applies to: management server, recording server, failover server, data collector Encryption: On Certificate issued by MS-Organization-P2P-Access [2021]. Expires 5/8/2021 Streaming media certificate Applies to clients and servers that retrieve data streams from the record server Encryption: On Certificate issued by MS-Organization-P2P-Access [2021]. Expires 5/8/2021 Certificate issued by MS-Organization-P2P-Access [2021]. Expires 5/8/2021	_	- C		×
Language selection Server certificate Applies to: management server, recording server, failover server, data collector Encryption: On Certificate issued by MS-Organization-P2P-Access [2021]. Expires 5/8/2021 Streaming media certificate Applies to clients and servers that retrieve data streams from the record server Encryption: On				
Applies to: management server, recording server, failover server, data collector Encryption: On Certificate issued by MS-Organization-P2P-Access [2021]. Expires 5/8/2021 Streaming media certificate Applies to clients and servers that retrieve data streams from the record server Encryption: On	ption. <u>Learn</u>	arn more		
Certificate issued by MS-Organization-P2P-Access [2021]. Expires 5/8/2021 Streaming media certificate Applies to clients and servers that retrieve data streams from the record server Encryption: On	data			
Streaming media certificate Applies to clients and servers that retrieve data streams from the record server Encryption: On)		
Streaming media certificate Applies to clients and servers that retrieve data streams from the record server Encryption: On	~	De	etails	
Applies to clients and servers that retrieve data streams from the record server Encryption: On				
Certificate issued by MS-Organization-P2P-Access [2021]. Expires 5/8/2021			etails	
Certificate issued by MS-Organization-P2P-Access [2021]. Expires 5/8/2021	~	De	etalls	
		Ар	oply	

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).

Install Active Directory Certificate Services

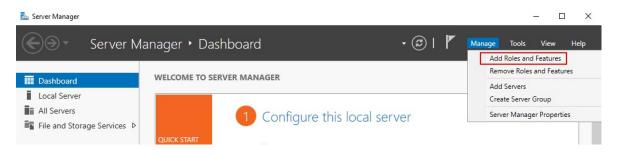
Active Directory Certificate Services (AD CS) is a Microsoft product that performs public key infrastructure (PKI) functionality. It acts as a Server Role that enables you to construct public key infrastructure (PKI) and give open key cryptography, computerized authentication, and advanced mark abilities 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 85)
- In a Workgroup environment (see Install certificates in a Workgroup environment for communication with the Management Server or Recording Server on page 103)

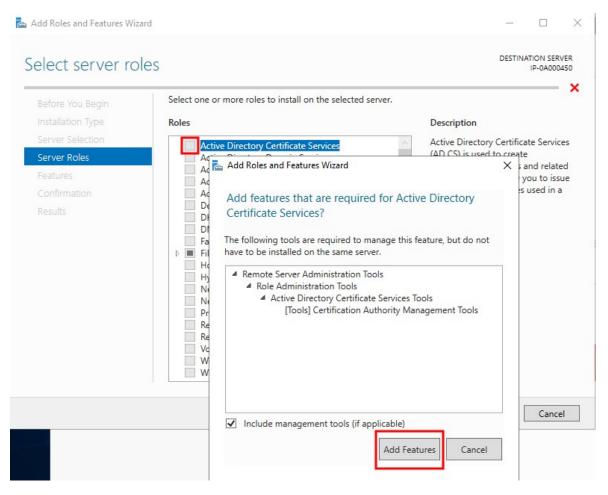
To install AD CS:

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.

Add Roles and Features Wize	ard	-		×
Select role servi	ces	DESTIN	NATION SER	
Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Web Server Role (IIS) Role Services Confirmation Results	✓ Certification Authority Network ✓ Certificate Enrollment Policy Web Service make ✓ Certificate Enrollment Web Service mane ✓ Certification Authority Web Enrollment other	s vork Device Enrollr es it possible to iss lage certificates for er network devices e network accounts	routers and that do not	nd
	< Previous Next >	Install	Cance	el

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.

Server Manager • Dashboard 📥 Add Roles and Features Wizard × WELCOME TO SERVER MANAGER DESTINATION SERVER IP-0A000467 Installation progress View installation progress 1 Confie 1 Feature installation age Services D Configuration req 2 Add ed. Installation succeeded on IP-0A000467. Active Directory Certificate Services Additional steps are required to configure Active Directory Certificate Services on the destination server Configure Active Directory Certificate Services on the destination server 3 Add VHAT'S NEW 4 Crea Certification Authority Network Device Enrollment Service Certificate Enrollment Policy Web Service Certificate Enrollment Web Service 5 Con Certification Authority Web Enrollment mote Server Administration Tools Role Administration Tools Rei ROLES AND SERVER GROUPS Roles: 3 | Server groups: 1 | Servers total You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details. AD CS 1 All Servers Export configuration settings Manageability Manageability < Previous Next > Close Cancel Events Events

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.

• 🔊 🍢
Post-deployment Configura TASKS 💌 🛛 🗙
Configuration required for Active Directory Certificate Services at IP-0A000467
Configure Active Directory Certificate Services on th
Feature installation
Configuration required. Installation succeeded on IP-0A000467.
Add Roles and Features

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**.

AD CS Configuration	- D ×
Credentials	DESTINATION SERVER IP-0A000450
Credentials Role Services	Specify credentials to configure role services
Confirmation	To install the following role services you must belong to the local Administrators group:
Progress Results	Standalone certification authority Certification Authority Web Enrollment Online Responder
	To install the following role services you must belong to the Enterprise Admins group:
	 Enterprise certification authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Network Device Enrollment Service
	Credentials: IP-0A000450\Administrator Change
	More about AD CS Server Roles < Previous

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

Click Next.

AD CS Configuration					_		×
Role Services				DES		ION SER P-0A000	
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Select Role Services to con	lent					
	More about AD CS Server Roles						
	< P	revious	Next >	Configu	ire	Cance	2l

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

AD CS Configuration	- D ×
Setup Type	DESTINATION SERVER IP-0A000450
Credentials Role Services Setup Type	Specify the setup type of the CA Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to
CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	 simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates. Enterprise CA Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies. Standalone CA Standalone CA Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).
	More about Setup Type
	< Previous Next > Configure Cancel

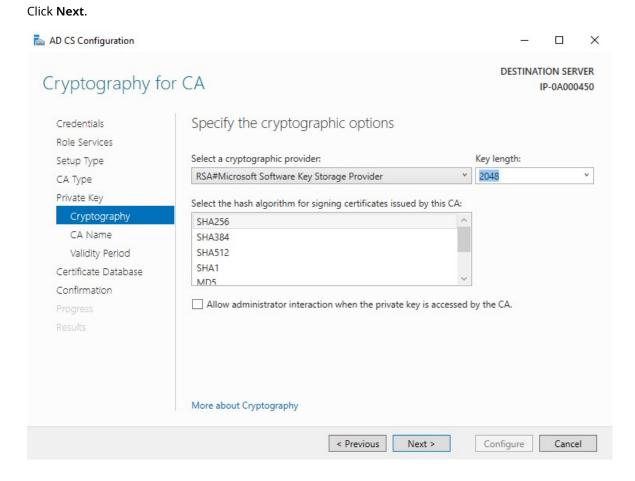
15. In CA Type, select the option to install a Root CA, and click Next.

AD CS Configuration	- 🗆 ×
СА Туре	DESTINATION SERVER IP-0A000450
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	 Specify the type of the CA When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy. Root CA Root CA Root CAs are the first and may be the only CAs configured in a PKI hierarchy. Subordinate CA subordinate CA receives and are authorized to issue certificates by the CA above them in the hierarchy.
	More about CA Type < Previous

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

D CS Configuration	:
rivate Key	DESTINATION SERVER
Credentials Role Services Setup Type	Specify the type of the private key To generate and issue certificates to clients, a certification authority (CA) must have a private key.
СА Туре	Oreate a new private key
Private Key	Use this option if you do not have a private key or want to create a new private key.
Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	 Use existing private key Use this option to ensure continuity with previously issued certificates when reinstalling a CA. Select a certificate and use its associated private key Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key. Select an existing private key on this computer Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.
	More about Private Key

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.



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."

AD CS Configuration	- 🗆 X
CA Name	DESTINATION SERVER IP-0A000450
Credentials Role Services Setup Type CA Type	Specify the name of the CA Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.
Private Key Cryptography CA Name	Common name for this CA: IP-0A000450-CA
Validity Period Certificate Database Confirmation	Distinguished name suffix: Preview of distinguished name:
Progress Results	CN=IP-0A000450-CA
	More about CA Name
	< Previous Next > Configure Cancel

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

AD CS Configuration							_		×
Validity Period						D	ESTINAT	ION SER	
Credentials Role Services Setup Type	Select th	fy the validity	the certifica	te generated	for this certit	fication aut	hority (C/	A):	
СА Туре	5	Years	×						
Private Key Cryptography CA Name Validity Period	The vali	ration Date: 4/27/202 dity period configure tes it will issue.			hould exceed	l the validity	y period 1	for the	
Certificate Database									
Confirmation									
Progress									
	More at	oout Validity Period							
			< Pre	evious	Next >	Config	gure	Cance	el

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.

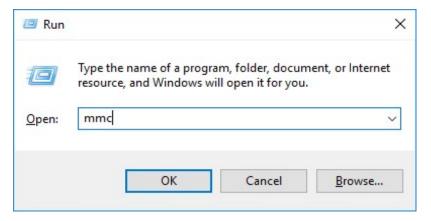


Microsoft provides extensive documentation for Windows Server operating systems, which includes templates for server certificates, installation of the CA, and certificate deployment can be found in Microsoft's Server Certificate Deployment Overview.

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....

	onsole1 - [Console Root]						- 🗆 ×
🚡 Fil	e Action View Favorite New Open	s Window	Help				- & ×
\$	New	Ctrl+N					
	Open	Ctrl+0	Name			Actions	
	Save	Ctrl+S		e are no iter	ns to show in this view.	Console Root	•
	Save As		1000000 100000			More Actions	•
	Add/Remove Snap-in	Ctrl+M					
	Options						
	Recent File						
	Exit						
_							

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

Click OK.

		122			
ap-in	Vendor	^		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor			Certificates - Current U	Remove
Authorization Manager	Microsoft Cor				
Certificate Templates	Microsoft Cor				
Certificates	Microsoft Cor				Move Up
Certification Authority	Microsoft Cor				Move Down
Component Services	Microsoft Cor		Add >		Plove Down
Computer Managem	Microsoft Cor				
Device Manager	Microsoft Cor				
Disk Management	Microsoft and				
Enterprise PKI	Microsoft Cor				
Event Viewer	Microsoft Cor				
Folder	Microsoft Cor				
Group Policy Object	Microsoft Cor	¥.			Advanced
cription:				· L	
inpuon:					

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

	iew Favorites Window	Help		
Console Root Certificates - () Personal) Personal Fri F		Object Ty <u> </u> Certifi		
> 📔 En 🛛 🗚	All Tasks	>	Find Certificates	
> 📫 Ac V > 📫 Tru N	'iew Jew Window from Here	>	Request New Certificate Import	
> <u> </u>	lew Taskpad View		Advanced Operations >	Create Custom Request
> 🦳 Cli	lefresh xport List			Enroll On Behalf Of Manage Enrollment Policies
> 🧮 Sn 🛛 🛏	lelp			

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

5. 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.

	V
	\sim

🛱 Certificate Enrollment

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by you	Add New
Custom Request	
Proceed without enrollment policy	
	Next Cance

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

– 🗆 X

	Certificate	Enroll	ment
--	-------------	--------	------

Custom request

Chose an option from the list below and configure the certificate options as required.

Template:	(No template) CNG key	~
	Suppress default extensions	
Request format:	○ <u>P</u> KCS #10	
	● <u>C</u> MC	

Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template.

Next Cancel

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

- 🗆 🗙

Next

Cancel

🔄 Certificate Enrollment

Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

Custom request	STATUS: Available	Details 🔺
The following option	s describe the uses and validity period that apply to this	type of certificate:
Key usage:	Digital signature Key certificate signing Key encipherment	
Application polic		
Validity period (d	ays):	
		Properties

90	Install	certificates	in a domai	n for	communication	with the	Management	Server or	Recording	Server
50	mstan	certificates	in a domai	1101	communication	vvici ci c	management	SCIVCI OI	Recording .	JUIVUI

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

Seneral	Subject	Extensions	Private Key	Signature		
A friend	lly name	and descript	ion will make	e it easier to ident	ify and use a certif	ficate.
Friendly	name:					
TestLa	Domain	.com				
Descrip	tion:					
TestLa	Domain	.com				

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.

			Certifica	te Propert	ties	×
General	Subject	Extensions	Private Key	Signature		
can entr can be Subject	er inform used in a of certifie	ation about certificate. cate		subject nam	which the certificate e and alternative na	
Subject	name:		_			
Type:					CN=MJT-12A	
Comm	non name	e v		Add >		
Value:			<	Remove		
Alternat	tive name	8				
Type:			_			
Directo	ory name	~	·			
Value:				Add >		
			<	Remove		
				OF	Cancel	Apply

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

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

General Subject	Extensions	Private Key	Signature			
The following are	e the certific			tificate type.	-	^
Key usage					~	
Extended Key U	sage (applic	ation policie	s)		^	
certificate can b certificates issue Available option Client Authentio Code Signing Secure Email Time Stamping Microsoft Trust Microsoft Time IP security end s IP security tunn	e used. Selected by this ter s: cation ^ List Signin Stamping system	ct the applica mplate.		Vindows 2000) defin equired for valid sign Selected options: Server Authentica	natures of	=
A Make the Exte	ended Key U	sage critical		< 111	>	
- · ·						~

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.

	Subject	Extensions	Private Key	Signature		
Crypto	ographic	Service Prov	ider			*
Key op	otions					^
Set the	key leng	th and expor	t options for	the private key		
Key size	e: 2048				~	
✓ Mak	e private	key exportal	ole			
	w private	key to be ar	chived			
and the second		key to be ar e key protect				
and the second						
Stro		e key protect				~
Select	ng privato Hash Alg	e key protect		s request		^
Select Select	ng privato Hash Alg	e key protect jorithm orithm to be	tion	s request	~	^
Select Select	ng privato Hash Alg Hash Algo	e key protect jorithm orithm to be	tion	s request	~	^
Select Select H Hash A	ng privato Hash Alg Hash Algo	orithm orithm to be sha256	tion	s request	~	*
Select Select H Hash A	ng privato Hash Alg Hash Algo Ilgorithm	orithm orithm to be sha256	tion	s request	~	~

- 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.

Ì

- 🗆 X

Certificate Enrollment

Where do you want to save the offline request?

If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish.

Browse
Finish Cano

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 73.

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.

107Test1 - Notepad	-		×
File Edit Format View Help			
<pre>File Edit Format View Help BEGIN NEW CERTIFICATE REQUEST MIIF2AYJKoZIhvcNAQcCoIIFyTCCBcUCAQMxDzANBglghkgBZQ CCsGAQUFBwwCoIIEEASCBAwwggQIMGYwZAIBAgYKKwYBBAGCNwd AwIBATFHMEUGCSsGAQQBgjcVFDE4MDYCAQUMDENsdXN0ZXIxVEV UjFURU1QXEFkbWluaXN0cmF0b3IMB01NQy5FWEUwggOYoIIDIA AgEAMBcxFTATBgNVBAMMDENsdXN0ZXIxVEVNUDCCASIwDQYJKoZ ggEPADCCAQoCggEBAKVp0982yi05tcnypaTujsFBe9jwOyRp+c3 dVMVTSU9s9rTMWmUDzP+zLumOmC6gCWIo5RgiT+dLjOvq+Z6AUM ZktV8ut805gi46dkQ4MD71btX6mnjjUB294Xwf8yUVP1Be0dkfd zczK1yUZmY576IBwf6LZMujXbNDD5ZXzdhG3pggarNdzHvg0RI JN2d0SZms4Utj21DekFde3BsENvcvk0/PHZk8b8Bww050+ya3tH bqL+Zy4pEP1jKnTwM1IyPmsXyw7gx6CrTw8ntqECAwEAAaCCAS8 Nw0CAzEOFgwxMC4wLjE0MzkzLjIwRQYJKwYBBAGCNxUUMTgwNg cjFURU1QDBpDTFVTVEVSMVRFTVBcQWRtaW5pc3RyYXRvcgwHTU2 hkiG9w0BCQ4xUzBRMBMGA1UdJQQMMAoGCCsGAQUFBwMBMBBsGCS9 MAwwCgYIKwYBBQUHAwEwHQYDVR00BBYEF0BsTd6/Hpi6c18h5HF CisGAQQBgjcNAgIxWDBWAgEAHk4ATQBpAGMAcgBvAHMAbwBmAH0 AHcAYQByAGUAIABLAGUAeQAgAFMAdABvAHIAYQBnAGUAIABQAH1 AHIDAQAwDQYJKoZIhvcNAQELBQADggEBAFGoQLCtyiv0XG0T04 OAPtDKNDGskV/dq6rqgpYEKiQfWZeSndE0zxieJtES/115hmV06</pre>	oKATFTMI VNUAwaQQ IBATCCA4 ZIhvcNAQ 5N00xf8Q WC1H+WVQ qjUVnn6I Jvro4IJQ k7jDbvwQ RAJDbvWQ BWHAYKKQ IBBQwMQ 1DLkVYR sGAQQBg 488hWc QAIABTAQ IAbwB2AQ	FECAQA avVU1R 40wggJ QEBBQA DcN0Dy JsaVbJ EAYzHd arM6Es Da1VXE wYBBAG 2x1c3R TBgBgk jcVCgQ 011MGY G8AZgB GkAZAB 50sQUn	W F I I I I I I I I I I I I I I I I I I
XjUze/+WIiZifGFnkMKYwrzKgx7qIr\Undo			
m3dWazix8dSVOQIRZ3Lr7yXg9iiF49 EX7yVZFyEAs/6uoApcKXc2KPgBP8aHe Cut			j
Tp4XCYYiuyw/+iHqyNca2fvIIm8Hpb(Copy			В
izCCAYcCAQOAFOBsTd6/Hpi6c18h5H			4
FwYJKoZIhvcNAQkDMQoGCCsGAQUFBwu OY6dr8BzietMf5QwmoRNzg8MRGSQiN: Delete			
+q73I6NKKLzg7ROhm16Xj7tL4Id2iVk Select All			
1WR7EktvnBLYuBQVPGYb+gwd8EfBh9 r+5Z7i0E2HZpsBrS1d1+u89F0Pi+W/a Right to left Reading ord	der)
nIi7k+ce+EDoHhXkbSD+fHYFbUqaTYL Show Unicode control c			J
2PmPVkUJGJEUMwfo8rb4xb9taP6ycUJ T8XTFWM0JCPMykW2	haracter	>	В
END NEW CERTIFICATE REQUE: Open IME			
< Reconversion			>

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.

Microsoft Active Directory Certifie × +	• - • ×
← → C ▲ Not secure 10.0.4.103/certsrv/	☆ 🚨 Update 🔅
Microsoft Active Directory Certificate Services – IP-0A000467-CA	<u>Home</u>

Welcome

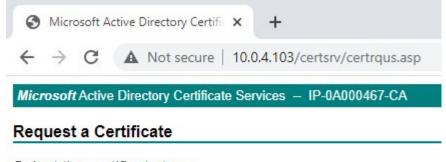
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see <u>Active Directory Certificate Services</u> <u>Documentation</u>.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

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



Select the certificate type: <u>Web Browser Certificate</u> <u>E-Mail Protection Certificate</u>

Or, submit an advanced certificate request.

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.

🔶 🕘 🏉 htt	tp:// 192.168.50.108 /certsn	. ク マ Ċ Ø Microsoft Active Directory ×	6) fr 🛱 🧐
Microsoft Active	e Directory Certificate S	ervices CLUSTER2TEMP-CA	Home
Submit a Cer	rtificate Request o	r Renewal Request	
	est generated by ar	e CA, paste a base-64-encoded CMC or PKCS #10 certi n external source (such as a Web server) in the Saved F	
Base-64-encode	1WR7EktvnBLÝuBQ d r+527iOE2HZpsBr st nIi7k+ce+EDoHhX 2PmPVkUJGJEUMwfc T8XTFWMOJCPMykW2	VPGYD+gwd8EfBh9K9Qqvd5fMu: Sldl+u89F0Pi+W/a8/YV7BhAl: kbSD+fHYFbUqaTYUfgU4u5Pq6: S8rb4xb9taP6ycUZwieLrNWw31 2 TIFFICATE REQUEST	
Additional Attril	kutes:	>	
Attributes	5.	>	
		Submit >	

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 .

 \sim

- 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**.

Welcome to the	e Certificat	e Import V	Wizard	
This wizard helps you co lists from your disk to a		ertificate trust	lists, and certificate	revocation
A certificate, which is iss and contains information connections. A certificat	used to protect	data or to esta	blish secure network	¢
Store Location Current User				
To continue, dick Next.				

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

🗧 🛃 Certificate Import Wizard	×
Certificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate.	
 Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Browse 	Select Certificate Store × Select the certificate store you want to use. Personal Trusted Root Certification Authorities Enterprise Trust Trusted Publishers Show physical stores OK Cancel
Next Car	ncel

- 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...**.

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

File Action View Favorites Window	Help			
🔶 🔿 🙋 📆 🔏 🖬 🗙 🗒 🗟 🛛				
Console Root	Issued To		Issued By	Expiration
✓ ☐ Certificates (Local Computer)	Cluster1TEN	AD.	CLUSTER2TEMP-CA	10/26/202
 Personal Certificates 		Open		
> 📋 Trusted Root Certification Authoritie		All Tasks	Open	
Enterprise Trust Intermediate Certification Authoritie		Cut	Request Certificate with New Key.	•
Trusted Publishers		Сору	Renew Certificate with New Key	
 Untrusted Certificates Third-Party Root Certification Author 		Delete	Manage Private Keys	
Certificates		Properties	Advanced Operations	>
Trusted People		Help	Export	

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

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.

Server Configurator			
Encryption	Encryption		
Registering servers	It is recommended to secure communication with encryption	. <u>Learn n</u>	nore
Language selection	Server certificate Applies to: management server, recording server, failover server, data collector		
	Encryption: On		
	Remainer	~	Detail
	Certificate issued by MS-Organization-P2P-Access [2021]. Expires 5/8/2021		
	Applies to clients and servers that retrieve data streams from the record server Encryption: On		
	Republica	~	Detail
	Certificate issued by MS-Organization-P2P-Access [2021]. Expires 5/8/2021		
	Certificate issued by MS-Organization-P2P-Access [2021]. Expires 5/8/2021		
	Certificate issued by MS-Organization-P2P-Access [2021], Expires 5/8/2021		
	Certificate issued by MS-Organization-P2P-Access [2021]. Expires 5/8/2021		
	Certificate issued by MS-Organization-P2P-Access [2021], Expires 5/8/2021		
	Certificate issued by MS-Organization-P2P-Access [2021], Expires 5/8/2021		

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.

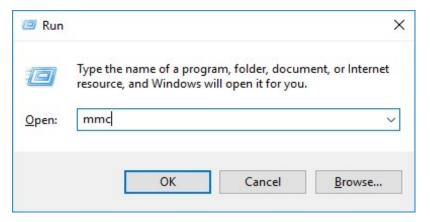
Install certificates in a Workgroup environment for communication with the Management Server or Recording Server

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....

	onsole1 - [Console Root]						- 🗆 ×
🚡 Fil	e Action View Favorite New Open	s Window	Help				- & ×
\$	New	Ctrl+N					
	Open	Ctrl+0	Name			Actions	
	Save	Ctrl+S		e are no iter	ns to show in this view.	Console Root	•
	Save As		1000000 100000			More Actions	•
	Add/Remove Snap-in	Ctrl+M					
	Options						
	Recent File						
	Exit						
_							

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

Click OK.

ap-in	Vendor	~		Selected snap-ins:	Edit Extensions	
ActiveX Control	Microsoft Cor			Certificates (Local Computer)	Cure Exteriorono	
	Microsoft Cor				Remove	
Certificates	Microsoft Cor	=				
Component Services	Microsoft Cor				Maria Ha	_
	Microsoft Cor			Move Up	_	
Device Manager	Microsoft Cor	-		Move Down		
Disk Management	Microsoft and		Add >	Add >	-	
Event Viewer	Microsoft Cor					
Folder	Microsoft Cor					
Group Policy Object	Microsoft Cor					
Internet Informatio	Microsoft Cor					
Internet Informatio	Microsoft Cor					
IP Security Monitor	Microsoft Cor					
IP Security Policy M	Microsoft Cor	~			Advanced	
cription:						
	ws you to browse					_

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

» 🖄 📰	📋 🖪 😖 🔽 📷		
onsole Root Certificates	- Current User	ype ficates	
Tri 📔	Find Certificates		
> 📔 En	All Tasks	Find Certificates	
> 📫 Ac > 📫 Tri	View > New Window from Here	Request New Certificate Import	
Dr 📔 Ur	New Taskpad View	Advanced Operations >	Create Custom Request
Tru	Refresh Export List		Enroll On Behalf Of Manage Enrollment Policies
> 📫 Sn	Help		

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

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

Click Next.

– 🗆 🗙

🔄 Certificate Enrollment

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Add Nev

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

– 🗆 X

-	Certificate Enrollment
---	------------------------

Custom request

Chose an option from the list below and configure the certificate options as required.

Template:	(No template) CNG key	~
	Suppress default extensions	
Request format:	○ <u>P</u> KCS #10	
	● <u>C</u> MC	

Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template.

Next Cancel

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

tificate Enrollment		
Click Next to use the options already equest, and then click Next.	r selected for this template, or click Details to cu	stomize the certifica
Custom request	(i) STATUS: Available	Details
Key usage:	the uses and validity period that apply to this ty	ype of certificate:
Application policies:		
Validity period (days):		Properties
		Properties

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

General Subject Extensions Private Ke	y Signature
A friendly name and description will m	ake it easier to identify and use a certificate.
Friendly name:	
TestLabDomain.com	
Description:	
TestLabDomain.com	

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.

			Certifica	te Properti	ies	
General	Subject	Extensions	Private Key	Signature		
can ent can be Subject	er inform used in a of certifie	ation about certificate. cate		subject name	which the certificate is e and alternative name	
Subject	name:		_			
Type:					CN=MJT-12A	
Comm	non name	e v		Add >		
Value:			<	Remove		
Alternat	tive name	E				
Type:			_			
Direct	ory name	· ·	·			
Value:				Add >		
			<	Remove		
				OK	Cancel	Apply

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

General Subject Extension		Signature		
The following are the certif	cate extension	s for this cer	tificate type.	^
Key usage				~
Extended Key Usage (appl	ication policie	s)		^
An application policy (call certificate can be used. Sel certificates issued by this to Available options: Client Authentication Code Signing Secure Email Time Stamping Microsoft Trust List Signin Microsoft Trust List Signin Microsoft Time Stamping IP security end system IP security tunnel termina	ect the applica emplate.			natures of ≣
IP security user	Vsage critical		< 111	>
				×

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.

Cryptographic Service Provider Key options Set the key length and export options for the private key. Key size: 2048 Make private key exportable Allow private key to be archived Strong private key protection Select Hash Algorithm Select Hash Algorithm to be used for this request Hash Algorithm:	*
Set the key length and export options for the private key. Key size: 2048 Make private key exportable Allow private key to be archived Strong private key protection Select Hash Algorithm Select Hash Algorithm to be used for this request	^
Key size: 2048 Make private key exportable Allow private key to be archived Strong private key protection Select Hash Algorithm Select Hash Algorithm to be used for this request	
 Make private key exportable Allow private key to be archived Strong private key protection Select Hash Algorithm Select Hash Algorithm to be used for this request 	
Allow private key to be archived Strong private key protection Select Hash Algorithm Select Hash Algorithm to be used for this request	
Allow private key to be archived Strong private key protection Select Hash Algorithm Select Hash Algorithm to be used for this request	
Strong private key protection Select Hash Algorithm Select Hash Algorithm to be used for this request	
Select Hash Algorithm Select Hash Algorithm to be used for this request	
Select Hash Algorithm to be used for this request	
Select Hash Algorithm to be used for this request	
Select Hash Algorithm to be used for this request	~
Hash Algorithm: sha256 V	
310250	
Colort Conneture Formet	
Select signature romat	
	*
Select Signature Format	

- 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.

Ì

- 🗆 X

Certificate Enrollment

Where do you want to save the offline request?

If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish.

Browse
Finish Cano

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 73.

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.

107Test1 - Notepad	-		×
File Edit Format View Help			
<pre>File Edit Format View Help BEGIN NEW CERTIFICATE REQUEST MIIF2AYJKoZIhvcNAQcCoIIFyTCCBcUCAQMxDzANBglghkgBZQ CCsGAQUFBwwCoIIEEASCBAwwggQIMGYwZAIBAgYKKwYBBAGCNwd AwIBATFHMEUGCSsGAQQBgjcVFDE4MDYCAQUMDENsdXN0ZXIxVEV UjFURU1QXEFkbWluaXN0cmF0b3IMB01NQy5FWEUwggOYoIIDIA AgEAMBcxFTATBgNVBAMMDENsdXN0ZXIxVEVNUDCCASIwDQYJKoZ ggEPADCCAQoCggEBAKVp0982yi05tcnypaTujsFBe9jwOyRp+c3 dVMVTSU9s9rTMWmUDzP+zLumOmC6gCWIo5RgiT+dLjOvq+Z6AUM ZktV8ut805gi46dkQ4MD71btX6mnjjUB294Xwf8yUVP1Be0dkfd zczK1yUZmY576IBwf6LZMujXbNDD5ZXzdhG3pggarNdzHvg0RI JN2d0SZms4Utj21DekFde3BsENvcvk0/PHZk8b8Bww050+ya3tH bqL+Zy4pEP1jKnTwM1IyPmsXyw7gx6CrTw8ntqECAwEAAaCCAS8 Nw0CAzEOFgwxMC4wLjE0MzkzLjIwRQYJKwYBBAGCNxUUMTgwNg cjFURU1QDBpDTFVTVEVSMVRFTVBcQWRtaW5pc3RyYXRvcgwHTU2 hkiG9w0BCQ4xUzBRMBMGA1UdJQQMMAoGCCsGAQUFBwMBMBBsGCS9 MAwwCgYIKwYBBQUHAwEwHQYDVR00BBYEF0BsTd6/Hpi6c18h5HF CisGAQQBgjcNAgIxWDBWAgEAHk4ATQBpAGMAcgBvAHMAbwBmAH0 AHcAYQByAGUAIABLAGUAeQAgAFMAdABvAHIAYQBnAGUAIABQAH1 AHIDAQAwDQYJKoZIhvcNAQELBQADggEBAFGoQLCtyiv0XG0T04 OAPtDKNDGskV/dq6rqgpYEKiQfWZeSndE0zxieJtES/115hmV06</pre>	oKATFTMI VNUAwaQQ IBATCCA4 ZIhvcNAQ 5N00xf8Q WC1H+WVQ qjUVnn6I Jvro4IJQ k7jDbvwQ RAJDbvWQ BWHAYKKQ IBBQwMQ 1DLkVYR sGAQQBg 488hWc QAIABTAQ IAbwB2AQ	FECAQA avVU1R 40wggJ QEBBQA DcN0Dy JsaVbJ EAYzHd arM6Es Da1VXE wYBBAG 2x1c3R TBgBgk jcVCgQ 011MGY G8AZgB GkAZAB 50sQUn	W F I I I I I I I I I I I I I I I I I I
XjUze/+WIiZifGFnkMKYwrzKgx7qIr\Undo			
m3dWazix8dSVOQIRZ3Lr7yXg9iiF49 EX7yVZFyEAs/6uoApcKXc2KPgBP8aHe Cut			j
Tp4XCYYiuyw/+iHqyNca2fvIIm8Hpb(Copy			В
izCCAYcCAQOAFOBsTd6/Hpi6c18h5H			4
FwYJKoZIhvcNAQkDMQoGCCsGAQUFBwu OY6dr8BzietMf5QwmoRNzg8MRGSQiN: Delete			
+q73I6NKKLzg7ROhm16Xj7tL4Id2iVk Select All			
1WR7EktvnBLYuBQVPGYb+gwd8EfBh9 r+5Z7i0E2HZpsBrS1d1+u89F0Pi+W/a Right to left Reading ord	der)
nIi7k+ce+EDoHhXkbSD+fHYFbUqaTYL Show Unicode control c			J
2PmPVkUJGJEUMwfo8rb4xb9taP6ycUJ T8XTFWM0JCPMykW2	haracter	>	В
END NEW CERTIFICATE REQUE: Open IME			
< Reconversion			>

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.

S Microsoft Active Directory Certifi × +	• - • ×
← → C ▲ Not secure 10.0.4.103/certsrv/	🖈 😩 Update 🔋
Microsoft Active Directory Certificate Services – IP-0A000467-CA	Home
Welcome	

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see <u>Active Directory Certificate Services</u> <u>Documentation</u>.

Select a task:

Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

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

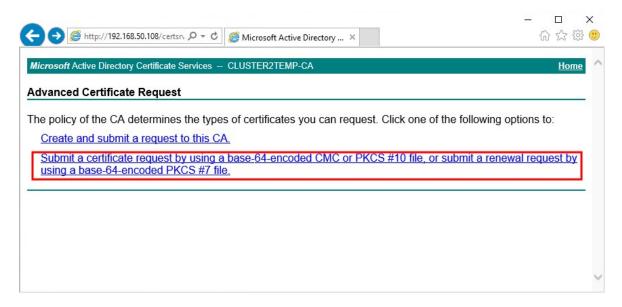


Request a Certificate

Select the certificate type: <u>Web Browser Certificate</u> <u>E-Mail Protection Certificate</u>

Or, submit an advanced certificate request.

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



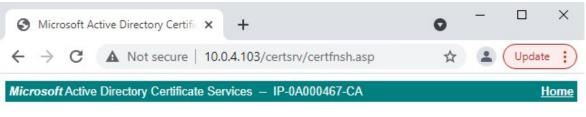
7. Paste the contents of the .req file into the form. If it is required to select a Certificate Template, select **Web Server** from the Certificate Template list.

🗲 🕞 🏉 http	://192.168.50.108/certsn. 🄎 👻 🖉 Microsoft Active Directory 🗴	- □ × 公公 ②
Microsoft Active	Directory Certificate Services CLUSTER2TEMP-CA	Home
Submit a Cert	ificate Request or Renewal Request	
	ved request to the CA, paste a base-64-encoded CMC or PKCS #10 certifi st generated by an external source (such as a Web server) in the Saved Re	
Saved Request:		
	<pre>lWR7EktvnBLYuBQVPGYb+gwd8EfBh9K9Qqvd5fMu: r+5Z7i0E2HZpsBrSldl+u89F0Pi+W/a8/YV7BhAl: nIi7k+ce+EDoHhXkbSD+fHYFbUqaTYUfgU4u5Pq6; 2PmPVkUJGJEUMwfo8rb4xb9taP6ycUZwieLrNWw3] TSXTFWMOJCPMykW2 END NEW CERTIFICATE REQUEST</pre>	
Additional Attribu	ites:	
Attributes:	< >	
-	Submit >	

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



Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.

Your Request Id is 6.

Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with this web browser within 10 days to retrieve your certificate

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.

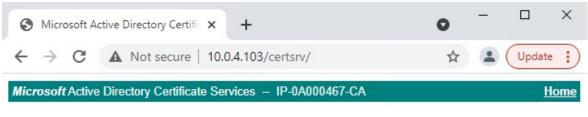
In the **Pending Requests** folder, right-click on the matching Request ID, and from the **All Tasks** list, select **Issue**.

• 🔿 🙋 📰 🙆 🗟 🗊				
Console Root	Request ID	Binary Request	Request Status Code	Actions
 Certification Authority (Local) IP-0A000467-CA 	5	All Tas	sks > View	Attributes/Extensions
Revoked Certificates Issued Certificates		Refres	h Expo	rt Binary Data
Pending Requests Failed Requests		Help	Deny	

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

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.



Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see <u>Active Directory</u> <u>Certificate Services Documentation</u>.

Select a task:

Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

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



Select the certificate request you want to view: <u>Saved-Request Certificate (6/1/2021 1:36:18 PM)</u> 6. Select **DER encoded**, and download the certificate chain.

Attp://192.168.50.108/certsrv P = C	1	口 分 公 锁	× •
Microsoft Active Directory Certificate Services CLUSTER2TEMP-CA		<u>Home</u>	^
Certificate Issued			-
The certificate you requested was issued to you.			
● DER encoded or ○ Base 64 encoded			
DER encoded or Base 64 encoded Download certificate Download certificate chain			
			-
The certnew.p7b download has completed. Open 🔻 Open folder View downloads	×		~

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

↓ ↓ ↓ ↓ Download File Home Share	View		
$\leftarrow \rightarrow \checkmark \uparrow \checkmark$ Thi	is PC > Downloads Name	Date modified	Туре
Cuick access Cuick access Desktop Downloads Documents Pictures	Certnew Open Install Certificate Scan with Windows I Open with	10/26/2021 2:22 PM Defender	PKCS #7 Certificates

8. Accept the security warning if it appears.

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

Welcome to the	e Certifica	ate Import	Wizard	
This wizard helps you o lists from your disk to a			lists, and certific	ate revocation
A certificate, which is is and contains informatic	on used to prote	ct data or to est	ablish secure net	work
connections. A certifica	ite store is the s	ystem area Whe	re ceruncates are	екерт.
Current User				
O Local Machine				
To continue, click Next				

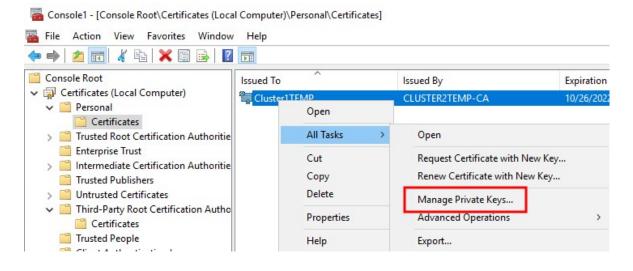
9. Choose a store location. Select **Place all certificates in the following store**, and click the **Browse...** button to open the **Select Certificate Store** window.

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

🗧 🛃 Certificate Import Wizard	
Certificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for	
Automatically select the certificate store based on the type of certificate O Automatically select the certificate store based on the type of certificate O Place all certificates in the following store Certificate store: D Browse	Select Certificate Store × Select the certificate store you want to use. Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Show physical stores OK Cancel
Next Can	cel

- 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.

ODEATOR OWNER		
CREATOR OWNER		
SYSTEM		
Administrators (CLUSTER1	TEMP\Administrator	s)
	Add	Remove
missions for NETWORK RVICE	Allow	Deny
Full control		
Read	\checkmark	
Special permissions		
opeoidi permissions		
special permissions or advan	ced settings.	Advanced

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.

Server Configurator				×
Encryption	Encryption			
Registering servers	It is recommended to secure communication with encryption. Lear	m mo	ore	
Language selection	Server certificate Applies to: management server, recording server, failover server, data collector			
	Encryption: On			
	Narahan v		Details	
	Certificate issued by MS-Organization-P2P-Access [2021]. Expires 5/8/2021			
	Streaming media certificate Applies to clients and servers that retrieve data streams from the recording server Encryption: On			
	Remains		Details	
	Certificate issued by MS-Organization-P2P-Access [2021]. Expires 5/8/2021			
			Apply	

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 85
- Install certificates in a Workgroup environment for communication with the Management Server or Recording Server on page 103

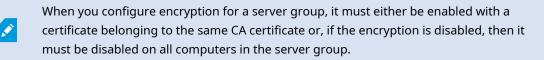
Enable XProtect Event Server encryption

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.



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.

			×
Encryption configuration successful			×
	n. <u>Learn m</u>	ore	
Select certificate	~	Details	
No certificate selected Event server and add-ons Applies to: event server LPR server			
Encryption: On		0.11	
Certificate issued by I Expires 1/8/2022	~	Details	
		Apply	
	Encryption It is recommended to secure communication with encryption Streaming media certificate Applies to clients and servers that retrieve data streams from the recon- server Encryption: Off Select certificate No certificate selected Event server and add-ons Applies to: event server, LPR server Encryption: On	Encryption It is recommended to secure communication with encryption. Learn m Streaming media certificate Applies to clients and servers that retrieve data streams from the recording server Encryption: Off Select certificate No certificate selected Event server and add-ons Applies to: event server, LPR server Encryption: On	Encryption configuration successful Encryption Encryption Streaming media certificate Applies to clients and servers that retrieve data streams from the recording server Encryption: Off Select certificate No certificate selected Event server and add-ons Applies to: event server, LPR server Encryption: On Certificate issued by I Expires 1/8/2022

5. Click Apply.

To complete the enabling of encryption, the next step is to update the encryption settings on each related addon 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:



Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see <u>Active Directory Certificate Services</u> <u>Documentation</u>.

Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> Download a CA certificate, certificate chain, or CRL

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

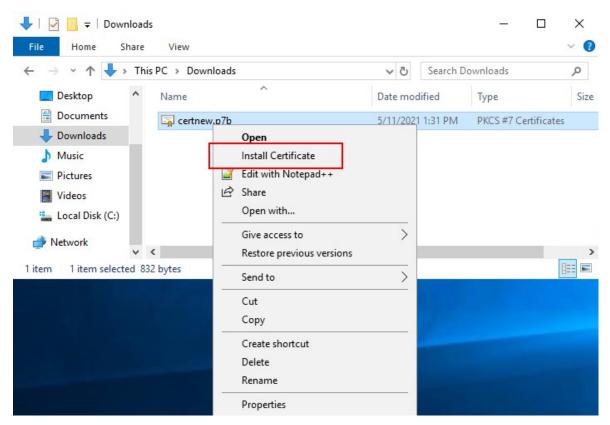
2. Click Download a CA certificate, certificate chain, or CRL.

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

S Microsoft Active Directory Certifi × +	o –		×
← → C ▲ Not secure 10.0.4.103/certsrv/certcarc.asp		*	:
Microsoft Active Directory Certificate Services – IP-0A000467-CA		Н	ome
Download a CA Certificate, Certificate Chain, or CRL			
To trust certificates issued from this certification authority, install this CA certificate.			
To download a CA certificate, certificate chain, or CRL, select the certificate and en	coding met	hod.	
CA certificate:			
Current [IP-0A000467-CA]			
Encoding method:			
● DER ○ Base 64			
Install CA certificate Download CA certificate Download CA certificate chain Download latest base CRL			

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.

🔶 🛷 Certificate Import Wizard

Welcome to the Certificate Import Wizard

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

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

To continue, click Next.

Next

Х

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.

Certificate Import Wizard	
Certificate Store	
Certificate stores are system areas where	e certificates are kept.
the certificate.	cate store, or you can specify a location for store based on the type of certificate
Place all certificates in the following	store
Certificate store:	
	Browse

Mark Connect	Next Consel
Next Cancel	Next Cancel

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

Click Next.

Select Certificate Store	×	
Select the certificate store you want to use.		
	^	tificates are kept.
	ties V	store, or you can specify a location for
<	>	e based on the type of certificate
Show physical stores	cel	re

Cance	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.

pperties	-
Recording server information	
Name:	
Recording server 1	
Description:	
Covers sector 1	~
	~
Host name:	
DATE TO BE ATTAINANT &	
Local web server address:	
https:// k:7563/	
Web server address:	
https://www.recordingserver1.dk:89/	
Time zone:	
(UTC+01:00) Brussels, Copenhagen, Madrid, Paris	
Info 🥑 Storage 👔 Failover 💠 Multicast 🚏 Network	

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.

perties		
Failover server infor	ation	
Name:		
Failover recording s	erver 1	
Description:		
Failover for Record	ng server 1	^
		~
Host name:		
ALC: NO. OF COMPANY	.local	
Local web server a	ldress:	
https://	.local:7563/	
Web server addres	:	
https://www.fai	overrecordingserver1:89/	
UDP port: 8844		
Database location:		
C:\MediaDatabase		
Enable this failo	er server	
Info 💱 Network	🗘 Multicast	

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

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"

Appendix B | Create Server SSL Certificate script

```
# 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
```

Appendix C | Create CA Certificate script

```
# 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/.

