

MOBOTIX HUB – Certificates Guide

V2.03

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	e Management Server or Recording
Server	57
Install Active Directory Certificate Services	74
Install certificates in a domain for communication with the Management S	erver or Recording Server 86 Install
certificates in a Workgroup environment for communication with the Ma	•
or Recording Server	104
Install certificates for communication with the Event Server	126
Import client certificates	129
View encryption status to clients	135
View encryption status on a failover recording server	136
Appendix A Create CA Certificate script	137
Appendix B Create Server SSL Certificate script	138
Appendix C Create Failover Management Server Certificate script	139

Copyright, trademarks, and disclaimer

Copyright © 2023 MOBOTIX AG

Trademarks

MOBOTIX HUB is a registered trademark of MOBOTIX AG.

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.

MOBOTIX AG 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 MOBOTIX 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.

MOBOTIX recommends that you establish a Public Key Infrastructure (PKI) for creating and distributing certificates. A PKI is a set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. In a Windows domain, it's recommended to establish a PKI using the Active Directory Certificate Services (AD CS). If you are unable to build a PKI, either due to having different domains without trust between them or due to not using domains at all, it's possible to manually create and distribute certificates.

WARNING: Creating and distributing certificates manually isn't recommended as a secure way of distributing certificates. If you choose manual distribution, you are responsible for always keeping the private certificates secure. When you keep the private certificates secure, the client computers that trust the certificates are less vulnerable to attacks.

When do you need to install certificates?

First, decide whether your system 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 MOBOTIX HUB VMS system is set up in a Windows Workgroup environment
- Before you install or upgrade to MOBOTIX HUB VMS 2019 R1 or newer, if you want to enable encryption during the installation.
- Before you enable encryption, if you installed MOBOTIX HUB 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 MOBOTIX HUB VMS, secure communication is obtained by using TLS/SSL with asymmetric encryption (RSA). TLS/SSL

uses a pair of keys-one private, one public-to authenticate, secure, and manage secure connections.

A certificate authority (CA) is anyone who can issue root certificates. This can be an internet service that issues root certificates, or anyone who manually generates and distributes a certificate. A CA can issue certificates to web services, that is to any software using https communication. This certificate contains two keys, a private key and a public key. The public key is installed on the clients of a web service (service clients) by installing a public certificate. The private key is used for signing server certificates that must be installed on the server.

Whenever a service client calls the web service, the web service sends the server certificate, including the public key, to the client. The service client can validate the server certificate using the already installed public CA certificate. The client and the server can now use the public and private server certificates to exchange a secret key and thereby establish a secure TLS/SSL connection.

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

See Transport Layer Security for more information about TLS.

In MOBOTIX HUB 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:

- MOBOTIX HUB Desk Client
- Management Client
- · Management Server (for System Monitor and for images and AVI video clips in email notifications)
- MOBOTIX HUB Mobile Server
- MOBOTIX HUB Event Server
- MOBOTIX HUB LPR
- MOBOTIX Open Network Bridge

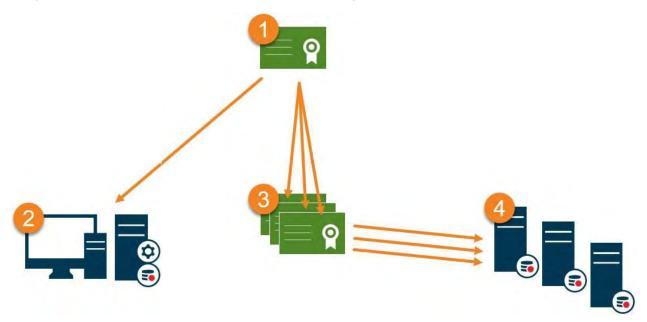
- MOBOTIX HUB DLNA Server
- · Sites that retrieve data streams from the recording server through Milestone Interconnect
- Third-party MIP SDK integrations that support HTTPS

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 MOBOTIX HUB VMS.



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

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 MOBOTIX HUB 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 MOBOTIX HUB 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:

Ì

• MOBOTIX HUB Mobile Server

In MOBOTIX HUB VMS, encryption is enabled or disabled per Mobile Server. You enable or disable encryption either during installation of the MOBOTIX HUB 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 MOBOTIX HUB Mobile client and MOBOTIX HUB 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

8 | Overview of the scenarios and procedures used with certificates

MOBOTIX HUB 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 the Recording Servers. Before you enable encryption, you must install security certificates on the Management Server and all Recording Servers, including Failover Recording Servers.

Third-party or commercial CA certificate

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

See:

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

Domain

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

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

See:

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

Workgroup

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

See:

Install certificates in a Workgroup environment for communication with the Management Server or Recording Server on page 104

MOBOTIX HUB 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 126

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:

- MOBOTIX HUB Desk Client
- Management Client
- Management Server (for System Monitor and for images and AVI video clips in email notifications)
- MOBOTIX HUB Mobile Server
- MOBOTIX HUB Event Server
- MOBOTIX HUB LPR
- MOBOTIX Network Bridge
- MOBOTIX HUB DLNA Server
- Sites that retrieve data streams from the recording server through MOBOTIX 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 129

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. MOBOTIX HUB Mobile will not use installed certificates. MOBOTIX HUB Mobile can only use trusted third-party certificates. If the MOBOTIX HUB servers (Management Server and Recording Server) are installed on computers that are joined to the Domain, and the users who are logging into the Desk 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 129.

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 MOBOTIX HUB 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 MOBOTIX HUB servers use secure encrypted communications and to manage the certificates that the MOBOTIX HUB servers use.

The Server Configurator is installed by default on any computer that hosts an MOBOTIX HUB server. Open

the Server Configurator from:

• The Windows Start menu

or

• The MOBOTIX HUB 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	0	
	DocCert1 Certificate issued by mit-MJT-DC-CA, DC=mit, DC=local. Expires 4/27/2022	Ŷ	Details
	Mobile streaming media certificate Applies to mobile and web clients that retrieve data streams from the server	mobile	
	Encryption: On		
	DocCert1	*	Details
	Certificate issued by m/t-MUT-DC-CA, DC=mit, DC=local. Equires 4/27/2022		
		1	Apply

Use the Server Configurator to choose the certificates that the MOBOTIX HUB 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 MOBOTIX HUB VMS systems.

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

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

Creating and distributing certificates manually

Important to know:

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

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

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

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

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

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

Create CA certificate

On a computer with restricted access and not connected to your MOBOTIX HUB 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.



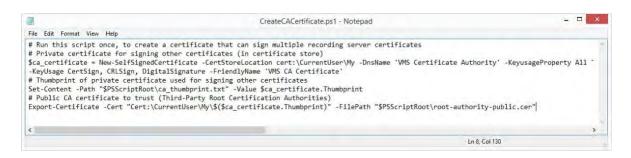
Be aware that when you create certificates in this way, the certificates are related to the computer they are installed on. If the computer name changes, then the VMS will not be able to start until the certificates are created again and re-installed on the computer.

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.



- 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.

II []]] ∓ I					Cert		
Open <u>n</u> ew window	*	Open Window	vs Powe <u>r</u> Shell	. Open •	Select all		
Open command grompt		Open Window	vs PowerShell as administrator	Properties History Open	Select		
Open Windows Powe <u>r</u> Shell							
Delete history				Date modified	Туре	Size	
				04-02-2019 11:31	File folder		
Alla				04-02-2019 11:31	File folder		
Help				04-02-2019 11:31	File folder		
1				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 Script		1 Ki
📕 This PC							

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

Dicar	tory: C:\Certifi	ratar.				
DIFEC		caces				
ode	LastW	riteTime	Length	Name		
a	31-01-2019	09:29	844	root-authority-public.cer		

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.



 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 MOBOTIX HUB client is installed.



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

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



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

F .	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, click Next.	
	©Next Cancel	

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

Certifi	cate Store				
C	ertificate stores are sy	stem areas wher	e certificates an	e kept.	
	indows can automatica e certificate. O Automatically sele				
T	Place all certification	A CALCULATION OF A CALC	AND A PROPERTY OF	and the second	2.22
	Certificate store:	1			
					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.

ø

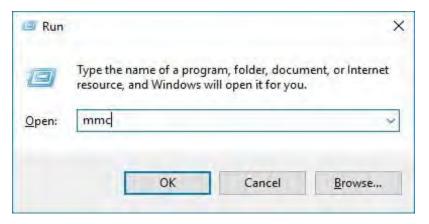
If you receive a security warning that you are about to install a root certificate, click **Yes** to continue.

Completing th	e Certificate Import Wizard
compressing in	e centinente import trizula
The certificate will be in	nported after you dick Finish.
You have specified the	
Certificate Store Sele Content	cted by User Trusted Root Certification Authorities Certificate

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....

Open Ctrl+0 Save Ctrl+S	
Save Ctrl+S	Actions
Save As There are no items to show in this view.	Console Root More Actions
Add/Remove Snap-in Ctrl+M	More Actions
Options	
Recent File	
Exit	

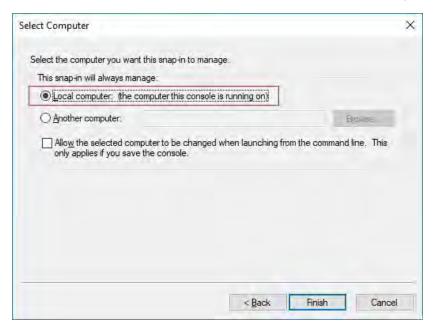
10. Select the **Certificates** snap-in and click **Add**.

vailable <u>s</u> nap-ins: Snap-in	Vendor		Selected snap-ins:	Edit Extensions
and the second second				Eart Extensions
ActiveX Control	Microsoft Cor			Remove
Authorization Manager				
Certificates	Microsoft Cor			Mineub
Component Services	Microsoft Cor			Constraints of the second s
Device Manager	Microsoft Cor	r i		THERE DEAC
Disk Management	Microsoft and		<u>A</u> dd >	
Event Viewer	Microsoft Cor	1		
Folder	Microsoft Cor			
Group Policy Object	Microsoft Cor			
Internet Informatio	Microsoft Cor			
Internet Informatio	Microsoft Cor			
IP Security Monitor	Microsoft Cor	4		Advanced
····		-		
scription:				

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 Computer account 	
	Beck Next > Cancel

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



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

hap-in Vi		1.1	T.	Console Root	- N. C. L.
	/endor	^		Console Root	Edit Extensions
to the state of th	Microsoft Cor		L L	tight Cer uncates (Local Computer	Rendys
a second s	Microsoft Cor				
	Microsoft Cor				
	Microsoft Cor				(MprsTp)
Consultance	Microsoft Cor				There Davo
	Microsoft Cor		Add >		methe Fields
Disk Management M	Microsoft and		Bunning		
Event Viewer M	Microsoft Cor				
i alee	Microsoft Cor				
a set over a set over the set	Microsoft Cor				
Internet Informatio M	Microsoft Cor				
	Microsoft Cor				
IP Security Monitor M	Microsoft Cor	v			Ad <u>v</u> anced

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

Console1 - [Console Root\Certificates (Local Con Eile <u>A</u> ction <u>V</u> iew Fav <u>o</u> rites <u>W</u> indow <u>H</u> e	Construction of the second second	onties/Certificates]			>
🔶 🙍 💼 🗎 🙆 🔒 🖬 📷					
Console Root	Issued To	Issued By	Exp ^	Actions	
Certificates (Local Computer)	10.5.14.40	10.5.14.40	20:	Certificates	
 Personal Trusted Root Certification Authorities Certificates Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Third-Party Root Certification Authorities Trusted People Client Authentication Issuers Preview Build Roots AAD Token Issuer eSIM Certification Authorities Homegroup Machine Certificates Remote Desktop Certificate Enrollment Requests Smart Card Trusted Roots Trusted Devices Web Hosting Windows Live ID Token Issuer 	40.5.6.101 AddTrust External CA Root Baltimore CyberTrust Root	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 GTE CyberTrust Global Root Hotspot 2.0 Trust Root CA - 03	20: 20: 20: 20: 20: 20: 20: 20:	More Actions	
		Microsoft Root Certificate Authori NO LIABILITY ACCEPTED, (c)97 Ve Starfield Class 2 Certification Auth Starfield Services Root Certificate			

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.



1

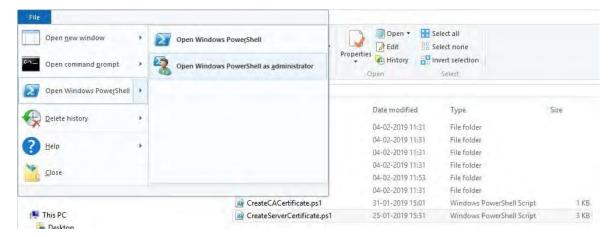
The computer that you use for creating certificates must run Window 10 or Windows Server 2016 or newer.

- 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.

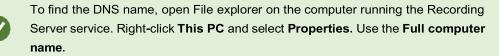


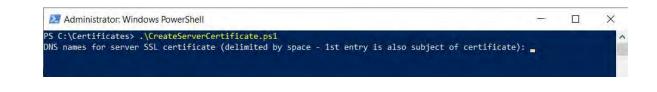
It is very important that the lines break in the same places as in Appendix B. You can add the line breaks in Notepad or alternatively, reopen this PDF with Google Chrome, copy the contents again and paste it into Notepad.

- 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**.





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 MOBOTIX HUB 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

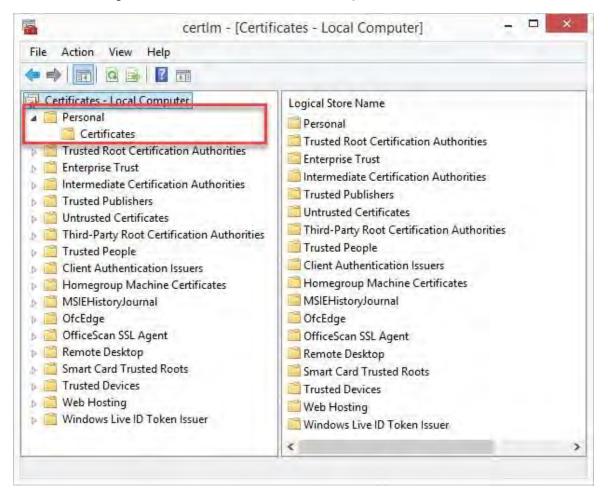
After you created the SSL certificates, install them on the computers that run the server service.

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.



 $\label{eq:linear} \textbf{4.} \quad \textbf{Select to import the certificate in the store of the } \textbf{Local Machine} \text{ and click } \textbf{Next}.$

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.	
	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 Ourrent User Ourrent User

5. Browse to the certificate file and click Next.

Specify the file you want to impo	et .	
Specify the file you want to impo	rt.	
File name:		
5:\Lisers\gis\Documents\My Re	ceived Files/VMS-REC-01.p	Browse
Note: More than one certificate	can be stored in a single fil	le in the following formats
Personal Information Exchang	ge-PKCS #12 (.PFX,.P12)	
Cryptographic Message Synta	ax Standard- PKCS #7 Cert	tificates (.P7B)
Microsoft Serialized Certificate	e Store (.SST)	

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

vate key protection
To maintain security, the private key was protected with a password.
the state of the second st
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.
V Include all extended properties.

 $7. \ \ \mathsf{Place} \ \mathsf{the} \ \mathsf{file} \ \mathsf{in} \ \mathsf{the} \ \mathsf{Certificate} \ \mathsf{Store} : \mathsf{Personal} \ \mathsf{then} \ \mathsf{click} \ \mathsf{Next}.$

Certificate S			ré i l	
Certific	ate stores are sys	stem areas where	certificates are kep	t,
Windov	vs can automatical	lly select a certific	ate store, or you ca	n specify a location for
the cer	tificate.			
OF	Automatically selec	ct the certificate s	tore based on the t	ype of certificate
• F	Place all certificate	s in the following s	store	
1	Certificate store:			
	Personal			Browse

8. Verify the information and click $\ensuremath{\textit{Finish}}$ to import the certificate.

	you dick Finish.
ou have specified the following set	
Certificate Store Selected by User Content File Name	Personal PFX C:\Users\gis\Desktop\VMS-REC-01.pfx

Contract of the

9. The imported certificate appears in the list.

Þ⇒ 2 ╦ 🖹 🙆 🗟 🛛 🖬		
 Certificates - Local Computer Personal Certificates Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Trusted People Client Authentication Issuers Client Authentication Issuers MSIEHistoryJournal OfcEdge OfficeScan SSL Agent Smart Card Trusted Roots Trusted Devices Web Hosting 	Issued To	Issued By Iocalhost VMS Certificate Authority VMS Certificate Authority

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	Request Certificate with New Key
Сору	Renew Certificate with New Key
Delete	Manage Private Keys
Properties	Advanced Operations
Help	Export

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

roup or user names:		
Administrators (Administrat	ors)	
NETWORK SERVICE		
	A <u>d</u> d	Remove
ermissions for NETWORK ERVICE	Allow	Deny
Full control		
Read	D	
Special permissions		
or special permissions or advar	and an Marca	
	and nottings	Advanced

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

Create SSL certificate for the failover management server

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

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

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



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

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



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

 In Notepad, select File -> Save as, name the file CreateFailoverCertificate.ps1 and save it locally in the same folder as the CA certificate:

 $\label{eq:constraint} Example: C: \ CreateFailoverCertificate.ps1.$

- 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	•	Open Windows Pov	verShell	Open •	Select all			
Open command prompt	+	Open Windows Pov	verShell as administrator	Properties	Select			
Open Windows Powe <u>r</u> Shell	*							
A				Date modified	Ту	De	Size	
Delete history	*			04-02-2019 11	31 File	folder		
a				04-02-2019 11	31 File	folder		
Help	*			04-02-2019 11	31 File	folder		
				04-02-2019 11	31 File	folder		
Close				04-02-2019 11	53 File	folder		
				04-02-2019 11	:31 File	folder		
See 2.			CreateCACertificate.ps1	31-01-2019 15	:01 Wi	ndows PowerShell Script		1 K
🖳 This PC		1	CreateServerCertificate.ps1	25-01-2019 15	31 Wi	ndows PowerShell Script		3 KI

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

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

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

Press Enter.

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



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

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

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

Install certificates for communication with the Mobile Server

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

In MOBOTIX HUB VMS, encryption is enabled or disabled per Mobile Server. You enable or disable encryption either during installation of the MOBOTIX HUB 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.



1

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

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

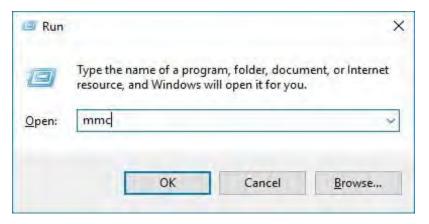
Add a CA certificate to the server

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



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

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



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

Open Ctrl+0 Save Ctrl+S	
Save Ctrl+S	Actions
Save As There are no items to show in this view.	Console Root More Actions
Add/Remove Snap-in Ctrl+M	More Actions
Options	
Recent File	
Exit	

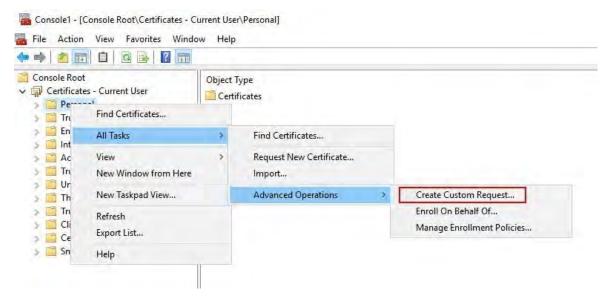
3. Select the Certificates snap-in and click Add.

Click OK.

/ailable snap-ins:		_		Selected snap-ins:	
Snap-in	Vendor	~		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor	T		Certificates - Current Us	Remove
Authorization Manager	Microsoft Cor				Renove
Certificate Templates	Microsoft Cor				-
Certificates	Microsoft Cor				No etto
Certification Authority	Microsoft Cor				al and a second
Component Services	Microsoft Cor		Add >		Manue Canan
Computer Managem	Microsoft Cor		AUU >		
🗄 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
Bar of the second		-		1	
escription:					

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

Operations > Create Custom Request.



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

Click Next.

- 🗆 X

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 New
Next Cancel

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

	- 🗆 X
🙀 Certificate Enrollr	nent
Custom req	uest
Chose an optic	on from the list below and configure the certificate options as required.
Template:	(No template) CNG key -
	Suppress default extensions
Request fo	rmat: O <u>P</u> KCS #10
	<u> <u> <u> </u> <u> </u></u></u>
option is spec	nival is not available for certificates based on a custom certificate request, even when this ified in the certificate template.
	<u>N</u> ext Cancel
an error	uest format depends on the CA. If the wrong format is chosen, the CA will issue when the certificate signing request (CSR) is submitted. Check with the CA 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				and the second se	tify and use a certi	ficate.
TestLal	Domain	.com				
Descrip	tion:					
TestLat	Domain	.com				
					-1	
				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:

General	Subject	Extensions	Private Key	Signature		
The sub can ent	oject of a er inform	certificate is	the user or c	omputer to w	hich the certificate and alternative nan	
Subject	of certifi	cate				
The use	er or com	puter that is	receiving the	certificate		
Subject	name:					
Type:					CN=Test for Do	cs
Count	ry			Add:	O=MJT OU=MJT Lab	
Value:			×	Remove	L=Maple Grove S=MN C=USA	
Alternat	tive name	e;	7		1	
Туре:					Ter	
Direct	ory name					
Value:	1			Ädd>~		
			14	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 fol	lowing ar	e the certific	ate extension	ns for this ce	ertificate type.		^
Key us	sage					^	
The ke	y usage e	extension des	cribes the p	urpose of a (certificate.		
Availal	ole option	15;			Selected options:		
CRL si	the second se				Digital signature Key certificate signing		
Deciph	ner only		_		Key encipherment		
	ier only		A	.dd >			
	reement pudiation			1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1			
	provincio		< R	emove			
			1.7				
	_	_					
☑ Mak	these k	ey usages cr	itical				
Extend	ded Key U	lsage (applic	ation policie	s)		*	
Basic	constrain	ts				*	
							v

Ì

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

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

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

	ties				×
General Subject	Extensions	Private Key	Signature		
Cryptographic	Service Prov	ider			۲
Key options					*
Set the key leng	gth and expor	t options for	the private key.		
Key size: 204	8		~		
Make private	e key exportal	ole		4	
Allow privat	e key to be an	chived			
Strong priva	te key protect	tion			
Select Hash Al	gorithm				~
Select Hash Alg	-	used for this	s request		
and the second sec				1000	
Hash Algorithm	sha256			~	
Hash Algorithn	sha256			~	
Hash Algorithn Select Signatu				~	•
				~	~
				~	*
				~	*

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.

Click Next to use the optio request, and then click Next	ns already selected for this template, or click Details to t.	customize the certificate
Custom request	i STATUS: Available	Details 🔺
Key usage: Application polici Validity period (da		ope or centrates
		Properties

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.

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 proces to your hard disk or removable media. Enter the location and name of click Finish.	
File Name:	
File Name: C:\Users\Administrator\Desktop\CSR6.1.21	Browse,
	Browse
C:\Users\Administrator\Desktop\CSR6.1.21 File format: Base 64	Browse
C:\Users\Administrator\Desktop\CSR6.1.21 File format:	Browse,,,
C:\Users\Administrator\Desktop\CSR6.1.21 File format:	Browse
C:\Users\Administrator\Desktop\CSR6.1.21 File format:	Browse
C:\Users\Administrator\Desktop\CSR6.1.21 File format: Base 64	Browse,

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

1

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.

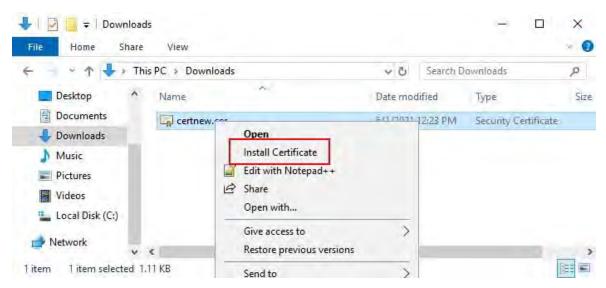
CSR6.1.21 - Notepad

File Edit Format View Help ----BEGIN NEW CERTIFICATE REQUEST----MIIGBAYJKoZIhvcNAQcCoIIF9TCCBfECAQMxDzANBg1ghkgBZQMEAgEFADCCBEoG CCsGAQUFBwwCoIIEPASCBDgwggQ0MGQwYgIBAgYKKwYBBAGCNwoKATFRME8CAQAw AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QLTBBMDAwNDY3DB1JUC0wQTAw MDQ2N1xBZG1pbm1zdHJhdG9yDAdNTUMuRVhFMIIDxqCCA8ICAQEwgg07MIICowIB ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAgMAk10MRQwEgYDVQQHDAtNYXBsZSBH cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UECgwDTUpUMRYwFAYDVQQDDA1U ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7G1/ 5z1YrUG0o4dW1/b3o35rpc00by0UE0K1NWjaIy4YrRPM9HjhKReThbcSnxddj6eR Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ//Zi08bEPobLv8YnWieNDuw lkaJWWRx3mbl/Yz0f1bwZrKFT3nkrXYOFYmZOR19W0J+Iin0BtziwiC8DHt+bxST nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9gC47RP9yMjyuuEtpdR9ERoR qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs18zBATRXkk/kRI+Po6cXNJp Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEAYI3DQIDMQ4WDDEwLjAuMTc3 NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/wQEAwICpDAdBgNVHQ4EFgQU vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCNxUUMTYwNAIBBQwLSVAtMEEw MDA0NjcMGU1QLTBBMDAwNDY3XEFkbWluaXN0cmF0b3IMB01NQy5FWEUwZgYKKwYB BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFMAbwBmAHQAdwBh AHIAZQAgAEsAZQB5ACAAUwB0AG8AcgBhAGcAZQAgAFAAcgBvAHYAaQBkAGUAcgMB ADANBgkqhkiG9w0BAQsFAAOCAQEAqtKb5HCh2a1BD2QcKdFuhVQbNxg+G5wcVkZt 7bXdwVuzoAxd9BFd+uVy4D3TmvXtineT3GVWQbKJCcxRZeTKPBFnHG0SeaYupUrG cX4ySsKR1xGSuOhsfIVa/5NXiIYgYxMhlz3nt2CDw+RNqAp/1gLV2cLsui01y5ib 088po4/b9eiXV7A1DWFy7ecw/7Z20a07Sa0OaRbwzGJ8He1IiVEjfyAt7KLoufAq LkeSaJtjokkJuGPdr+ykjfuCmIF4hSbcOxzVkPCQbiHOwSxDG1kgYHZ8Xru665Q6 0L70gBXCc7tcecDieqbYmp50LJPpqE0DQiYjzg57j3eYIFNYYjAAMAAxggGLMIIB hwIBA4AUvruQxeU1yku5Cem3anpu1cbMEDAwDQYJYIZIAWUDBAIBBQCgSjAXBgkq hkiG9w0BCQMxCgYIKwYBBQUHDAIwLwYJKoZIhvcNAQkEMSIEICk1SKp5MUjMa+vr DU1UXU+V05r1F8bNdM0mDgYfmjCiMA0GCSqGSIb3DQEBAQUABIIBAEjqqe4GSGE4 oZQj0vbWrAP0Ab2u8epFm7ZIMZzsJSzR0z98m+R+1R2mCoqWC0SSafybJ701Jh1y A3eqzDYxAu9p9drJft317sGAERE/i1D3BFvKZZQH0sz0JNRwDp3qByHHzVCULUEI JSOpYvI1s3S23ZYEedQLp35Xy87378zLLGLpgGKTK4teav1IitUJwVCKikL47uyF uOY4XLagwI1WWALsPF1+5ZcVNZMvsgzsbuMEXvjBkFKyhMv49oisgFcLJ1AoMtWn 7Mbg8K6ckbKkVpuvmWThkVTp1W3hIS/i/J0X7c2unA25LxAC/P/LyWhPt/Vk/ogf 06jNaHC/zBQ=

-----END NEW CERTIFICATE REQUEST----

Windows (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

O Current User

Local Machine

To continue, click 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. Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers </th
	Show physical stores OK Cancel

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 MOBOTIX HUB Mobile client and MOBOTIX HUB 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.

Server Configurator			
incryption	Encryption		
egistering servers	It is recommended to secure communica	ition with encryption. Learn	more
anguage selection	Server, certificate Applies to: management server, recording serve collector	er, failover server, data	
	Encryption: On		
	The second se	~	Details
	Camillicate instead by MS-Organization-P2P-Access [202	7], http://di/di/di/di/di/di/di/di/di/di/di/di/di	
	Mobile streaming media certificate Applies to mobile and web clients that retrieve server	data streams from the mobile	
	Encryption: On	0	
	Name	~	Details
	Certificate issued by Exp	pices 5/3/2121	

5. Click Apply.



When you apply certificates, the Mobile Server service restarts.

For more information, you may want to see:

Powershell Process Video.

Whitepaper on certificates with the Mobile Server.

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.



1

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.

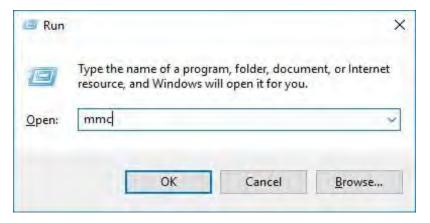
Add a CA certificate to the server

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 MOBOTIX HUB server, open the Microsoft Management Console.



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

Open Ctrl+0 Save Ctrl+S	
Save Ctrl+S	Actions
Save As There are no items to show in this view.	Console Root More Actions
Add/Remove Snap-in Ctrl+M	More Actions
Options	
Recent File	
Exit	

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

Click OK.

/ailable snap-ins:				Selected snap-ins:	
Snap-in	Vendor	~		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor	T		Certificates - Current U	Remove
Authorization Manager	Microsoft Cor				Remove
Certificate Templates	Microsoft Cor				
Certificates	Microsoft Cor				Uporth
Certification Authority	Microsoft Cor				Mary Court
Component Services	Microsoft Cor		Add >		Contrast Contrast
Computer Managem	Microsoft Cor		AUU >		
🖥 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
bar of the				1	
escription:					

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

Operations > Create Custom Request.

Console Root	- Current User	Object Ty		
> Tri	Find Certificates			
> 📫 En	All Tasks	>	Find Certificates	
Ac	View New Window from Here	>	Request New Certificate Import	
Ur 📔 Ur	New Taskpad View		Advanced Operations	Create Custom Request
Tru Cli	Refresh Export List			Enroll On Behalf Of Manage Enrollment Policies
5 🚞 Sn	Help			

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

Click Next.

- 🗆 X

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	

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	n the list below and configure the certificate options as required.
Template:	(No template) CNG key
	Suppress default extensions
Request format:	O <u>P</u> KCS #10
	⊙ <u>c</u> Mc
	not available for certificates based on a custom certificate request, even when this n the certificate template.
	<u>N</u> ext Cancel
an error when	ormat depends on the CA. If the wrong format is chosen, the CA will issue the certificate signing request (CSR) is submitted. Check with the CA 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 TestLabDomain.com	General	Subject	Extensions	Private Key	Signature			
Description:	A friend	ly name	A	1		lentify and	use a certif	icate.
	TestLab	Domain	.com					1
TestLabDomain.com	Descript	tion:						-
	TestLab	Domain	.com					
OK Castal					OK		Cancel	

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:

The subject of a certificate is the user or computer to which the certificate is issu can enter information about the types of subject name and alternative name valu can be used in a certificate. Subject of certificate The user or computer that is receiving the certificate Subject name: Type: Country Add	
The user or computer that is receiving the certificate Subject name: Type: CN=Test for Docs O=MJT	
Subject name: Type: O=MJT	
Type: CN=Test for Docs O=MJT	
O=MJT	
Country V Add OU=MJT Lab	
Value: < Remove L=Maple Grove S=MN C=USA	
Alternative name:	
Туре:	
Directory name 🛛 🗸	
Value: Add	
< Rémiove	

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 fol	lowing an	e the certific	ate extension	ns for this ce	ertificate type.		^
Key us	sage					^	
The ke	y usage e	extension des	cribes the p	urpose of a	certificate.		
Availat	ble option	15:			Selected options:		
CRL si	the second se				Digital signature Key certificate signing		
	ner only		_		Key encipherment		
	ner only		A	.dd >			
	reement epudiation		-		*		
Non re	providence		< R	lemove			
			1.				
⊠ Mak	ce these k	ey usages cr	itical				1
Extend	ded Key U	Jsage (applic	ation policie	es)		¥	Ĩ
	constrain	ts				*	
Basic							1.14

Ì

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

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

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

Certificate Pr	operti	ies				×
General Sub	oject	Extensions	Private Key	Signature		
Cryptogra	phic S	Service Prov	ider			۲
Key option	ns					*
		th and expo	t options for	the private key.		
Key size:	2048			~	L	
Make pr	ivate	key exportal	ble		-	
Allow pr	ivate	key to be ar	chived			
Strong	orivate	e key protect	tion			
Select Has	h Ala	orithm				~
			used for this	request		
Hash Algo	rithm:	sha256			~	
Select Sign	nature	E Format				~
Select Sign	nature	e Format				*
Select Sign	nature	E Format				*
Select Sign	nature	e Format		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.

Click Next to use the optio request, and then click Nex	ns already selected for this template, or click Details to t.	customize the certificate
Custom request	i) STATUS: Available	Details 🔺
Key usage: Application polici Validity period (d.		
		Properties

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.

ertificate Enrollment	
eruncate enrollment	
Where do you want to save the offline request?	
If you want to save a copy of your certificate request or want to proces to your hard disk or removable media. Enter the location and name of click Finish.	
File Name:	
C:\Users\Administrator\Desktop\CSR6.1.21	Browse
C:\Users\Administrator\Desktop\CSR6.1.21 File format:	Browse
C:\Users\Administrator\Desktop\CSR6.1.21	Browse
C:\Users\Administrator\Desktop\CSR6.1.21 File format: Base 64	Browse

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

Ì

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 MOBOTIX HUB 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.

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

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.

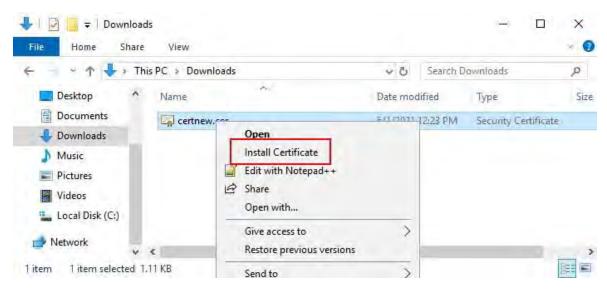
CSR6.1.21 - Notepad

File Edit Format View Help ----BEGIN NEW CERTIFICATE REQUEST----MIIGBAYJKoZIhvcNAQcCoIIF9TCCBfECAQMxDzANBg1ghkgBZQMEAgEFADCCBEoG CCsGAQUFBwwCoIIEPASCBDgwggQ0MGQwYgIBAgYKKwYBBAGCNwoKATFRME8CAQAw AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QLTBBMDAwNDY3DB1JUC0wQTAw MDQ2N1xBZG1pbm1zdHJhdG9yDAdNTUMuRVhFMIIDxqCCA8ICAQEwgg07MIICowIB ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAgMAk10MRQwEgYDVQQHDAtNYXBsZSBH cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UECgwDTUpUMRYwFAYDVQQDDA1U ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7G1/ 5z1YrUG0o4dW1/b3o35rpc00by0UE0K1NWjaIy4YrRPM9HjhKReThbcSnxddj6eR Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ//Zi08bEPobLv8YnWieNDuw lkaJWWRx3mbl/Yz0f1bwZrKFT3nkrXYOFYmZOR19W0J+Iin0BtziwiC8DHt+bxST nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9gC47RP9yMjyuuEtpdR9ERoR qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs18zBATRXkk/kRI+Po6cXNJp Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEAYI3DQIDMQ4WDDEwLjAuMTc3 NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/wQEAwICpDAdBgNVHQ4EFgQU vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCNxUUMTYwNAIBBQwLSVAtMEEw MDA0NjcMGU1QLTBBMDAwNDY3XEFkbWluaXN0cmF0b3IMB01NQy5FWEUwZgYKKwYB BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFMAbwBmAHQAdwBh AHIAZQAgAEsAZQB5ACAAUwB0AG8AcgBhAGcAZQAgAFAAcgBvAHYAaQBkAGUAcgMB ADANBgkqhkiG9w0BAQsFAAOCAQEAqtKb5HCh2a1BD2QcKdFuhVQbNxg+G5wcVkZt 7bXdwVuzoAxd9BFd+uVy4D3TmvXtineT3GVWQbKJCcxRZeTKPBFnHG0SeaYupUrG cX4ySsKR1xGSuOhsfIVa/5NXiIYgYxMhlz3nt2CDw+RNqAp/lgLV2cLsui01y5ib 088po4/b9eiXV7A1DWFy7ecw/7Z20a07Sa00aRbwzGJ8He1IiVEjfyAt7KLoufAq LkeSaJtjokkJuGPdr+ykjfuCmIF4hSbcOxzVkPCQbiHOwSxDG1kgYHZ8Xru66506 0L70gBXCc7tcecDieqbYmp50LJPpqE0DQiYjzg57j3eYIFNYYjAAMAAxggGLMIIB hwIBA4AUvruQxeU1yku5Cem3anpu1cbMEDAwDQYJYIZIAWUDBAIBBQCgSjAXBgkq hkiG9w0BCQMxCgYIKwYBBQUHDAIwLwYJKoZIhvcNAQkEMSIEICk1SKp5MUjMa+vr DU1UXU+V05r1F8bNdM0mDgYfmjCiMA0GCSqGSIb3DQEBAQUABIIBAEjqqe4GSGE4 oZQj0vbWrAP0Ab2u8epFm7ZIMZzsJSzR0z98m+R+1R2mCoqWC0SSafybJ701Jh1y A3egzDYxAu9p9drJft317sGAERE/i1D3BFvKZZQH0sz0JNRwDp3gByHHzVCULUEI JSOpYvI1s3S23ZYEedQLp35Xy87378zLLGLpgGKTK4teav1IitUJwVCKikL47uyF uOY4XLagwI1WWALsPF1+5ZcVNZMvsgzsbuMEXvjBkFKyhMv49oisgFcLJ1AoMtWn 7Mbg8K6ckbKkVpuvmWThkVTp1W3hIS/i/J0X7c2unA25LxAC/P/LyWhPt/Vk/ogf 06jNaHC/zBQ=

-----END NEW CERTIFICATE REQUEST-----

Windows (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

O Current User

Local Machine

To continue, click 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 fo 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	Show physical stores

5. Finish the Install Certificate wizard.

Enable encryption to and from the Management Server

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

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

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



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

Prerequisites:

• A server authentication certificate is trusted on the computer that hosts the management server First,

enable encryption on the management server.

Steps:

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

or

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

Select Details to view Windows Certificate Store information about the selected certif	icate.
--	--------

LOT		Ц
Encryption		
It is recommended to secure communication with encrypti	on. <u>Learn m</u>	ore
Server certificate Applies to: management server, recording server, failover server, dat collector, api gateway, log server	a	
Encryption: Off		
Select certificate	~	
No certificate selected		
Streaming media certificate Applies to clients and servers that retrieve data streams from the rec server	cording	
Encryption: Off		
Select certificate	~	
No certificate selected		
Mobile streaming media certificate Applies to mobile and web clients that retrieve data streams from th server	e mobile	
Encryption: Off		
Select certificate	~	
No certificaite selected		
		Apply
	Encryption Server certificate Applies to: management server, recording server, failover server, data collector, api gateway, log server Encryption: Off Select certificate No certificate selected Streaming media certificate Applies to clients and servers that retrieve data streams from the recording server. Encryption: Off Select certificate No certificate selected Mobile streaming media certificate Applies to mobile and web clients that retrieve data streams from the recording server. Encryption: Off Select certificate	Encryption Server certificate Applies to: management server, recording server, failover server, data collector, api gateway, log server Encryption: Off Select certificate No certificate selected Streaming media certificate Select certificate No certificate No certificate No certificate Select certificate No certificate Select certificate No certificate No certificate Select certificate

5. Click Apply.

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

Install Active Directory Certificate Services

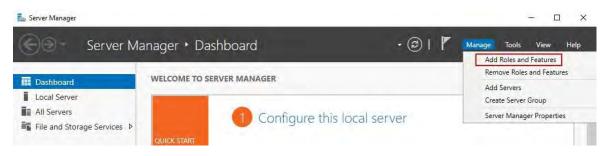
Active Directory Certificate Services (AD CS) is a Microsoft product that performs public key infrastructure (PKI) functionality. It acts as a Server Role that enables you to construct public key infrastructure (PKI) and give open key cryptography, computerized authentication, and advanced mark abilities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

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

- In a domain environment (see Install certificates in a domain for communication with the Management Server or Recording Server on page 86)
- In a Workgroup environment (see Install certificates in a Workgroup environment for communication with the Management Server or Recording Server on page 104)

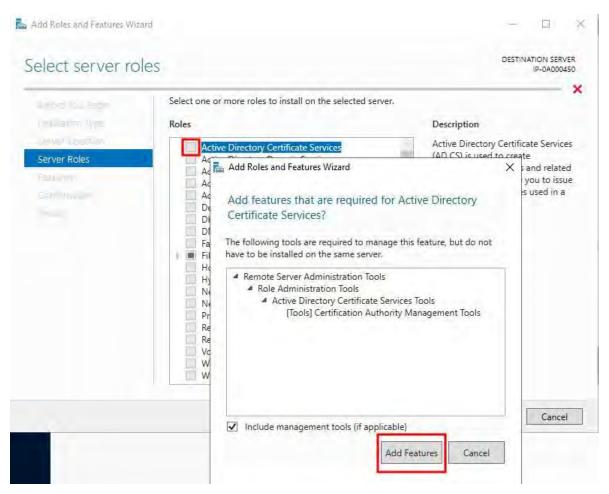
To install AD CS:

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.

Before You Begin	Select the role services to install for Active Directo	ry Certificate Services
Installation Type Server Selection Server Roles Features AD CS Role Services Web Server Role (IIS) Role Services Confirmation	Role services Certification Authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Certification Authority Web Enrollment Network Device Enrollment Service Online Responder	Description Network Device Enrollment Service makes it possible to issue and manage certificates for routers and other network devices that do not have network accounts.

Click Next.

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

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

Select the Notification Flag in the Server Manager application.

_	WELCOME TO SERVE	PMANAGER			DESTINATION SERVER	
1	WELCOWE TO SERVE	IN MANAGER	Installation pro	gress	DESTINATION SERVER (P-0A000467	
		1 Confie		View installation progress		
Services Þ	OUICK START			Feature installation		
		2 Add		Configuration required. Installation succeeded on IP-0A000467.		
		3 Add		Active Directory Certificate Services Additional steps are required to configure Active Directory Certificate Service	+	
	WHAT'S NEW	4 Crea		destination server Configure Active Directory Certificate Services on the destination server		
		5 Con	Land and the second sec	Certification Authority	_	
		3 10	Results	Network Device Enrollment Service Certificate Enrollment Policy Web Service		1 m
	LEARN MORE			Certificate Enrollment Web Service Certification Authority Web Enrollment		
	ROLES AND SERVER			Remote Server Administration Tools Role Administration Tools	.÷	
	AD CS	1		You can close this wizard without interrupting running tasks. View task pr page again by clicking Notifications in the command bar, and then Task D Export configuration settings	ogress or open this Netails.	All Servers 1
	() Manageability	r		experi comgenera aconga		D Manageability
	Events			< Previous Next > CI	ose Cancel	Events

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

 ${\it Click} \ on the link to begin the configuration of the installed services.$

	• © I 🗗
i,	Post-deployment Configura
	Configuration required for Active Directory Certificate Services at IP-0A000467
ſ	Configure Active Directory Certificate Services on the
D	Feature installation
	Configuration required. Installation succeeded on IP-0A000467.
	Add Roles and Features
	Task Details

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**.

and all the			DESTINA	TION SER	VER
Credentials				IP-0A000)450
Credentials	Specify credentials to configure role	e services			
Role Services					
	To install the following role services you must belon	g to the local Admin	istrators grou	p:	
	Standalone certification authority				
	 Certification Authority Web Enrollment Online Responder 				
	To install the following role services you must belon	a to the Enterprise A	dmins aroup		
	 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				

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

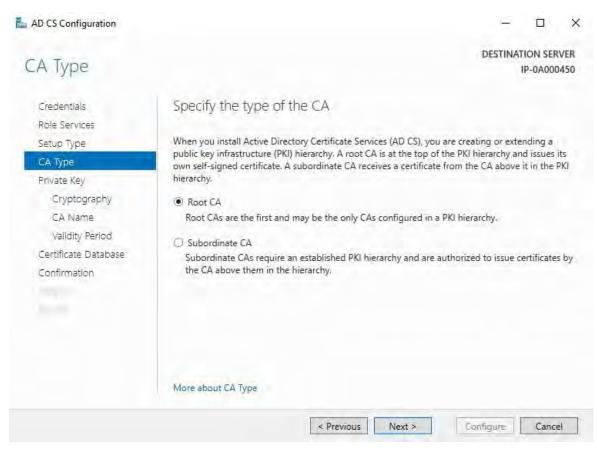
Click Next.

📥 AD CS Configuration		- 🗆 X
Role Services		DESTINATION SERVER IP-0A000450
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation	Select Role Services to configure	
	More about AD CS Server Roles < Previous Next >	Configure Cancel

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

AD CS Configuration	
Setup Type	DESTINATION SERVER IP-0A000450
Credentials Rolé Services	Specify the setup type of the CA
Setup Type CA Type	Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.
Private Key Cryptography CA Name Validity Period Certificate Database Confirmation	 Enterprise CA Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies. 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

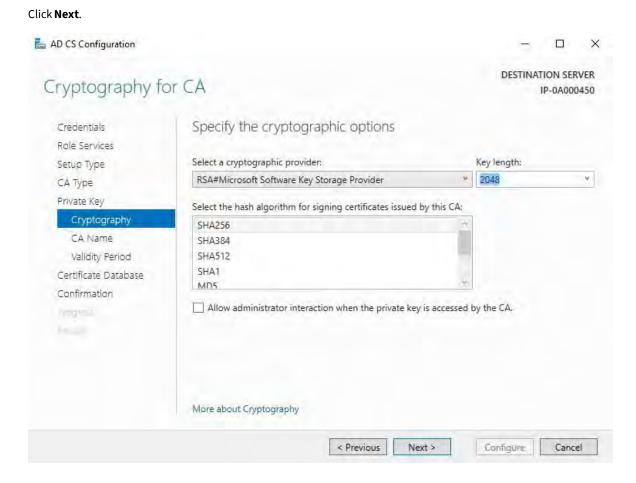
15. In **CA Type**, select the option to install a **Root CA**, and click **Next**.



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



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



18. In **CA Name**, enter the name for the CA and click $\mbox{Next}.$

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

— — >
DESTINATION SERVER IP-0A000450
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.
Common name for this CA:
IP-0A000450-CA
Distinguished name suffix:
Preview of distinguished name:
CN=IP-0A000450-CA
More about CA Name

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

📥 AD CS Configuration						-		×
Validity Period						DESTIN	ATION SEI IP-0A00	
Credentials Role Services Setup Type		ify the validity he validity period fo		e generated	for this certific	cation authority	(CA):	
CA Type	5	Years	*					
Private Key	CA expi	iration Date: 4/27/2	026 3:27:00 PM					
Cryptography CA Name Validity Period Certificate Database		idity period configu ates it will issue.	red for this CA	certificate sl	nould exceed t	the validity perio	od for the	
Confirmation								
	More al	bout Validity Period						
			< Prev	ious I	Next >	Configure	Cano	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.

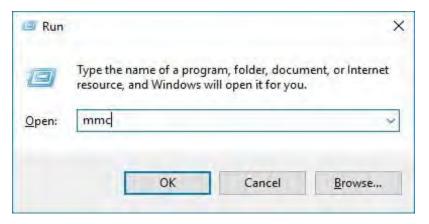


Microsoft provides extensive documentation for Windows Server operating systems, which includes templates for server certificates, installation of the CA, and certificate deployment can be found in Microsoft's Server Certificate Deployment Overview.

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 MOBOTIX HUB server, open the Microsoft Management Console.



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

Open Ctrl+O Save Ctrl+S Save As There are no items to show in this view. Add/Remove Snap-in Ctrl+M Options More Actions Recent File Image: Ctrl+S Exit Image: Ctrl+S	Save As Add/Remove Snap-in Ctrl+M Options Recent File	New Ctrl Open Ctrl		
Save As Intere are no items to show in this view. Add/Remove Snap-in Ctrl+M Options Recent File	Save As Intereare no items to show in this view. Add/Remove Snap-in Ctrl+M Options Recent File		+S	
Add/Remove Snap-in Ctrl+M Options Recent File	Add/Remove Snap-in Ctrl+M Options Recent File	Save As	There are no items to show in this view.	
Recent File	Recent File	Add/Remove Snap-in Ctrl	M	More Actions
		Options		
Exit		Recent File		
		Exit		

3. Select the Certificates snap-in and click Add

				Selected snap-ins:	
nap-in	Vendor	^		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor			Certificates (Local Computer)	71004
Authorization Manager	Microsoft Cor				Rendire
the second se	Microsoft Cor				
Component Services	Microsoft Cor				(Mine Ub)
Computer Managem	Microsoft Cor	11	_		
Device Manager	Microsoft Cor		Add >		THEYE DEVIC
Disk Management	Microsoft and		- AUG 2		
Event Viewer	Microsoft Cor				
Folder	Microsoft Cor				
Group Policy Object	Microsoft Cor				
Internet Informatio	Microsoft Cor				
IP Security Monitor	Microsoft Cor				
IP Security Policy M	Microsoft Cor	4			Advanced
1		-	1		1

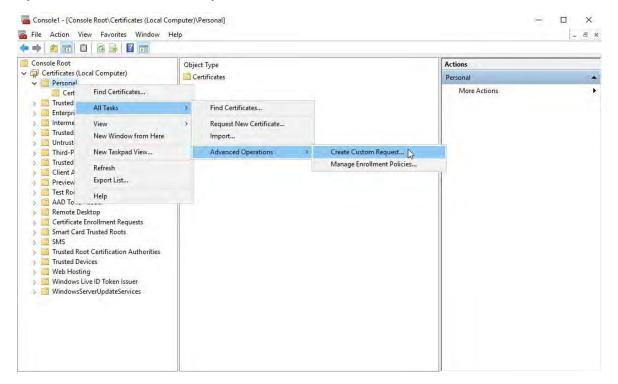
4. In Certificates snap-in, select Computer account.

Certificates snap-in	×
This snap-in will always manage certificates for:	
O My user account	
O Service account	
Computer account	
	Next > Cancel

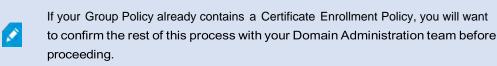
- 5. In Select Computer, select Local computer.
 - Select Finish, then OK.

elect Computer		
Select the computer you want this snap	in to manage.	
This snap-in will always manage:		
Docal computer: (the computer the computer the computer)	nis console is running on)	
O Another computer:	Evolution	
only applies if you save the conso	e changed when launching from the command line. This ole.	
only applies if you save the conso	ole.	
only applies if you save the conso	ole.	

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



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



Click Next.

- 🗆 X

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 Cancel
	Litext Conce

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

ustom request	
hose an option fron	n the list below and configure the certificate options as required.
Template:	(No template) CNG key
	Suppress default extensions
Request format:	O <u>P</u> KCS #10
	● <u>C</u> MC
	not available for certificates based on a custom certificate request, even when this the certificate template.
ption is specified in	the certificate template.

Next

Cancel

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

-	X

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	i) STATUS: Available	Details A
The following options	describe the uses and validity period that apply to this	type of certificate:
Key usage:	Digital signature Key certificate signing Key encipherment	
Application polici		
Validity period (da	ys):	
and the second		Properties

94	Install	certificates	in	a domain	for	communication	with	the	Management	Server	or	Recording	Serve	r
----	---------	--------------	----	----------	-----	---------------	------	-----	------------	--------	----	-----------	-------	---

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

	-					
			Private Key	the second se		
A friend	lly name	and descript	ion will make	e it easier to ide	ntify and use a cer	tificate.
Friendly	/ name:					
TestLa	Domain	com				
Descrip	tion:					
TestLa	Domain	.com				
					Cancel	

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

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

General Sub	oject Extension	ns Private Key	Signature	
can enter in can be used Subject of c The user or	formation abo in a certificate ertificate computer that	ut the types of	subject name	hich the certificate is issued. You and alternative name values that
Subject nam	ne	-		CN=MJT-12A
Type: Common	name	-	Add >	EN SULL OF A
Value	nanne		1	
(eine		×	Remove	
Alternative	name			
Туре:				
Directory r	name	¥		
Value:			Add≥	
		с.	Remove	
				1

12. 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 the certific	te extensions for this certificate type.	^
Key usage	Ŷ	
Extended Key Usage (applic	ation policies)	
certificate can be used. Selec certificates issued by this ter Available options: Chent Authentication Code Signing Secure Email Time Stamping Microsoft Trust List Signin Microsoft Time Stamping IP security end system IP security tunnel termina	enhanced key usage in Windows 2000) defines how a t the application policy required for valid signatures of nplate. Selected options: Server Authenticotion Add > < Remove	
IP security user	د س » sage critical	
		~

Click OK.

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

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

	Propertie					
Seneral S	ubject	Extensions	Private Key	Signature		
Cryptog	raphic S	ervice Prov	ider			۲
Key optio	ons					*
		h and expo	rt options fo	r the private key	1.	
Key size:	2048				*	
Make	private k	ey exporta	ble			
			17.00			
Allow	private k	cey to be an	cnived			
		key to be a				
Strong	, private	key protec				*
Select Ha	ash Algo	key protec		is request		•
Select Ha	ash Algo	key protec prithm rithm to be	tion	s request	~	•
Select Ha	ash Algo	key protec prithm rithm to be	tion	s request	Ŷ	*
Select Ha Select Ha Select Ha Hash Alg	ash Algo ash Algo ash Algo ash rithm:	key protec prithm rithm to be sha256	tion	is request	×	*
Select Ha	ash Algo ash Algo ash Algo ash rithm:	key protec prithm rithm to be sha256	tion	s request	×	*
Select Ha Select Ha Select Ha Hash Alg	ash Algo ash Algo ash Algo ash rithm:	key protec prithm rithm to be sha256	tion	is request	~	*
Select Ha Select Ha Select Ha Hash Alg	ash Algo ash Algo ash Algo ash rithm:	key protec prithm rithm to be sha256	tion	is request	×	*

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

16. Click Finish.

rtificate Enrollment	
Where do you want to save the offline request?	
lf you want to save a copy of your certificate request or want to pr to your hard disk or removable media. Enter the location and nam click Finish.	rocess the request later, save the reque the of your certificate request, and then
File Name: C:\Users\Administrator\Desktop\CSR6.1.21	Browse
	E. Drowsen
File format:	
File format:) Base 64) Binary	
🖲 Base 64	
🖲 Base 64	
🖲 Base 64	Finish Can

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

1

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

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

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

107Test1 - Notepad	-		×
File Edit Format View Help			
File Edit Format View Help BEGIN NEW CERTIFICATE REQUEST MIIF2AYJKoZIhvcNAQcCoIIFyTCCBcUCAG CCsGAQUFBwwCoIIEEASCBAwwggQIMGYwZA AwIBATFHMEUGCSsGAQQBgjcVFDE4MDYCAG UjFURU1QXEFkbWluaXN0cmF0b3IMB01NQ AgEAMBcxFTATBgNVBAMMDENsdXN0ZXIxVF ggEPADCCAQoCggEBAKVp0982yi05tcnypa dVMVTSU9s9rTMWmUDzP+zLumOmC6gCWI05 ZktV8ut805gi46dkQ4MD71btX6mnjjUB25 zczK1yUZmY576IBwf6LZMujXbNDD5ZXzdH JN2d0SZms4Utj21DekFde3BsENvcvk0/PF bqL+Zy4pEPIjKnTwM1IyPmsXyw7gx6CrTF Nw0CAzEOFgwxMC4wLjE0MzkzLjIwRQYJKK cjFURU1QDBpDTFVTVEVSMVRFTVBcQWRtak hkiG9w0BCQ4xUzBRMBMGA1UdJQQMMAoGCC MAwwCgYIKwYBBQUHAwEwHQYDVR00BBYEFC CisGAQQBgjcNAgIxWDBWAgEAHk4ATQBpAC	QMxDzANBglghkgBZQMEAgEF AIBAgYKKwYBBAGCNwoKATFT QUMDENsdXN0ZXIxVEVNUAwa ySFWEUwggOYoIIDIAIBATCC EVNUDCCASIwDQYJKoZIhvcN aTujsFBe9jwOyRp+c5N00xf SRgiT+dLjOvq+Z6AUWC1H+W 94Xwf8yUVP1Be0dkfqjUVnn nG3pggarNdzHvg0RIJvro4I HZk8b8Bww050+ya3tk7jDbv w8ntqECAwEAAaCCAS8wHAYKI wYBBAGCNxUUMTgwNgIBBQwM wSpc3RyYXRvcgwHTU1DLkVYI CsGAQUFBwMBMBsGCSsGAQQB DBsTd6/Hpi6c18h5HHq88hW	MFECAQ Q0xVU1 A40wgg AQEBBQ BOcN0D VUsaVb 5EAYzH J0rM6E wOa1VX KwYBBA Q2x1c3 RTBgBg gjcVCg c911MG	Aw RF J1 AD JC JC SJ GC R1 Q0 YG
AHCAYQByAGUAIABLAGUAeQAgAFMAdABvAH AHIDAQAwDQYJKoZIhvcNAQELBQADggEBAH OAPtDKNDGskV/dq6rqgpYEKiQfWZeSndE0	HIAYQBnAGUAIABQAHIAbwB2 FGoQLCtyivOXG0T0U4MS9Vnl	AGKAZA USØsQU	B1 InN
XjUze/+WIiZifGFnkMKYwrzKgx7qIr m3dWazix8dSVOQIRZ3Lr7yXg9iiF49	Undo	yuztoi	
EX7yVZFyEAs/6uoApcKXc2KPgBP8aHe Tp4XCYYiuyw/+iHqyNca2fvIIm8Hpb(Cut		2
izCCAYcCAQOAFOBsTd6/Hpi6c18h5H FwYJKoZIhvcNAQkDMQoGCCsGAQUFBw	Copy Paste		
OY6dr8BzietMf5QwmoRNzq8MRGSQiN:	Delete		
+q73I6NKKLzg7ROhm16Xj7tL4Id2iV 1WR7EktvnBLYuBQVPGYb+gwd8EfBh9P	Select All		
r+5Z7i0E2HZpsBrSldl+u89F0Pi+W/a	Right to left Reading order		
nIi7k+ce+EDoHhXkbSD+fHYFbUqaTYU 2PmPVkUJGJEUMwfo8rb4xb9taP6ycU T8XTFWM0JCPMykW2	Show Unicode control characters Insert Unicode control character	>	3
END NEW CERTIFICATE REQUES	Open IME		~
<	Reconversion		8 16

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.

Update :
1

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.

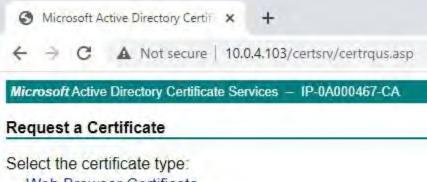
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

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.



Web Browser Certificate E-Mail Protection Certificate

Or, submit an advanced certificate request.

 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.

Microsoft Active	Directory Certificat	e Services – CLUSTER2TEMP-CA	Home
Submit a Cert	ificate Reques	t or Renewal Request	
		the CA, paste a base-64-encoded CMC or PKCS #10 an external source (such as a Web server) in the Sav	
	r+527i0E2H2ps nIi7k+ce+EDoH 2PmPVkUJGJEUM TSXTFWM0JCPMy	BQVPGYb+gwd8EfBh9K9Qgvd5fMu: BrSldl+u89F0Pi+W/a8/YV7BhAl: hXkbSD+fHYFDUgaTYUfgU4u5Pg6: wfo8rb4xb9taP6ycUZwieLrNWw31 kW2 CERTIFICATE REQUEST	
Additional Attrib	utes:		
Attributes:	4	2	

7. Click Submit.

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

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

Install the certificate manually

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

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

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

1.

Certificate Import Wizard

Welcome to the Certificate Import Wizard	
This wizard helps you copy certificates, certificate trust lists, and certificate revoc lists from your disk to a certificate store.	ation
A certificate, which is issued by a certification authority, is a confirmation of your i and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	dentity
Store Location	
Current User	
O Local Machine	

X

To continue, click 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 the certificate.	for
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.
	Show physical stores

- 5. Finish the Install Certificate wizard.
- 6. Go to the Microsoft Management Console (MMC) certificates snap-in.
- 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]

🗢 🔿 🙍 💼 🔏 🖬 🗙 🗟 🚱				
Console Root	Issued To	~	Issued By	Expiration
Certificates (Local Computer) Orersonal Certificates	Cluster17	EMD Open	CLUSTER2TEMP-CA	10/26/202
🔉 🚞 Trusted Root Certification Authoritie		All Tasks	Open	
 Enterprise Trust Intermediate Certification Authoritie Trusted Publishers 		Cut Copy	Request Certificate with Ne Renew Certificate with New	
 Untrusted Certificates Third-Party Root Certification Author 		Delete	Manage Private Keys	
Certificates		Properties Help	Advanced Operations Export	,

8. Verify that the account that is running the MOBOTIX HUB 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, MOBOTIX HUB software uses the NETWORK SERVICE account. In a domain environment, service accounts are commonly used to install and run MOBOTIX HUB 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

1

- · 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			
legistering servers	It is recommended to secure communication with encryptio	n. <u>Learn m</u>	nore	
anguage selection	Server certificate Applies to: management server, recording server, failover server, data collector			
	Encryption: On			
	Concession in the local data and	4	Details	
	Camplicate issued by MS-Organization-P29-Actess (2021), Expires 3/8/2021			
	Streaming media certificate Applies to clients and servers that retrieve data streams from the reco server	rding		
	Encryption: On			
	Teaching and the second s	4	Details	
	Certificate Instead by MS-Organization 8(9). Access (2021), Instead 578/2021			
			Apply	
			Арріу	

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.

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

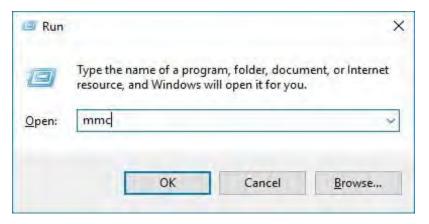
Install certificates in a Workgroup environment for communication with the Management Server or Recording Server

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 MOBOTIX HUB server, open the Microsoft Management Console.



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

New Ctrl+N Open Ctrl+C		1
Save Ctrl+S	Name	Actions
Save As	There are no items to show in this view.	Console Root More Actions
Add/Remove Snap-in Ctrl+M		More Actions
Options		
Recent File		
Exit		

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

Click **OK**.

lable snap-ins:				Selected snap-ins:	-
ap-in	Vendor	$(\Delta \cdot)$		Console Root	Edit Extensions.,
ActiveX Control	Microsoft Cor				
Authorization Manager		10			Remove.
Certificates	Microsoft Cor	Ξ			
Component Services	Microsoft Cor	1			MoveUp
Computer Managem					
Device Manager	Microsoft Cor		1		Move Down
Disk Management	Microsoft and		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	<u></u>			Advanced
IP Security Policy M	Microsoft Cor	~			Advanced
motion:					
- Kasa	ows you to browse				

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

Certificates	- Current User	Object T	Гуре ficates		
Tri	Find Certificates				
En En	All Tasks	>	Find Certificates		
📄 Ac	View	>	Request New Certificate		
Tri Ur	New Window from Here		Import		
Th	New Taskpad View		Advanced Operations	[Create Custom Request
Tri Tri	Refresh				Enroll On Behalf Of
Cli	Export List				Manage Enrollment Policies
📔 Sn	Help				

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

Click Next.

- 🗆 X

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	

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

ertificate Enrollment		
Custom request		
Chose an option from	the list below and configure the certificate options as rea	quired.
Template:	(No template) CNG key	-
	<u>Suppress</u> default extensions	
Request format:	○ <u>P</u> KCS #10	
	● <u>c</u> mc	
	not available for certificates based on a custom certificate the certificate template.	e request, even when this
		Next Car

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

Certificate Information		
Click Next to use the options already request, and then click Next.	r selected for this template, or click Details to cu	stomize the certifica
Custom request	i) STATUS: Available	Details
The following options describe Key usage: Application policies: Validity period (days):	the uses and validity period that apply to this ty	pe of certificate: 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 Key	Signature		
A friend	lly name			and the second se	ify and use a certi	ficate.
	name:	_				
TestLak	Domain.	com				
Descript	tion:					
TestLat	Domain.	.com				
				OK	Caricel	Apply

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.

General	Subject	Extensions	Private Key	Signature	
can enter can be us Subject o The user	r inform sed in a of certific or comp	ation about certificate. cate		subject name	hich the certificate is issued. You and alternative name values that
Subject r Type:	name:				CN=MJT-12A
1	on name			Add >	and a second second
Value:				Remove	
Alternati	ve name	2	1		
Туре:			-		
Directo	ry name		•		
Value:				≤bbA	
			E	Remove	

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

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 the certific	ate extensions for this certificate type.	^
Key usage	v	
Extended Key Usage (applie	ation policies)	
	d enhanced key usage in Windows 2000) defines how a ct the application policy required for valid signatures of mplate. Selected options: Server Authentication	
Secure Email Time Stamping Microsoft Trust List Signii Microsoft Time Stamping IP security end system IP security tunnel termina IP security user	Add > < Remove	
Make the Extended Key U		~

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

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

	es		>
General Subject	Extensions Private Key Signature		
Cryptographic S	ervice Provider		۲
Key options			*
Set the key lengt	h and export options for the private key.		
Key size: 2048		~	
Make private	ey exportable		
Allow private	key to be archived		
Strong private	key protection		
Select Hash Algo	orithm		
SCIECCI IDSH MIG			~
	rithm to be used for this request		*
		~	*
Select Hash Algo		>	*
Select Hash Algo	sha256	~	*
Select Hash Algo Hash Algorithm:	sha256	~	*
Select Hash Algo Hash Algorithm:	sha256	~	*
Select Hash Algo Hash Algorithm:	sha256	~	*

- 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.

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 pro to your hard disk or removable media. Enter the location and name click Finish.	
File Name:	
C:\Users\Administrator\Desktop\CSR6.1.21	Browse
C:\Users\Administrator\Desktop\CSR6.1.21 File format:	Browse.,.
C:\Users\Administrator\Desktop\CSR6.1.21	Browse
C:\Users\Administrator\Desktop\CSR6.1.21 File format:	Browse
C:\Users\Administrator\Desktop\CSR6.1.21 File format:	Browse.,
C:\Users\Administrator\Desktop\CSR6.1.21 File format:	Browse
C:\Users\Administrator\Desktop\CSR6.1.21 File format:	Browse

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

Ì

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

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

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

107Test1 - Notepad	- [X C	
File Edit Format View Help			
BEGIN NEW CERTIFICATE REQUEST MIIF2AYJKoZIhvcNAQcCoIIFyTCCBcUCAQ CCsGAQUFBwwCoIIEEASCBAwwggQIMGYwZA AwIBATFHMEUGCSsGAQQBgjcVFDE4MDYCAQ UjFURU1QXEFkbWluaXN0cmF0b3IMB01NQy AgEAMBcxFTATBgNVBAMMDENsdXN0ZXIxVF ggEPADCCAQoCggEBAKVp0982yi05tcnypa dVMVTSU9s9rTMWmUDzP+zLumOmC6gCWI05 ZktV8ut805gi46dkQ4MD71btX6mnjjUB25 zczK1yUZmY576IBwf6LZMujXbNDD5ZXzdH JN2d0SZms4Utj21DekFde3BsENvcvk0/PF bqL+Zy4pEP1jKnTwM1IyPmsXyw7gx6CrTw Nw0CAzEOFgwxMC4wLjE0MzkzLjIwRQYJKw cjFURU1QDBpDTFVTVEVSMVRFTVBcQWRtaw	QMxDzANBglghkgBZQMEAgEFADC AIBAgYKKwYBBAGCNwoKATFTMFE QUMDENsdXN0ZXIxVEVNUAwaQ0x ySFWEUwggOYoIIDIAIBATCCA40 EVNUDCCASIwDQYJKoZIhvcNAQE aTujsFBe9jwOyRp+c5N00xf8Oc 5RgiT+dLjOvq+Z6AUWC1H+WVUs 94Xwf8yUVP1Be0dkfqjUVnn6EA nG3pggarNdzHvg0RIJvro4IJ0r HZk8b8Bww050+ya3tk7jDbvw0a w8ntqECAwEAAaCCAS8wHAYKKwY wYBBAGCNxUUMTgwNgIBBQwMQ2x W5pc3RyYXRvcgwHTU1DLkVYRTB	CAQAw VU1RF wggJ1 BBQAD N0Dyg aVbJc YzHdS M6EsJ 1VXE9 BBAGC 1c3R1 gBgkq	
hkiG9w0BCQ4xUzBRMBMGA1UdJQQMMAoGC0 MAwwCgYIKwYBBQUHAwEwHQYDVR00BBYEF0 CisGAQQBgjcNAgIxWDBWAgEAHk4ATQBpA0 AHcAYQByAGUAIABLAGUAeQAgAFMAdABvAH AHIDAQAwDQYJKoZIhvcNAQELBQADggEBAH OAPtDKNDGskV/dq6rqgpYEKiQfWZeSndE0 XjUze/+WIiZifGFnkMKYwrzKgx7qIr m3dWazix8dSV0QIRZ3Lr7yXg9iiF49-	DBsTd6/Hpi6c18h5HHq88hWc91 GMAcgBvAHMAbwBmAHQAIABTAG8 HIAYQBnAGUAIABQAHIAbwB2AGk FGoQLCtyivOXG0T0U4MS9VnUS0	1MGYG AZgB0 AZAB1 sQUnN	
EX7yVZFyEAs/6uoApcKXc2KPgBP8aHe Tp4XCYYiuyw/+iHqyNca2fvIIm8Hpb(izCCAYcCAQOAFOBsTd6/Hpi6c18h5HH FwYJKoZIhvcNAQkDMQoGCCsGAQUFBw OY6dr8BzietMf5QwmoRNzq8MRGSQiN1 +q73I6NKKLzg7ROhm16Xj7tL4Id2iV	Cut Copy Paste Delete	2 3 4 1	
1WR7EktvnBLYuBQVPGYb+gwd8EfBh9 r+5Z7iOE2HZpsBrSldl+u89F0Pi+W/a nIi7k+ce+EDoHhXkbSD+fHYFbUqaTV 2PmPVkUJGJEUMwfo8rb4xb9taP6ycU T8XTFWM0JCPMykW2 END NEW CERTIFICATE REQUES	Select All Right to left Reading order Show Unicode control characters Insert Unicode control character Open IME	× 3	
4	Reconversion	8.3	sī.

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.



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> <u>Download a CA certificate, certificate chain, or CRL</u>

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

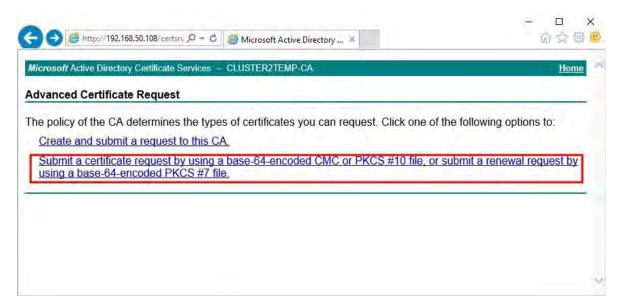


Request a Certificate

Select the certificate type: Web Browser Certificate E-Mail Protection Certificate

Or, submit an advanced certificate request.

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



 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.

	p;//192,168,50,108/certsr			
Microsoft Active	Directory Certificate S	ervices - CLUSTER2TEMP	-CA	Home
Submit a Cer	tificate Request o	r Renewal Request		
	est generated by ar		ncoded CMC or PKCS #10 co as a Web server) in the Save	ertificate request or PKCS #7 d Request box.
	<pre>1 r+5Z7i0E2HZpsBr t nIi7k+ce+EDoHhX 2PmPVkUJGJEUMwf TSXTFWM0JCPMykW</pre>	VFGYD+gwd3EfBh9K9Qqvd5 Sldl+u89F0P1+W/a8/YV7B kbSD+fHYFbUqaTYUfgU4u5 S8rb4xb9taP6ycUZwieLrN 2 RTIFICATE REQUEST	hAl. Pg6	
dditional Attrib	outes:			
Attributes		5		
		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



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).

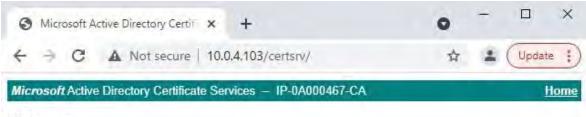
- 1. Open the Microsoft Management Console (MMC).
- 2. Navigate to the Certificate Authority snap-in.
- 3. Expand the Certificate Authority object.

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

Request ID	Binary Request	Request Statu	is Code	Actions
5	All Ta	sks 🤌		tributes/Extensions
	Refres	ih		Binary Data
	Help			1
	a service and a service of the servi	All Tar	arcon ur an All Tasks → All Tasks → Refresh	All Tasks > View At Refresh

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.

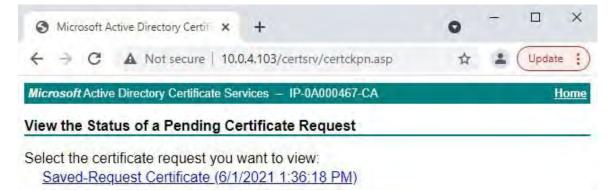
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

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.



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

Microsoft Activ	e Directory Certificate Services -	CLUSTER2TEMP-CA			Home
ertificate Is	sued				
he certificate	e you requested was issued	to you.			
Dente De	DER encoded or OBase (ownload certificate	64 encoded			
	Winded Contricate Criain				
		mpleted. Or	-	 View downloads	

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

	nloads hare View			
< - · ↑ ↓ ;	This PC > Dow	nloads		
1.0.1	Name	~	Date modified	Туре
 Quick access Desktop Downloads 	* Certne	Open Install Certificate	10/26/2021 2:22 PM	PKCS #7.Certificates
 Documents Pictures 	*	Scan with Windows Defende Open with	r	

8. Accept the security warning if it appears.

Select to install the certificate for the current user 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

Current User

O Local Machine

To continue, dick Next.

Next	Cancel
14600	Carreer

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

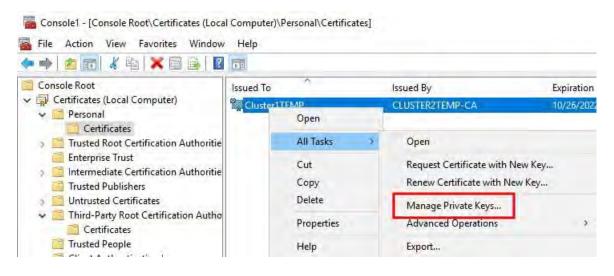
the **Personal** certificate store and click **OK**.

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

Click	Next.	
÷	🔄 Certificate Import Wizard	8
	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. O Automatically select the certificate store based on the type of certificate	Select Certificate Store
	Place all certificates in the following store Certificate store:	Select the certificate store you want to use.
	Browse	Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates
		Show physical stores
	Next	ancel

- 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 MOBOTIX HUB 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, MOBOTIX HUB software uses the NETWORK SERVICE account.

EWIP WUMINISTATOR	5)
Add	Remove
Allow	Deny
	Allow

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		9		×
Encryption	Encryption			
egistering servers	It is recommended to secure communication with encryptic	on. <u>Learn m</u>	nore	
anguage selection	Server certificate Applies to: management server, recording server, failover server, data collector			
	Encryption: On			
	Energies .	4	Details	
	Carolicate issued by MS-Organization-P29-Acteus (2021), Explores 5/8/2021			
	Streaming media certificate Applies to clients and servers that retrieve data streams from the reco server	ording		
	Encryption: On			
	Teaching Street	*	Details	
	Cartillicate instead by MS-Organization 9(9). Access (2021), hyperes 5(0/2021			
			Apply	1

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.



Ì

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 (Desk Client and Management Client) and the MOBOTIX HUB LPR plug-in must be updated to at least version 2022 R1.

HTTPS is only supported if every component is updated to at least version 2022 R1.

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

- Install third-party or commercial CA certificates for communication with the Management Server or Recording Server on page 57
- Install certificates in a domain for communication with the Management Server or Recording Server on page 86
- Install certificates in a Workgroup environment for communication with the Management Server or Recording Server on page 104

Enable MOBOTIX HUB Event Server encryption

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



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

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



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

Prerequisites:

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

First, enable encryption on the event server.

Steps:

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

or

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

× Server Configurator Encryption configuration successful Encryption **Registering servers** Encryption It is recommended to secure communication with encryption. Learn more Language selection Streaming media certificate Applies to clients and servers that retrieve data streams from the recording server Encryption: Off \cap Select certificate... No certificate selected Event server and add-ons Applies to: event server, LPR server Encryption: On Details Certificate issued by I Expires 1/8/2022 Apply

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

5. Click Apply.

To complete the enabling of encryption, the next step is to update the encryption settings on each related add-on 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> <u>Download a CA certificate, certificate chain, or CRL</u>

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

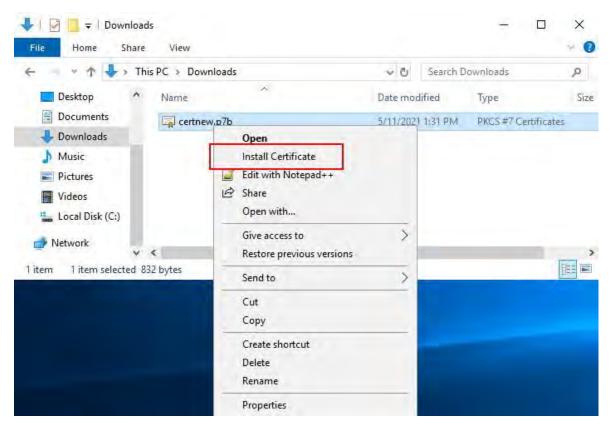
2. Click Download a CA certificate, certificate chain, or CRL.

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

Microsoft Active Directory Certif × +	• - • ×
← → C ▲ Not secure 10.0.4.103/certsrv/certcarc.asp	☆ ≛ :
Microsoft Active Directory Certificate Services – IP-0A000467-CA	Home
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 th	e certificate and encoding method.
CA certificate:	
Current [IP-0A000467-CA]	
· · · · ·	
And and a first of	
Encoding method: DER O Base 64	
● DER ○ Base 64	
DER Base 64 Install CA certificate	

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, dick Next.

B.Lardi	Connel
INEXT	Cancel

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 Sto	re				
Certificat	e stores are syst	em areas where	certificates are k	æpt.	
() Au	comatically select	t the certificate s	store based on th	e type of certifica	ate
Pla	ce all certificates	in the following	store		
Ce	rtificate store:				
				Bro	wse

	and the second second
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.	
	1 tificates are kept.
	store, or you can specify a location for
< > > Show physical stores	e based on the type of certificate
OK Cancel	Browse

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.

Recording server information	
Name:	
Recording server 1	
Description:	
Covers sector 1	14
	1496
Host name:	
and the second sec	
Local web server address:	
https://	
Web server address:	
https://www.recordingserver1.dk:89/	
Time zone:	
(UTC+01:00) Brussels, Copenhagen, Madrid, Paris	

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.

ailover server information	
Name	
Failover recording server 1	
Description:	
Failover for Recording server 1	
	1
Host name:	
Jocal	
Local web server address:	
https:// .local:7563/	
Web server address:	
https://www.failoverrecordingserver1:89/	
UDP port: 8844	
Database location:	
C:\MediaDatabase	
Enable this failover server	

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

Private certificate for signing other certificates (in certificate store)

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-gt0){
      $ipEntries = ($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

#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)

#Promptuser 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-gt0){
\$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"

${\ \ } {\ \ }$

\$serverAuthentication = '2.5.29.37={critical}{text}1.3.6.1.5.5.7.3.1'

$\# {\sf Now-create the management server certificate}$

#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



EN_02/25

MOBOTIX AG • Kaiserstrasse • D-67722 Langmeil • Tel.: +49 6302 9816-103 • sales@mobotix.com • www.mobotix.com

MOBOTIX is a trademark of MOBOTIX AG registered in the European Union, the U.S.A., and in other countries. Subject to change without notice. MOBOTIX do not assume any liability for technical or editorial errors or omissions contained herein. All rights reserved. © MOBOTIX AG 2023