

# **MOBOTIX HUB – Certificates Guide**

V2.04

# Table of Contents

© MOBOTIX Mx_GL_MX_ XDr	X AG www.mobotix.com (_HUB_Certificates_V2-04_EN.docx • 04.03.2025 • Page 2/ 126Certificates guide - Milestone XProtect® VMSCertificates guil M @ B C Protect® VMS	<b>XIT</b>
11	1 CREATE SSL CERTIFICATE 2	29
10	0 INSTALL CERTIFICATES ON THE CLIENTS 2	21
9.2	2 CREATE CA CERTIFICATE 1	18
9.1	1 IMPORTANT TO KNOW:	8
9	CREATING AND DISTRIBUTING CERTIFICATES MANUALLY	L8
8	POWERSHELL SCRIPTS 1	17
7.4	.4 Mobile streaming media certificate 1	L6
7.3	.3 STREAMING MEDIA CERTIFICATE	L6
7.2	2 Event server and add-ons	L6
7.1	.1 Server certificate	15
7	SERVER CONFIGURATOR (EXPLAINED) 1	L <b>4</b>
6	WHICH CLIENTS NEED CERTIFICATES? 1	12
5.7	.7 CLIENT 1	L <b>O</b>
5.6	.6 MOBOTIX HUB Event Server	L <b>O</b>
5.!	.5 WORKGROUP	L <b>O</b>
5.4	.4 DOMAIN	L <b>O</b>
5.3	.3 THIRD-PARTY OR COMMERCIAL CA CERTIFICATE	L <b>O</b>
5.2	2 MOBOTIX HUB MANAGEMENT SERVER AND RECORDING SERVER	9
5.1		9
5	OVERVIEW OF THE SCENARIOS AND PROCEDURES USED WITH CERTIFICATES	9
<b>4.</b> 1	.1 CERTIFICATE DISTRIBUTION	8
4	INTRODUCTION TO CERTIFICATES	7
3	WHEN DO YOU NEED TO INSTALL CERTIFICATES?	6
2	ABOUT THIS GUIDE	5
1	COPYRIGHT, TRADEMARKS, AND DISCLAIMER	4

# MOBOTIX HUB – Certificates Guide - Error! Use the Home tab to apply

12 I	MPORT SSL CERTIFICATE
12.1	MANAGE PRIVATE KEYS
13 C	REATE SSL CERTIFICATE FOR THE FAILOVER MANAGEMENT SERVER
14 I	NSTALL CERTIFICATES FOR COMMUNICATION WITH THE MOBILE SERVER
14.1	ADD A CA CERTIFICATE TO THE SERVER
14.2	UPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN
14.3	ENABLE ENCRYPTION ON THE MOBILE SERVER
15 I Mana	NSTALL THIRD-PARTY OR COMMERCIAL CA CERTIFICATES FOR COMMUNICATION WITH THE GEMENT SERVER OR RECORDING SERVER
15.1	ADD A CA CERTIFICATE TO THE SERVER
15.2	UPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN
15.3	ENABLE ENCRYPTION TO AND FROM THE MANAGEMENT SERVER
15.3.1	Prerequisites:
1532	TO INSTALL AD CS:
10.0.2	
15.4	INSTALL CERTIFICATES IN A DOMAIN FOR COMMUNICATION WITH THE MANAGEMENT SERVEROR RECORDING SERVER 80
<b>15.4</b> 15.4.1	INSTALL CERTIFICATES IN A DOMAIN FOR COMMUNICATION WITH THE MANAGEMENT SERVEROR RECORDING SERVER 80 ADD A CA CERTIFICATE TO THE SERVER
<b>15.4</b> 15.4.1 15.4.2	INSTALL CERTIFICATES IN A DOMAIN FOR COMMUNICATION WITH THE MANAGEMENT SERVEROR RECORDING SERVER 80 ADD A CA CERTIFICATE TO THE SERVER
<b>15.4</b> 15.4.1 15.4.2 <b>15.5</b>	INSTALL CERTIFICATES IN A DOMAIN FOR COMMUNICATION WITH THE MANAGEMENT SERVEROR RECORDING SERVER         80       ADD A CA CERTIFICATE TO THE SERVER
<b>15.4.1</b> 15.4.2 <b>15.5</b> 15.5.1	INSTALL CERTIFICATES IN A DOMAIN FOR COMMUNICATION WITH THE MANAGEMENT SERVEROR RECORDING SERVER         80         ADD A CA CERTIFICATE TO THE SERVER
<b>15.4</b> .1 15.4.2 <b>15.5</b> 15.5.1 <b>16</b>	INSTALL CERTIFICATES IN A DOMAIN FOR COMMUNICATION WITH THE MANAGEMENT SERVEROR RECORDING SERVER         80         ADD A CA CERTIFICATE TO THE SERVER
15.4.1 15.4.2 15.5 15.5.1 16	INSTALL CERTIFICATES IN ADOMAIN FOR COMMUNICATION WITH THE MANAGEMENT SERVEROR RECORDING SERVER         80         ADD A CA CERTIFICATE TO THE SERVER
15.4.1 15.4.2 15.5 15.5.1 16 II MANA 16.1	INSTALL CERTIFICATES IN ADOMAIN FOR COMMUNICATION WITH THE MANAGEMENT SERVEROR RECORDING SERVER         80       ADD A CA CERTIFICATE TO THE SERVER       81         UPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN.       88         INSTALL THE CERTIFICATE MANUALLY       91         ENABLE SERVER ENCRYPTION FOR MANAGEMENT SERVERS AND RECORDING SERVERS       94         NSTALL CERTIFICATES IN AWORKGROUP ENVIRONMENT FOR COMMUNICATION WITH THE GEMENT SERVER OR RECORDING SERVER       96         Add a CA CERTIFICATE TO THE SERVER       96
15.4.1 15.4.2 15.5 15.5.1 16 II MANA 16.1 16.1.1	INSTALL CERTIFICATES IN ADOMAIN FOR COMMUNICATION WITH THE MANAGEMENT SERVEROR RECORDING SERVER       80         ADD A CA CERTIFICATE TO THE SERVER       81         UPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN.       88         INSTALL THE CERTIFICATE MANUALLY       91         ENABLE SERVER ENCRYPTION FOR MANAGEMENT SERVERS AND RECORDING SERVERS.       94         NSTALL CERTIFICATES IN AWORKGROUP ENVIRONMENT FOR COMMUNICATION WITH THE GEMENT SERVER OR RECORDING SERVER       96         ADD A CA CERTIFICATE TO THE SERVER       96         UPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN.       104
15.4.1 15.4.2 15.5 15.5.1 16 II MANA 16.1 16.1.1 16.1.2	INSTALL CERTIFICATES IN A DOMAIN FOR COMMUNICATION WITH THE MANAGEMENT SERVER OR RECORDING SERVER         80       Add a CA CERTIFICATE TO THE SERVER       81         UPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN.       88         INSTALL THE CERTIFICATE MANUALLY       91         ENABLE SERVER ENCRYPTION FOR MANAGEMENT SERVERS AND RECORDING SERVERS       94         NSTALL CERTIFICATES IN A WORKGROUP ENVIRONMENT FOR COMMUNICATION WITH THE GEMENT SERVER OR RECORDING SERVER       96         ADD A CA CERTIFICATE TO THE SERVER       96         UPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN.       104         ISSUE CERTIFICATES MANUALLY       108
15.4.1 15.4.2 15.5.1 16 II MANA 16.1.1 16.1.2 16.1.3	INSTALL CERTIFICATES IN A DOMAIN FOR COMMUNICATION WITH THE MANAGEMENT SERVEROR RECORDING SERVER         80       ADD A CA CERTIFICATE TO THE SERVER       81         UPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN       88         INSTALL THE CERTIFICATE MANUALLY       91         ENABLE SERVER ENCRYPTION FOR MANAGEMENT SERVERS AND RECORDING SERVERS       94         NSTALL CERTIFICATES IN A WORK GROUP ENVIRONMENT FOR COMMUNICATION WITH THE GEMENT SERVER OR RECORDING SERVER       96         ADD A CA CERTIFICATE TO THE SERVER       96         UPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN       104         ISSUE CERTIFICATES MANUALLY       108         ENABLE SERVER ENCRYPTION FOR MANAGEMENT SERVERS AND RECORDING SERVERS       113
15.4.1 15.4.2 15.5 15.5.1 16 II MANA 16.1 16.1.2 16.1.3 16.2	INSTALL CERTIFICATES IN ADOMAIN FOR COMMUNICATION WITH THE MANAGEMENT SERVEROR RECORDING SERVER         80         ADD A CA CERTIFICATE TO THE SERVER         81         UPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN.         88         INSTALL THE CERTIFICATE MANUALLY         91         ENABLE SERVER ENCRYPTION FOR MANAGEMENT SERVERS AND RECORDING SERVERS.         94         NSTALL CERTIFICATES IN AWORKGROUP ENVIRONMENT FOR COMMUNICATION WITH THE         GEMENT SERVER OR RECORDING SERVER         96         ADD A CA CERTIFICATE TO THE SERVER         96         VPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN.         104         ISSUE CERTIFICATES MANUALLY         108         ENABLE SERVER ENCRYPTION FOR MANAGEMENT SERVERS AND RECORDING SERVERS         113         INSTALL CERTIFICATES FOR COMMUNICATION WITH THE EVENT SERVER
15.4.1 15.4.2 15.5 15.5.1 16 II MANA 16.1.1 16.1.2 16.1.3 16.2 16.3	INSTALL CERTIFICATES IN A DOMAIN FOR COMMUNICATION WITH THE MANAGEMENT SERVEROR RECORDING SERVER         80         ADD A CA CERTIFICATE TO THE SERVER         UPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN.         SINSTALL THE CERTIFICATE MANUALLY         91         ENABLE SERVER ENCRYPTION FOR MANAGEMENT SERVERS AND RECORDING SERVERS.         94         NSTALL CERTIFICATES IN A WORKGROUP ENVIRONMENT FOR COMMUNICATION WITH THE         GEMENT SERVER OR RECORDING SERVER.         96         ADD A CA CERTIFICATE TO THE SERVER         96         UPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN.         104         ISSUE CERTIFICATES MANUALLY         108         ENABLE SERVER ENCRYPTION FOR MANAGEMENT SERVERS AND RECORDING SERVERS.         108         ENABLE SERVER ENCRYPTION FOR MANAGEMENT SERVERS AND RECORDING SERVERS.         113         INSTALL CERTIFICATES FOR COMMUNICATION WITH THE EVENT SERVER.         114         ENABLE SERVER ENCRYPTION FOR MANAGEMENT SERVERS AND RECORDING SERVERS.         113         INSTALL CERTIFICATES FOR COMMUNICATION WITH THE EVENT SERVER.         114         ENABLE MOBOTIX HUB EVENT SERVER ENCRYPTION
<ul> <li>15.4.1</li> <li>15.4.2</li> <li>15.5</li> <li>15.5.1</li> <li>16 II</li> <li>MANA</li> <li>16.1.1</li> <li>16.1.2</li> <li>16.1.3</li> <li>16.2</li> <li>16.3</li> <li>16.3.1</li> </ul>	INSTALL CERTIFICATES IN A DOMAIN FOR COMMUNICATION WITH THE MANAGEMENT SERVEROR RECORDING SERVER         80         ADD A CA CERTIFICATE TO THE SERVER         MIDE CERTIFICATE TO THE SERVER         INSTALL THE CERTIFICATE TO RECEIVE A SIGNED CERTIFICATE IN RETURN         INSTALL THE CERTIFICATE MANUALLY         INSTALL CERTIFICATES IN A WORK GROUP ENVIRONMENT FOR COMMUNICATION WITH THE         GEMENT SERVER OR RECORDING SERVER         96         ADD A CA CERTIFICATE TO THE SERVER         OF
15.4.1 15.4.2 15.5 15.5.1 16 II MANA 16.1.1 16.1.2 16.1.3 16.2 16.3.1 16.3.1	INSTALL CERTIFICATES IN A DOMAIN FOR COMMUNICATION WITH THE MANAGEMENT SERVER OR RECORDING SERVER 80         ADD A CA CERTIFICATE TO THE SERVER       81         UPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN.       88         INSTALL THE CERTIFICATE MANUALLY       91         ENABLE SERVER ENCRYPTION FOR MANAGEMENT SERVERS AND RECORDING SERVERS.       94         NSTALL CERTIFICATES IN A WORKGROUP ENVIRONMENT FOR COMMUNICATION WITH THE         GEMENT SERVER OR RECORDING SERVER.       96         ADD A CA CERTIFICATE TO THE SERVER       96         UPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN.       104         ISSUE CERTIFICATES MANUALLY       108         ENABLE SERVER ENCRYPTION FOR MANAGEMENT SERVERS AND RECORDING SERVERS       113         INSTALL CERTIFICATES FOR COMMUNICATION WITH THE EVENT SERVER       114         ENABLE SERVER ENCRYPTION FOR MANAGEMENT SERVERS AND RECORDING SERVERS       113         INSTALL CERTIFICATES FOR COMMUNICATION WITH THE EVENT SERVER       114         ENABLE MOBOTIX HUB EVENT SERVER ENCRYPTION       115         PREREQUISITES:       115         IMPORT CLIENT CERTIFICATES       116
<ul> <li>15.4.1</li> <li>15.4.2</li> <li>15.5.1</li> <li>16 II</li> <li>MANA</li> <li>16.1.1</li> <li>16.1.2</li> <li>16.1.3</li> <li>16.2</li> <li>16.3.1</li> <li>16.3.2</li> <li>1. D</li> </ul>	INSTALL CERTIFICATES IN A DOMAIN FOR COMMUNICATION WITH THE MANAGEMENT SERVEROR RECORDING SERVER         80         ADD A CA CERTIFICATE TO THE SERVER       81         UPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN.         88         INSTALL THE CERTIFICATE MANUALLY         91         ENABLE SERVER ENCRYPTION FOR MANAGEMENT SERVERS AND RECORDING SERVERS.         94         NSTALL CERTIFICATES IN A WORKGROUP ENVIRONMENT FOR COMMUNICATION WITH THE         GEMENT SERVER OR RECORDING SERVERS         96         ADD A CA CERTIFICATE TO THE SERVER         96         UPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN.         104         ISSUE CERTIFICATE TO THE SERVER         96         UPLOAD THE .REQ FILE TO RECEIVE A SIGNED CERTIFICATE IN RETURN.         104         ISSUE CERTIFICATES MANUALLY         108         INSTALL CERTIFICATES MANUALLY         108         INSTALL CERTIFICATES MANUALLY         108         INSTALL CERTIFICATES FORCOMMUNICATIONWITH THE EVENT SERVER
<ul> <li>15.4.1</li> <li>15.4.2</li> <li>15.5</li> <li>15.5.1</li> <li>16 II</li> <li>MANA</li> <li>16.1.1</li> <li>16.1.2</li> <li>16.1.3</li> <li>16.2</li> <li>16.3.1</li> <li>16.3.2</li> <li>1. D</li> <li>16.4</li> </ul>	INSTALL CERTIFICATES IN ADOMAIN FOR COMMUNICATION WITH THE MANAGEMENT SERVEROR RECORDING SERVER 80         ADD A CA CERTIFICATE TO THE SERVER

## 1 Copyright, trademarks, and disclaimer

Copyright © 2025 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 adjust 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 HUB system installation folder.

### 2 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.

## 3 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 Δ

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

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 7/ 126Certificates guide - Milestone XProtect® VMSCertificates guide BOTIX XProtect® VMS

### 4.1 Certificate distribution

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



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

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

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

🔮 The CA certificate must be installed on the computer on which the management server is running Requirements for the private management server certificate:

- Issued to the management server so that the management server's host name is included in the certificate, either as subject (owner) or in the list of DNS names that the certificate is issued to
- Trusted on the management server itself, by trusting the CA certificate that was used to issue the management server certificate
- Trusted on all recording servers connected to the management server, by trusting the CA certificate that was used to issue the management server certificate

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.

### © MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 8/ 126Certificates guide - Milestone XProtect® VMSCertificates guide BOTIX XProtect<sup>®</sup> VMS

### 5 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

### 5.1 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

### <sup>52</sup> 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.

### 5.3 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

### 5.4 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

### 5.5 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** 5.6

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 5.7

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

### © MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 10/ 126Certificates guide - Milestone XProtect® VMSCertificates guide & Comparison of the State of th XProtect® VMS

### MOBOTIX HUB - Certificates Guide - Overview of the scenarios and procedures used

- 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

## 6 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

 $\bigcirc$ 

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.

## 7 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

# MOBOTIX HUB - Certificates Guide - Server Configurator (explained)

Milestone Server Configurator		Ŧ	
Encryption	Encryption		
Registering servers	It is recommended to secure communication with encryptio	n, <u>Learn m</u>	ore
Language selection	Server certificate Applies to: management server, recording server, failover server, data collector		
	Encryption: On		
	DocCert1	-	Details
	Certificate issued by mit-MJT-DC-CA, DC=mit, DC=local, Expires 4/27/2022		
	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 mjt-MJT-DC-CA, DC=mjt, DC=local. Expires 4/27/2022		
			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.

#### Server certificate 7.1

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 •

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 15/ 126Certificates guide - Milestone XProtect® VMSCertificates g XProtect<sup>®</sup> VMS

### **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.

### 7.3 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.

### 74 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.

### 8 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.

## 9 Creating and distributing certificates manually

### 9.1 Important to know:



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

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

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

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

Note that this setting might be controlled by a domain policy. In which case, it must be disabled at that level. Your certificate will now stay on the computer despite it is not from a "trusted third-party certificate authority," because Windows Update will not contact the Windows Update website to see if Microsoft has added the CA to its list of trusted authorities.

### 9.2 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.

1	CreateCACertificate.ps1 - Notepad	
File Edit Format View Help		
<pre># Run this script once, to create a # Private certificate for signing ot isc_acrificate = New-SelfSignedCert KeyUsage CertSign, CRLSign, Digital # Thumbprint of private certificate set-Content -Path "\$PSScriptRoot\ca_ # Public CA certificate to trust (Th Export-Certificate -Cert "Cert:\Current # Public CA certificate to trust (Th Export-Certificate -Cert "Cert:\Current # Public CA certificate -Cert "Certificate -Certificate -Certifica</pre>	<pre>certificate that can sign multiple recording server certificates her certificates (in certificate store) ficate - CertStoreLocation cert:\CurrentUser\My -DnsName 'VMS Certificate Author signature -FriendlyName 'VMS CA Certificate' used for signing other certificates humbprint.txt" -Value \$ca_certificate.Thumbprint hrd-Party Root Certificate.Thumbprint) entUser\My\\$(\$ca_certificate.Thumbprint)" -FilePath "\$PSScriptRoot\root-authori entUser\My\\$(\$ca_certificate.Thumbprint)")</pre>	ority' -KeyusageProperty All ` ity-public.cer"
		3
	Inß	Col 130

- In Notepad, click File -> Save as, name the file CreateCACertificate.ps1 and save it locally, like this: C:\Certificates\CreateCACertificate.ps1.
- 4. In File Explorer, go to C:\Certificates and select the CreateCACertificate.ps1 file.

5. In the File menu, select Open Windows PowerShell and then Open Windows PowerShell as administrator.

		1	Cert	
Open new window	Open Windows Powe <u>r</u> Shell	Open •	🚼 Select all	
Open command prompt	Open Windows PowerShell as administrator	Properties	Select	
Open Windows Powe <u>r</u> Shell				
C Palacelana		Date modified	Туре	Size
Delete history		04-02-2019 11:31	File folder	
<b>A</b>		04-02-2019 11:31	File folder	
Elip .		04-02-2019 11:31	File folder	
		04-02-2019 11:31	File folder	
Close		04-02-2019 11:31	File folder	
		04-02-2019 11:31	File folder	
Sec. 24	ReateCACertificate.ps1	31-01-2019 15:01	Windows PowerShell Script	ŤK
📕 This PC				

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

🛃 Admin	istrator: Windows Pov	werShell			×
PS C:\Cert	tificates> .\Cre	ateCACertific	cate.ps1		^
Direct	tory: C:\Certifi	cates			
Node	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.



### 10 Install certificates on the clients

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



See Import client certificates on page 129 for an alternative procedure to manually installing certificates on clients.

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



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

R.		
40	ertificate Import Wizard	
3	Welcome to the Certificate Import Wizard	
- 3	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
1000	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	
	<u>Current User</u> <u>Local Machine</u>	
6	To continue, click Next.	

- 10. In the Certificate **Import Wizard**, select to install the certificate in the store of the **Local Machine** and click **Next**.
- 11. Select to manually locate the store in which the certificate will be installed.

Certificate Store			
Certificate stores are	system areas where certi	ficates are kept.	
Windows can automa the certificate. Automatically s Place all certific Certificate sto	tically select a certificate s elect the certificate store cates in the following store re:	store, or you can spec based on the type of	ify a location for certificate
			Browse

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



13. On the Completing the Certificate Import Wizard dialog, click Finish.

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

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 23/ 126Certificates guide - Milestone XProtect® VMSCertificates g XProtect<sup>®</sup> VMS

Completing the	Certificate Import Wizard	
The certificate will be imp	ported after you dick Finish.	
You have specified the fo	ollowing settings:	
Certificate Store Select Content	ted by User Trusted Root Certification Authorities Certificate	
100 Y		

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



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

😅 Run		×
e	Type the name of a program, folder, doc resource, and Windows will open it for ye	ument, or Internet ou.
<u>O</u> pen:	mmd	*
	OK Cancel	Browse

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

Open Ctrl+	Name	Actions
Save Ctrl+	There are no items to show in this view.	Console Root
Add/Remove Span-in Ctrl+1		More Actions
Options		
Recent File		
Exit		

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

Snap-in ActiveX Control	Vendor Microsoft Cor	^	Console Root	Edit Extensions
Certificates	Microsoft Cor Microsoft Cor			(Mpreff)
Device Manager	Microsoft Cor Microsoft and	l	Add >	Mare Banc
Folder Group Policy Object	Microsoft Cor Microsoft Cor			
Internet Informatio	Microsoft Cor Microsoft Cor			
		Y		Ad <u>v</u> anced

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

Certificates snap-in	×
This snap-in will always manage certificates for: <ul> <li>My user account</li> <li>Service account</li> <li>Computer account</li> </ul>	
	Back Next > Cancel

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

elect the computer you want this snap-in to manage	je.	
Encal computer: the computer this console i	s running on)	
O Another computer:		Byrane
only applies if you save the console.	and a second second second	the seminaria lifte. Trite

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

vailable <u>s</u> nap-ins:		_	5	elected snap-ins:		
Snap-in	Vendor Microsoft Cor	^		Console Root	puter) E	dit E <u>x</u> tensions
Authorization Manager	Microsoft Cor Microsoft Cor					
Component Services	Microsoft Cor					Indes The
📩 Device Manager	Microsoft Cor Microsoft and	1	<u>A</u> dd >			CONTRACT DEVICE
Event Viewer	Microsoft Cor Microsoft Cor					
Group Policy Object	Microsoft Cor Microsoft Cor					
Internet Informatio	Microsoft Cor	>				Ad <u>v</u> anced
escription:						
The Certificates snap-in allo	ows you to browse	the	contents of the	certificate stores for vourself. a	a service, or a c	omputer.

21. Verify that the certificate is listed in the center view of the Trusted Root Certification Authorities

subtree.

© MUBOTIX AG www.mobotix.com Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 27/ 126Certificates guide - Milestone XProtect® VMSCertificates guide & Milestone XProtect® VMSCertificates g

File Action View Favorites Window He	lp.	and a standard			- A 0
					10.00
Console Root	Issued To	Issued By	Exp ^	Actions	
Personal	a 10.5.14.40 10.5.6.101	10.5.14.40 10.5.6.101	20: 20:	Certificates More Actions	
Certificates  Enterprise Trust  Intermediate Certification Authorities	AddTrust External CA Root	AddTrust External CA Root Baltimore CyberTrust Root CKMS	202 202 202		
P      Trusted Publishers     D      Intrusted Certificates     D      Third-Party Root Certification Authorities	Class 3 Public Primary Certificat	Class 3 Public Primary Certificatio Copyright (c) 1997 Microsoft Corp. DigiCert Assured ID Root CA	202 199 205		
Trusted People     Client Authentication Issuers     Preview Build Roots	DigiCert Global Root CA DigiCert High Assurance EV Ro	DigiCert Global Root CA DigiCert High Assurance EV Root DST Root CA X3	20: 20: 20:		
AD Token Issuer     SIM Certification Authorities     Merigroup Machine Certificates	GlobalSign	Equifax Secure Certificate Authority GeoTrust Global CA GlobalSign	20 <sup>2</sup> 202 202		
<ul> <li>Remote Desktop</li> <li>Certificate Enrollment Requests</li> <li>Smart Card Trusted Roots</li> </ul>	GlobalSign GlobalSign Root CA Go Daddy Class 2 Certification	GlobalSign GlobalSign Root CA Go Daddy Class 2 Certification Au	202 202 203		
	GTE CyberTrust Global Root Hotspot 2.0 Trust Root CA - 03	GTE CyberTrust Global Root Hotspot 2.0 Trust Root CA - 03	20 <sup>.</sup> 204		
	Microsoft Authenticode(tm) Ro	Microsoft Authenticode(tm) Root Microsoft Root Authority Microsoft Root Certificate Authori	200		
	Microsoft Root Certificate Auth	Microsoft Root Certificate Authori Microsoft Root Certificate Authori	202 203 203		
	NO LIABILITY ACCEPTED, (c)97	NO LIABILITY ACCEPTED, (c)97 Ve	202 200		
	Starfield Class 2 Certification A	Starried Class 2 Certification Auth Starfield Services Root Certificate Symantec Enterprise Mobile Root	20: 20: 20: ¥		

22. 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.

### 11 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).

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

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. In Appendix B in the back of this guide, you find a script for creating server certificates.

1. 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.
- 3. In File Explorer, go to C:\Certificates and select the CreateServerCertificate.ps1 file.
- 4. In the File menu, select Open Windows PowerShell and then Open Windows PowerShell as administrator.

Open <u>n</u> ew window	*	Open Windows PowerShell	Dopen •	Sele Sele	ect all ect none		
Open command prompt	÷	Open Windows PowerShell as administrator	Properties + History Open	inve inve	ert selection Select		
Open Windows Powe <u>r</u> Shell	*						
0			Date modified	ł	Туре	Size	
Delete history	*		04-02-2019 11	:31	File folder		
0.046			04-02-2019 11	:31	File folder		
<b>Э</b> цеір			04-02-2019 11	:31	File folder		
S Later			04-02-2019 11	:31	File folder		
Liose			04-02-2019 11	:53	File folder		
			04-02-2019 11	:31	File folder		
Que de la composición		🙀 CreateCACertificate.ps1	31-01-2019 15	:01	Windows PowerShell Script		1 KI
🜉 This PC		Create ServerCertificate,	s1 25-01-2019 15	:31	Windows PowerShell Script		3 KF

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



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

 Administrator: Windows PowerShell
 —
 —
 —
 X

 PS C:\Certificates> .\CreateServerCertificate.ps1

 DNS names for server SSL certificate (delimited by space - 1st entry is also subject of certificate):
 \_\_\_\_\_\_

7. 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.

8. 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.

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

### 12 Import SSL certificate

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



Remember that each certificate is created to a specific server.

- 10. Copy the relevant Subjectname.pfx file from the computer where you created the certificate to the corresponding server service computer.
- 11. On the server service computer, start Manage computer certificates.
- 12. Click on **Personal**, right-click **Certificates** and select **All Tasks** > **Import**.

File Action View Help	
File Action View Help	Logical Store Name Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates
<ul> <li>Third-Party Root Certification Authorities</li> <li>Trusted People</li> <li>Client Authentication Issuers</li> <li>Homegroup Machine Certificates</li> <li>MSIEHistoryJournal</li> <li>OfcEdge</li> <li>OfficeScan SSL Agent</li> <li>Remote Desktop</li> <li>Smart Card Trusted Roots</li> <li>Trusted Devices</li> <li>Web Hosting</li> <li>Windows Live ID Token Issuer</li> </ul>	<ul> <li>Third-Party Root Certification Authorities</li> <li>Trusted People</li> <li>Client Authentication Issuers</li> <li>Homegroup Machine Certificates</li> <li>MSIEHistoryJournal</li> <li>OfcEdge</li> <li>OfficeScan SSL Agent</li> <li>Remote Desktop</li> <li>Smart Card Trusted Roots</li> <li>Trusted Devices</li> <li>Web Hosting</li> <li>Windows Live ID Token Issuer</li> </ul>
	<

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

- 4	Certificate Import Wizard	
	Welcome to the Certificate Import Wizard	
	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
	Store Location	
	Local Machine	
	To continue, dick Next.	
	Canc	el

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

Specify the file you want to import.	
File name:	
C:\Users\gis\DocumentsWy Received	fliesWMS-REC-01.pb
Note: More than one certificate can be	e stored in a single file in the following formats:
Personal Information Exchange-PK	CS #12 (.PFX,.P12)
Cruptographic Macagae Suptay Sta	ndard-PKCS #7 Certificates (.P7B)
Ci yptograpnic Message Syntax Stal	
Microsoft Serialized Certificate Store	e (.SST)
Microsoft Serialized Certificate Store	e (.SST)
Microsoft Serialized Certificate Store	e (.SST)
Microsoft Serialized Certificate Store	e (.SST)

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

P	rivate key protection
	To maintain security, the private key was protected with a password.
-	
	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.
	I tech de all autoridad preservice
	Include all extended properties.

16. Place the file in the **Certificate Store**: **Personal** then click **Next**.

ertificate Store	
Certificate stores are system areas wh	iere certificates are kept,
Windows can automatically select a cer	rtificate store, or you can specify a location for
the certificate.	runcate store, or you can specify a location for
O Automatically select the certifica	ate store based on the type of certificate
Place all certificates in the follow	ving store
Certificate store:	
Personal	Browse

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

he certificate will be imported afte	r you dick Finish.
ou have specified the following se	ttings:
Certificate Store Selected by Use	r Personal
Content File Name	PFX C;\Users\gis\Desktop\VMS-REC-01.pfx

The imported certificate appears in the list.
P 🗭   📶 🔟   🚇 🖻   🔟 🔟		
<ul> <li>Certificates - Local Computer</li> <li>Personal</li> <li>Certificates</li> <li>Trusted Root Certification Authorities</li> <li>Enterprise Trust</li> <li>Intermediate Certification Authorities</li> <li>Trusted Publishers</li> <li>Untrusted Certificates</li> <li>Third-Party Root Certification Authorities</li> <li>Trusted People</li> <li>Client Authentication Issuers</li> <li>Homegroup Machine Certificates</li> <li>MSIEHistoryJournal</li> <li>OfcEdge</li> <li>OfficeScan SSL Agent</li> </ul>	Issued To * * * Iocalhost VMS Certificate Authority * VMS-REC-01	Issued By Iocalhost VMS Certificate Authority VMS Certificate Authority

18. To allow a service to use the private key of the certificate, right click the certificate and select All Tasks
 >

### 12.1 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

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

cunty		
group or user names:		
SYSTEM		
Administrators (Administrator	s)	
NETWORK SERVICE		
	Add	Remove
ermissions for NETWORK	1.250	22201010
ERVICE	Allow	Deny
Full control		
Read	P	
Special permissions		
	ed settings,	Advanced
or special permissions or advanc	2011-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1	Auganceu
	ed settings,	Advanced
for special permissions or advance lick Advanced.		

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

#### 13 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.

- 3. In Appendix C of this guide, copy the script for creating failover management server certificates.
- 4. 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.

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

Example: C:\Certificates\CreateFailoverCertificate.ps1.

- 6. In File Explorer, go to C:\Certificates and select the CreateFailoverCertificate.ps1 file.
- 7. In the File menu, select Open Windows Powershell and then Open Windows PowerShell as administrator.

Open <u>n</u> ew window	*	Open Windows PowerShell	Open •	1	Select all		
Open command grompt	÷	Open Windows PowerShell as administrator	Properties	4	Select:		
Open Windows Powe <u>r</u> Shell	*						
D. Annone			Date modifie	ed	Туре	Size	
Delete history	*		04-02-2019 1	11:3	1 File folder		
and a second sec			04-02-2019 1	1:3	1 File folder		
Help			04-02-2019 1	11:3	1 File folder		
1			04-02-2019 1	11:3	1 File folder		
Liose			04-02-2019 1	1:5	3 File folder		
			04-02-2019 1	11:3	1 File folder		
and a second		CreateCACertificate.ps1	31-01-2019 1	15:0	11 Windows PowerShell Script		1 K
🜉 This PC		CreateServerCertificate.p	s1 25-01-20191	15:3	1 Windows PowerShell Script		3 K

- 8. In PowerShell, enter .\CreateFailoverCertificate.ps1 at the prompt and press Enter.
- 9. 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.

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

#### © MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 39/ 126Certificates guide - Milestone XProtect® VMSCertificates g XProtect<sup>®</sup> VMS

# MOBOTIX HUB - Certificates Guide - Create SSL certificate for the failover



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.

#### 14 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.



٢

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.

#### 14.1 Add a CA certificate to the server

Add the CA certificate to the Mobile Server by doing the followingOn the computer that hosts the Mobile Server, open the Microsoft Management Console.

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

	ernet	an	orog ows	e of a p Windo	name and \	the r urce,	Tj re	e
Open: mmd	Y	_				nd	[	<u>O</u> pen:

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

# MOBOTIX HUB - Certificates Guide - Install certificates for communication with the

Open Ctrl+O	La contra c	A
Save Ctrl+S	Name There are no items to show in this view	Actions Console Root
Save As		More Actions
Add/Remove Snap-in Ctrl+M Options		
Recent File		
Exit		

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

Add or Remove Snap-ins

3. Click OK.

You can select span-ins for this console from those available on your computer and configure the selected set of span-ins. For
The carried carried in a service in a rescarbance of year compare and carried carried service and print for
extensible snap-ins, you can configure which extensions are enabled.

×

Snap-in	Vendor	^	Console Root	Edit Extensions
ActiveX Control	Microsoft Cor Microsoft Cor		Certificates - Current Us	Remove
Certificate Templates	Microsoft Cor Microsoft Cor			albeeth.
Certification Authority	Microsoft Cor Microsoft Cor			Marco Crown
Computer Managem	Microsoft Cor	Add	1>	
Device Manager     Disk Management	Microsoft Cor Microsoft and			
Enterprise PKI	Microsoft Cor			
Folder	Microsoft Cor			
Group Policy Object	Microsoft Cor	*		Advanced
Description:				
The Certificates snap-in all	ows you to browse	the content	s of the certificate stores for yourself, a	service, or a computer.
				OK Cance

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 42/ 126Certificates guide - Milestone XProtect® VMSCertificates guide & Milestone XProtect® VM

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.
- 6. 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 Cance

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

Contractor in and the		
Custom request		
Chose an option from	n the list below and configure the certificate options as required	d.
Template:	(No template) CNG key	
	Suppress default extensions	
Request format:	○ PKCS #10	
	<u>●</u> <u>C</u> MC	
Note: Key archival is option is specified in	not available for certificates based on a custom certificate requ the certificate template.	uest, even when this
Note: Key archival is option is specified in	not available for certificates based on a custom certificate requ the certificate template.	uest, even when this
Note: Key archival is option is specified in xpand to view the <b>Detai</b>	not available for certificates based on a custom certificate requ the certificate template.	uest, even when this <u>N</u> ext Cance

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

# MOBOTIX HUB - Certificates Guide - Install certificates for communication with the

	-					
General	Subject	Extensions	Private Key	Signature		
A friend	lly name	and descript	tion will make	e it easier to ider	itify and use a certi	ficate.
Friendly	name:					
TestLa	Domain	.com				
Descrip	tion:					
TestLa	bDomain	.com				
					-1	

10. 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:

Certificate Properties			×
General Subject Extensions	Private Key	Signature	
The subject of a certificate is can enter information about t can be used in a certificate.	the user or c the types of :	omputer to w subject name	hich the certificate is issued. You and alternative name values that
Subject of certificate			
The user or computer that is i	receiving the	certificate	
Subject name:	_		
Туре:			CN=Test for Docs
Country ~		Add	OU=MJT Lab
Value:	*	Remove	L=Maple Grove S=MN C=USA
Alternative name:	1		
Туре:			
Directory name 🔗			
Value:		Ádd >	
	10	Remove	
		OK	Cancel Apply

11. 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.

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

Ì

			1200 200 200				
General	Subject	Extensions	Private Key	Signature			
The fol	lowing ar	e the certific	ate extension	s for this cert	ificate type.		^
Key u	sage					^	
The ke	y usage e	extension des	cribes the pu	rpose of a ce	rtificate.		
Availal	ble option	15:			Selected optic	ins:	
CRL si Data e	gning ncipherm	ient			Digital signate Key certificate	ure signing	
Decipł	ner only				Key encipherr	ment	
Enciph	ner only		Ac	ld >			
Non re	reement						
-			510	inove			
☑ Mal	these k	ey usages cr	itical				
🗹 Mal	ce these k	ey usages cr	itical				
Mal	ce these k ded Key U	ey usages cr Isage (applic	itical ation policies	)		v	
Extend	ce these k ded Key U	ey usages cr Jsage (applic	itical ation policies	)		Ŷ	
Exten Basic	ce these k ded Key U constrain	ey usages cr Isage (applic ts	itical ation policies	)		*	
Extend Basic	ke these k ded Key U constrain	ey usages cr Isage (applic ts	itical ation policies	)		*	

13. 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.

# MOBOTIX HUB - Certificates Guide - Install certificates for communication with the

Certificate P	roperti	ies					×
General Si	ubject	Extensions	Private Key	Signature			
Cryptogr	raphic S	Service Prov	ider				٣
Key optio	ons						*
Set the ke	y lengt	th and expo	t options for	the private ke	ey.		
Key size:	2048				~		
Make p	orivate	key exportal	ole				
Allow	orivate	key to be ar	chived				
Strong	private	e key protect	tion				
Select Ha	ash Ala	orithm					*
Select Ha	sh Algo	prithm to be	used for this	request			
Hash Algo	orithm	sha256				-	
Select Sig	gnature	Format					*
				OK		Cancel	Apply

- 14. Unless the CA requires a signature, the next step is to click **OK**.
- 15. When all of the certificate properties have been defined, click **Next** on the **Certificate Enrollment** wizard.

- 🗆 X

Certificate Enri	ollment
------------------	---------

#### 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.

Key usage:	Digital signature Key certificate signing	
Application policie	s:	
Validity period (day	ys):	
		Properties

16. 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.

#### MOBOTIX HUB - Certificates Guide - Install certificates for communication with the

ick <b>Finish</b> .	
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 p to your hard disk or removable media. Enter the location and nar click Finish.	process the request later, save the reque me of your certificate request, and then
File Name:	Protocological
C:\Users\Administrator\Desktop\CSR6.1.21	Browse
File format:	
Base 64	
OBinary	

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

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

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

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

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

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

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

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

Ì

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 50/ 126Certificates guide - Milestone XProtect® VMSCertificates g XProtect<sup>®</sup> VMS

1. Browse to the location of the .reg 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

X

File Edit Format View Help

----BEGIN NEW CERTIFICATE REQUEST-----

MIIGBAYJKoZIhvcNAQcCoIIF9TCCBfECAQMxDzANBglghkgBZQMEAgEFADCCBEoG CCsGAQUFBwwcoIIEPASCBDgwggQ0MGQwYgIBAgYKKwYBBAGCNwoKATFRME8CAQAw AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QLTBBMDAwNDY3DB1JUC0wQTAw MDQ2N1xBZG1pbm1zdHJhdG9yDAdNTUMuRVhFMIIDxqCCA8ICAQEwgg07MIICowIB ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAgMAk10MRQwEgYDVQQHDAtNYXBsZSBH cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UECgwDTUpUMRYwFAYDVQQDDA1U ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7G1/ 5z1YrUGOo4dW1/b3o35rpcQQbyOUE0K1NWjaIy4YrRPM9HjhKReThbcSnxddj6eR Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ//Zi08bEPobLv8YnWieNDuw lkaJWWRx3mb1/Yz0f1bwZrKFT3nkrXY0FYmZ0R19W0J+Iin0BtziwiC8DHt+bxST nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9gC47RP9yMjyuuEtpdR9ERoR qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs18zBATRXkk/kRI+Po6cXNJp Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEAYI3DQIDMQ4WDDEwLjAuMTc3 NiMuMjA+BgkahkiG9w0BC04xMTAvMA4GA1UdDwEB/w0EAwICpDAdBgNVH04EFg0U vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCNxUUMTYwNAIBBQwLSVAtMEEw MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b3IMB01NQy5FWEUwZgYKKwYB BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFMAbwBmAHQAdwBh AHIAZQAgAEsAZQB5ACAAUwB0AG8AcgBhAGcAZQAgAFAAcgBvAHYAaQBkAGUAcgMB ADANBgkqhkiG9w0BAQsFAAOCAQEAqtKb5HCh2a1BD2QcKdFuhVQbNxg+G5wcVkZt 7bXdwVuzoAxd9BFd+uVy4D3TmvXtineT3GVWQbKJCcxRZeTKPBFnHG0SeaYupUrG cX4ySsKR1xGSuOhsfIVa/5NXiIYgYxMhlz3nt2CDw+RNqAp/1gLV2cLsui01y5ib 088po4/b9eiXV7A1DWFy7ecw/7Z20a07Sa00aRbwzGJ8He1IiVEjfyAt7KLoufAg LkeSaJtjokkJuGPdr+ykjfuCmIF4hSbcOxzVkPCQbiHOwSxDG1kqYHZ8Xru665Q6 0L7QgBXCc7tcecDieqbYmp50LJPpqEQDQiYjzg57j3eYIFNYYjAAMAAxggGLMIIB hwIBA4AUvruQxeU1yku5Cem3anpu1cbMEDAwDQYJYIZIAWUDBAIBBQCgSjAXBgkq hkiG9w0BC0MxCgYIKwYBB0UHDAIwLwYJKoZIhvcNAQkEMSIEICk1SKp5MUjMa+vr DU1UXU+V05r1F8bNdM0mDgYfmjCiMA0GCSqGSIb3DQEBAQUABIIBAEjqqe4GSGE4 oZQj0vbWrAP0Ab2u8epFm7ZIMZzsJSzR0z98m+R+1R2mCoqWC0SSafybJ701Jhly A3eqzDYxAu9p9drJft317sGAERE/i1D3BFvKZZQH0sz0JNRwDp3qByHHzVCULUEI JSOpYvI1s3S23ZYEed0Lp35Xy87378zLLGLpgGKTK4teav1IitUJwVCKikL47uyF uOY4XLagwI1WWALsPF1+5ZcVNZMvsgzsbuMEXvjBkFKyhMv49oisgFcLJ1AoMtWn 7Mbq8K6ckbKkVpuvmWThkVTp1W3hIS/i/J0X7c2unA25LxAC/P/LyWhPt/Vk/oqf 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.

© MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 51/126Certificates guide - Milestone XProtect® VMSCertificates guide & Comparison of the State of the XProtect® VMS

# MOBOTIX HUB - Certificates Guide - Install certificates for communication with the

↓     ↓     ↓     ↓     Dow       File     Home     S	nloads Share View					-		×
< - · ↑ ↓	This PC > 1	Downloads		~ Ö	Search D	lownloads		p
E Desktop	^ Name		~	Date mod	dified	Туре		Size
Documents     Downloads     Music     Pictures     Videos     Local Disk (C:)	ce	rtnew.	Open Install Certificate Edit with Notepad++ Share Open with	ENGLISH A	42:23 PM	Security Ce	ertificate	
Network	ve	_	Give access to Restore previous versions	>				>
1 item 1 item select	ed 1.11 KB		Send to	>				

×

- 3. Accept the security warning if it appears.
- 4. Select to install the certificate for the local machine and click Next.

Welcome to the	Certificate Import	Wizard	
This wizard helps you co lists from your disk to a	ny certificates, certificate trust ertificate store.	lists, and certificate revocation	
A certificate, which is iss and contains informatior connections. A certificat	ued by a certification authority used to protect data or to esta store is the system area wher	, is a confirmation of your identity ablish secure network re certificates are kept.	
Store Location			
O Current User			
Local Machine			
To continue, click Next.			

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

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 52/ 126Certificates guide - Milestone XProtect® VMSCertificates g XProtect<sup>®</sup> VMS

#### MOBOTIX HUB - Certificates Guide - Install certificates for communication with the

← 🔄 Ertificate Import Wizard	*
Certificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate.	
Automatically select the certificate store based on the type of certificate     Place all certificates in the following store     Certificate store:     Browse	Select Certificate Store × Select the certificate store you want to use.
Next 1	OK Cancel

6. Finish the Install Certificate wizard.

#### 14.3 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.

# MOBOTIX HUB – Certificates Guide - Install certificates for communication with the

Encryption	Encryption	
Registering servers	It is recommended to secure communication with encryption. Learn	more
Language selection	Server certificate Applies to: management server, recording server, failover server, data collector	
	Encryption: On	
	~	Detail
	Carrillicate innued by MS-Organization-P2P-Acoust [2021]. Expires 5/8/2021	
	Mobile streaming media certificate Applies to mobile and web clients that retrieve data streams from the mobile server	
	Encryption: On	
	Marran	Detail
	Cortificate issued by Expires 5/3/2121	
		Apply
		- dele-3

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.

#### 15 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.

#### 15.1 Add a CA certificate to the server

Add the CA certificate to the server by doing the following. On the computer that hosts the MOBOTIX HUB server, open the Microsoft Management Console.

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

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

📟 Run				×
e	Type the name of resource, and W	of a program indows wil	m, folder, docur I open it for you	ment, or Internet
Open:	mmc			×

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

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

Add or Remove Snap-ins

3. Click **OK**.

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For	
extensible snap-ins, you can configure which extensions are enabled.	

×

Snap-in	Vendor	~	Console Root	Edit Extensions.
ActiveX Control	Microsoft Cor	1	Certificates - Current Use	Remove
Authorization Manager	Microsoft Cor			Transford Free
Certificate Templates	Microsoft Cor			
Certificates	Microsoft Cor	16 C		
Component Services	Microsoft Cor	1-2-2-2		Manuel Crown
Computer Managem	Microsoft Cor	Add	×	
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
Description:				
The Certificates snap-in allo	ows you to browse	the contents	of the certificate stores for yourself, a s	ervice, or a computer.
1.0000000000000000000000000000000000000				
				DK Car
				UK Can
mobotiv com				

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 56/ 126Certificates guide - Milestone XProtect® VMSCertificates guide & Milestone XProtect® VM

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.
- 6. Click Next.

Certificate Enrollment

#### Select Certificate Enrollment Policy

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

X

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

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

8.	Expand to view the <b>Detai</b>	s of the custom request, and click <b>Properties</b> .	- 🗆 X
	📮 Certificate Enrollment		
	Custom request		
	Chose an option from	the list below and configure the certificate options as required.	
	Template:	(No template) CNG key	-
		<u>Suppress default extensions</u>	
	Request format:	○ <u>P</u> KCS #10	
		● <u>C</u> MC	
	Note: Key archival is option is specified in	not available for certificates based on a custom certificate reque the certificate template.	st, even when this
			Next Cancel
	The request for error when the sure you choo	mat depends on the CA. If the wrong format is chosen, the CA certificate signing request (CSR) is submitted. Check with the se properly.	will issue an CA to make

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



- 10. On the **Subject** tab, enter the parameters as required by the specific CA.
- 11. 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:

ertificate Propertie	5				×
General Subject B	Extensions	Private Key	Signature		
The subject of a ce can enter informat can be used in a ce	ertificate is tion about ertificate.	the user or c the types of	omputer to v subject name	which the certificate is and alternative name	issued. You e values that
Subject of certifica	te				
The user or compu	uter that is	receiving the	e certificate		
Subject name:		_			
Туре:				CN=Test for Docs	5
Country			Add	OU=MJT Lab	
Value:		~	Remove	L=Maple Grove S=MN C=USA	
Alternative name:		4			
Туре:				1	
Directory name		~			
Value:			Add >		
			Remiave		
			OK	Cancel	Apply

12. 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.

ertificat	e Propert	ties					×
General	Subject	Extensions	Private Key	Signature			
The foll	owing an	e the certific	ate extension	s for this cer	tificate type.	1	•
Key us	sage					~	
The ke	y usage e	extension des	cribes the pu	irpose of a ce	ertificate.	_	
Availat	ole option	15:			Selected options:		
CRL si Data e	gning ncipherm	ient	1		Digital signature Key certificate signin	ig	
Deciph	ner only				Key encipherment		
Key an	reement		A	aa >			
Non re	oudiation	n		relieve to			
⊠ Mak	te these k	ey usages cr	itical				
Extend	ded Key U	lsage (applic	ation policie	5)		•	
Basic	constrain	ts				*	,
				OK	Cancel	Apply	

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

Ì

14. 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 allof the options required before proceeding to the next step.

Certificate F	Properti	es					×
General S	ubject	Extensions	Private Key	Signature			
Cryptog	raphic S	Service Prov	ider				۲
Key opti	ons						*
Set the ke	ey lengt	h and export	t options for	the private k	ey,		
Key size:	2048				~		
Make	private	key exportal	ole				
Allow	private	key to be ar	chived				
Strong	private	key protect	tion				
Select H	ash Alg	orithm					~
Select Ha	ish Algo	orithm to be	used for this	s request			
Hash Alg	orithm:	sha256			~		
Select Si	gnature	Format					~
					_		
				OK	Ca	ncel	Apply

- 15. Unless the CA requires a signature, the next step is to click **OK**.
- 16. When all the certificate properties have been defined, click **Next** on the **Certificate Enrollment** wizard.

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.
 Click **Finish**.

rtificate Enrollment	
Where do you want to save the offline request?	
f you want to save a copy of your certificate request or want to proce	ss the request later, save the reque
to your hard disk or removable media. Enter the location and name of click Finish.	your certificate request, and then
to your hard disk or removable media. Enter the location and name of click Finish. File Name:	your centificate request, and then
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
to your hard disk or removable media. Enter the location and name of click Finish. File Name: C:\Users\Administrator\Desktop\CSR6.1.21 File format:	Browse
to your hard disk or removable media. Enter the location and name of click Finish. File Name: C:\Users\Administrator\Desktop\CSR6.1.21 File format: ) Base 64	Browse

Finish

Cancel

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

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



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.

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

- 🗆 X

File Edit Format View Help ----BEGIN NEW CERTIFICATE REQUEST----MIIGBAYJKoZIhvcNAQcCoIIF9TCCBfECAQMxDzANBg1ghkgBZQMEAgEFADCCBEoG CCsGAQUFBwwcoIIEPASCBDgwggQ0MGQwYgIBAgYKKwYBBAGCNwoKATFRME8CAQAw AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QLTBBMDAwNDY3DB1JUC0wQTAw MDQ2N1xBZG1pbm1zdHJhdG9yDAdNTUMuRVhFMIIDxqCCA8ICA0Ewgg07MIICowIB ADBpM0wwCgYDV00GEwNVU0ExCzAJBgNVBAgMAk10MR0wEgYDV00HDAtNYXBsZSBH cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UECgwDTUpUMRYwFAYDVQQDDA1U ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7G1/ 5z1YrUG0o4dW1/b3o35rpcQQbyOUE0K1NWjaIy4YrRPM9HjhKReThbcSnxddj6eR Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ//Zi08bEPobLv8YnWieNDuw lkaJWWRx3mb1/Yz0f1bwZrKFT3nkrXY0FYmZ0R19W0J+Iin0BtziwiC8DHt+bxST nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9gC47RP9yMjyuuEtpdR9ERoR qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs18zBATRXkk/kRI+Po6cXNJp Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEAYI3DQIDMQ4WDDEwLjAuMTc3 NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/wQEAwICpDAdBgNVHQ4EFgQU vruQxeU1yku5Cem3anpu1cbMEDAwQwY3KwYBBAGCNxUUMTYwNAIBBQwLSVAtMEEw MDA0NjcMGU10LTBBMDAwNDY3XEFkbW1uaXN0cmF0b3IMB01NQy5FWEUwZgYKKwYB BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwByAGYAdAAgAFMAbwBmAHQAdwBh AHIAZQAgAEsAZQB5ACAAUwB0AG8AcgBhAGcAZQAgAFAAcgBvAHYAaQBkAGUAcgMB ADANBgkqhkiG9w0BAQsFAAOCAQEAqtKb5HCh2a1BD2QcKdFuhVQbNxg+G5wcVkZt 7bXdwVuzoAxd9BFd+uVy4D3TmvXtineT3GVWQbKJCcxRZeTKPBFnHG0SeaYupUrG cX4ySsKR1xGSuOhsfIVa/5NXiIYgYxMhlz3nt2CDw+RNgAp/lgLV2cLsui01y5ib 088po4/b9eiXV7A1DWFy7ecw/7Z20a07Sa00aRbwzGJ8He1IiVEjfyAt7KLoufAg LkeSaJtjokkJuGPdr+ykjfuCmIF4hSbcOxzVkPCQbiHOwSxDG1kqYHZ8Xru665Q6 0L7QgBXCc7tcecDieqbYmp50LJPpqEQDQiYjzg57j3eYIFNYYjAAMAAxggGLMIIB hwIBA4AUvruQxeU1yku5Cem3anpu1cbMEDAwDQYJYIZIAWUDBAIBBQCgSjAXBgkg 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**.

↓     ↓     ↓     ↓     Dow       File     Home     S	nload hare	s View					-		×
< - · ↑ ↓	Thi	s PC > Down	nloads		~ Č	Search D	ownloads		P
E. Desktop	^	Name		~	Date mod	lified	Туре		Size
<ul> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>Local Disk (C:)</li> </ul>	ĺ	Certnew	v.	Open Install Certificate Edit with Notepad++ Share Open with	511/2021	12:23 PM	Security C	ertificate	3
Network		<		Give access to Restore previous versions	>				>
1 item 1 item select	ed 1.	11 KB		Send to	>				

- 3. Accept the security warning if it appears.
- 4. 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
------	--------

X

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

© MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 66/ 126Certificates guide - Milestone XProtect® VMSCertificates g XProtect<sup>®</sup> VMS

🗧 🧬 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.	on for
<ul> <li>Automatically select the certificate store based on the type of certificate</li> <li>Place all certificates in the following store</li> <li>Certificate store:</li> <li>Browse</li> </ul>	Select Certificate Store X Select the certificate store you want to use.
	Show physical stores

6. Finish the Install Certificate wizard.

#### 15.3 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.

#### 15.3.1 Prerequisites:

J.

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.

A server authentication certificate is trusted on the computer that hosts the management server First, enable encryption on the management server.

Steps:

- 7. 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
- 1. In the Server Configurator, under Server certificate, turn on Encryption.
- 2. 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.
- 3. Select a certificate to encrypt communication between the recording server, management server, failover server, and Data Collector server.
- 4. Select **Details** to view Windows Certificate Store information about the selected certificate.

Milestone Server Configura	tor	-	LL ×	
Encryption	Encryption			
Registering servers	It is recommended to secure communication with encryption. Learn more			
Language selection	Server certificate Applies to: management server, recording server, failover collector, api gateway, log server	r server, data		
	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 mobile server			
	Encryption: Off			
	Select certificate	~		
	No certificate selected			
			Apply	

5. Click Apply.

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 68/ 126Certificates guide - Milestone XProtect® VMSCertificates g XProtect<sup>®</sup> VMS

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)

### 15.3.2 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.

nod I su kepn	Select one or more roles to install on the select	ted server.
ever te prior	Active Directory Certificate Services	Active Directory Certificate Service
21 million	Ad Ad Ad Ad Ad Ad Ad Ad Ad Ad	uired for Active Directory to manage this feature, but do not server. an Tools ls ificate Services Tools on Authority Management Tools
		(if applicable)

- 6. Click Next.
- 7. In Features, click Next. All of the required features are selected for installation.
- 8. In AD CS, read the description of the Active Directory Certificated Services, and click Next.
- 9. In Role Services, select the following:
  - Certification Authority
  - Certification Enrollment Policy Web Service
  - Certification Enrollment Web Service
  - Certification Authority Web Enrollment
  - Network Device Enrollment Service

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

Add Roles and Features Wiza	ru,				
Select role servi	ces	DESTINATION SERVER IP-0A000450			
Before You Begin	Select the role services to install for Active Directory Ce	ertificate Services			
Server Selection Server Roles Features AD CS	Certification Authority     Certificate Enrollment Policy Web Service     Certificate Enrollment Web Service     Certification Authority Web Enrollment     Network Device Enrollment Service	Network Device Enrollment Service makes it possible to issue and manage certificates for routers and other network devices that do not have network accounts.			
Role Services Web Server Role (IIS) Role Services Confirmation	Online Responder				

- 10. Click Next.
- 11. In Confirmation, select Restart the destination server automatically if required, and click Install.

- 12. When the installation is done, click the  $\ensuremath{\textbf{Close}}$  button.
- 13. Select the Notification Flag in the Server Manager application.



- 14. A message to begin post deployment configuration is listed under the Notification Flag.
- 15. Click on the link to begin the configuration of the installed services.

	• 🕮 I 🧗
A	Post-deployment Configura
	Configuration required for Active Directory Certificate Services at IP-0A000467
ſ	Configure Active Directory Certificate Services on thus
0	Feature installation
	Configuration required. Installation succeeded on IP-0A000467.
	Add Roles and Features
	Task Details

- 16. The Active Directory Certificate Services configuration wizard starts.
- 17. 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.
- 18. Enter the required account information and click **Next**.
| AD CS Configuration          |  |  | $\overline{-}$ |          | ×           |
|------------------------------|--|--|----------------|----------|-------------|
| Credentials                  |  |  | DESTINA        | TION SER | VER<br>)450 |
| Credentials<br>Role Services | Specify credentials to configure role<br>To install the following role services you must belong<br>• Standalone certification authority<br>• Certification Authority Web Enrollment<br>• Online Responder<br>To install the following role services you must belong<br>• Enterprise certification authority<br>• Certificate Enrollment Policy Web Service<br>• Certificate Enrollment Policy Web Service<br>• Certificate Enrollment Web Service<br>• Network Device Enrollment Service | SERVICES<br>to the local Adminis<br>to the Enterprise Ac<br>Change | strators grou  | p:       |             |
|                              | More about AD CS Server Roles  |  |                |          |             |

- 19. In **Role Services**, select the following services:
  - Certification Authority
  - Certification Authority Web Enrollment
- 20. Click Next.

ole Services		DESTINA	IP-0A000	45(
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			

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

The Table	DESTINATION SERVE
etup Type	1P-0A0004
Credentials	Specify the setup type of the CA
Role Services	
Setup Type	Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to
СА Туре	simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.
Private Key	
Cryptography	Enterprise CA Enterprise CAs must be domain members and are typically online to insue certificates or
CA Name	certificate policies.
Validity Period	Standalone (A
Certificate Database	Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require A
Confirmation	DS and can be used without a network connection (offline).
	More about Setup Type
	And Designed and

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

СА Туре	DESTINATION SERVER
Credentials Role Services	Specify the type of the CA
Setup Type	public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its
Private Key	own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.
Cryptography	Root CA
CA Name	Root CAs are the first and may be the only CAs configured in a PKI hierarchy.
Validity Period	C Subordinata CA
Certificate Database	Subordinate CA Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates b
Confirmation	the CA above them in the hierarchy.
	More about CA Type
	New Press of the

23. n Private Key, select the option to create a new private key, and click Next.

Ab co comgulation	/
Private Key	DESTINATION SERVER IP-0A000450
Credentials Role Services	Specify the type of the private key
CA Type Private Key	Create a new private key     Use this option if you do not have a private key or want to create a new private key
Cryptography CA Name Validity Period Certificate Database Confirmation	<ul> <li>Use existing private key</li> <li>Use this option to ensure continuity with previously issued certificates when reinstalling a CA.</li> <li>Select a certificate and use its associated private key</li> <li>Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.</li> <li>Select an existing private key on this computer</li> <li>Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.</li> </ul>
	More about Private Key

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

Click Next.

Cryptography fo	or CA		DESTINATION	ON SERVE
Credentials Role Services Setup Type CA Type	Specify the cryptographic options Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider	¥	Key length: 2048	
Private Key Cryptography CA Name Validity Period Certificate Database Confirmation	Select the hash algorithm for signing certificates issued by SHA256 SHA384 SHA512 SHA1 MD5	accessed b	by the CA.	
	More about Cryptography			

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

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

CA Nama	DESTINATION SERVER
CAINAILE	IP-0A000450
Credentials	Specify the name of the CA
Role Services	
Setup Type	Type a common name to identify this certification authority (CA). This name is added to all
СА Туре	certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.
Private Key	
Cryptography	Common name for this CA:
CA Name	IP-0A000450-CA
Validity Period	Distinguished name suffix:
Certificate Database	
Confirmation	Preview of distinguished name:
	CN=IP-0A000450-CA
	More about CA Name
	More about CA Name

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

📥 AD CS Configuration					÷		×
Validity Period					DESTINA	TION SER	VER 0450
Credentials Role Services	Spec	ify the validit	y period				
Setup Type	Select t	he validity period f	for the certificate generat	ed for this certificat	tion authority (C	:A):	
СА Туре	5	Years	*				
Private Key	CA exp	iration Date: 4/27/2	2026 3:27:00 PM				
Cryptography	The val	idity period config	ured for this CA certificate	e should exceed the	validity period	for the	
CA Name	certifica	ates it will issue.			10-10-1 <b>2</b> ,519-10-2		
Validity Period							
Certificate Database							
Confirmation							
	More a	bout Validity Period	d				
			< Previous	Next >	Configure	Cance	et ]

- 27. 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
- 28. Click Next.
- 29. In **Confirmation**, review the selected configuration options and click **Configure** to begin the process of configuration.
- 30. When the configuration is done, click **Close**.
- 31. When prompted to configure any additional role services, click No.
- 32. Reboot the local server to ensure it is ready to serve as the Active Directory Certificate Server.

# 15.4 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.

#### 15.4.1 Add a CA certificate to the server

Ì

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.

😅 Run			×
e	Type the name of a p resource, and Windo	rogram, folder, docun ws will open it for you	nent, or Internet
<u>O</u> pen:	mmd		¥
	OF	Cancel	Proves

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

Save As Add/Remove Snap-in Ctrl+M Options Recent File Exit	Save As Add/Remove Snap-in Ctrl+M Options Recent File Exit	Save As Add/Remove Snap-in Ctrl+M Options Recent File Exit	
Save As     There are no items to show in this view.     Console root     More Actions       Add/Remove Snap-in     Ctrl+M       Options       Recent File       Exit	Save As     Add/Remove Snap-in     Ctrl+M       Options     Recent File       Exit     Nore Actions	Save As Add/Remove Snap-in Ctrl+M Options Recent File Exit	
Add/Remove Snap-in Ctrl+M Options Recent File Exit	Add/Remove Snap-in Ctrl+M Options Recent File Exit	Add/Remove Snap-in Ctrl+M Options Recent File Exit	
Options Recent File Exit	Options       Recent File       Exit	Options Recent File Exit	
Recent File Exit	Recent File       bit	Recent File Exit	
Exit		Exit	

© MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 81/126Certificates guide - Milestone XProtect® VMSCertificates g XProtect<sup>®</sup> VMS

3. Select the Certificates snap-in and click AddIn Certificates snap-in, select Computer account.

Snanjn	Vandor	~		Console Root	Edit Extensions.
	VENDO	107		Certificates (Local Computer)	Lore Externoionon
Activex Control	Microsoft Cor			and the second second second	Ready's
Certificates	Microsoft Cor				
Component Services	Microsoft Cor				I Mona Ubi
Computer Managem	Microsoft Cor				
B Device Manager	Microsoft Cor				There Dave
Disk Management	Microsoft and		Add >		-
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
and the second				-	
scription:					

4. In Select Computer, select Local computer.

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

COLUMN A PARA			
Select the computer you want this snap-in to r	manage.		
This snap-in will always manage:			
Local computer: (the computer this con	nsole is running on)		
O Another computer:		Browne	

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

ISOIE ROOL		Obje	ct Type			Actions	
Certificates (Li Personal	ocal Computer)	0	ertificates			Personal	
Cert	Find Certificates					More Actions	
Trusted	All Tasks	3	Find Certificates				
interme	View	>	Request New Certificate				
Trusted	New Window from Here		Import				
Third-P	New Taskpad View		Advanced Operations	>	Create Custom Request		
Trusted	Refresh				Manage Enrollment Policies		
Preview	Export List					1	
Test Ro	Help						
AAD To		11					
Certificate	esktop Forollment Requests						
Smart Card	d Trusted Roots						
📃 SMS							
Trusted Ro	ot Certification Authorities						
Trusted De	vices						
Web Hosti	ng Sas ID Tabas Isaas						
Windows I	enverlindateServices						
windows5	erveropuateservices						

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

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 83/ 126Certificates guide - Milestone XProtect® VMSCertificates give Other Contents of the Content of the Conte XProtect<sup>®</sup> VMS



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

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

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	
	(e) ⊆MC	
Note: Key archival is option is specified in	not available for certificates based on a custom certi the certificate template.	ficate request, even when thi

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

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

Coporal		E Contractor	-	-				
A friend Friendly	Subject Ily name a / name:	Extensions and descript	Private Key ion will make	Signature it easier to ide	entify and	l use a certi	ficate.	
TestLa	bDomain,	com						e certificate
Descrip	tion:							
TestLa	bDomain.	com						Details 🔺 ficate:
								operties
								Cance

12. 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.

13. 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 foll	lowing are	e the certific	ate extension	s for this cer	tificate	type.		^
Key us	sage						v	
Extend	ded Key U	sage (applic	ation policie	5)			^	
An app certific certific Availab	ate can b ates issue ble option	e used. Selected by this ter	t the applicanplate.	tion policy r	Selec	for valid si ted option	ines now a ignatures of is: icotion	
Code S Secure Time S Micros IP secu IP secu IP secu IP secu	Email Email Stamping Soft Trust Soft Time urity end s urity tunn urity user	List Signii Stamping system el termina	< R	dd > emove	<	н	2	
Mak	the Exte	ended Key U	sage critical					~

- 14. On the **Private Key** tab, expand the **Key options** menu.
- 15. Set the key size to 2048 and select the option to make the private key exportable. Click **OK**.

	Propert	ies				>
General S	ubject	Extensions	Private Key	Signature		
Cryptog	raphic !	Service Prov	ider			۲
Key opti	ons					*
Set the k	ey lengt	th and expo	t options for	the private key.		
Key size:	2048			~		
Make	private	key exportal	ble		-	
Allow	private	key to be ar	chived			
Strong	private	e key protect	tion			
Select H	ash Alg	orithm				*
Select Ha	sh Algo	orithm to be	used for this	request		
	- differen				1000	
Hash Alg	orithm	SUBST			~	
Hash Alg	oritnm	504230			~	
Hash Alg Select Si	gnature	e Format			~	v
Hash Alg Select Si	gnature	Format			×	~
Hash Alg Select Si	gnature	e Format			×	~

- 16. When all of the certificate properties have been defined, click **Next** on the **Certificate Enrollment** wizard.
- 17. 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.
- 18. 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 p to your hard disk or removable media. Enter the location and nar click Finish.	process the request later, save the requine of your certificate request, and the
File Name: C:\Users\Administrator\Desktop\CSR6.1.21	Browse
File format:	Breathantin
(a) Daga E/	
Base 64     Binary	
<ul> <li>Base 64</li> <li>Binary</li> </ul>	
<ul> <li>Base 64</li> <li>Binary</li> </ul>	

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

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

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

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

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

Ì

i i vi iesti - Notepaŭ	- 0	×
File Edit Format View Help		
BEGIN NEW CERTIFICATE REQUE	ST	
IIIF2AYJKoZIhvcNAQcCoIIFyTCCBcU	AQMxDzANBglghkgBZQMEAgEFADCCE	3B4G
CsGAQUFBwwCoIIEEASCBAwwggQIMGYw	ZAIBAgYKKwYBBAGCNwoKATFTMFECA	AQAw
wIBATFHMEUGC5sGAQQBgjcVFDE4MDYG	AQUMDENsdXN0ZXIxVEVNUAwaQ0xVL	J1RF
jFURU1QXEFkbWluaXN0cmF0b3IMB01N	Qy5FWEUwggOYoIID1AIBATCCA40wg	ggJ1
gEAMBcxFTATBgNVBAMMDENsdXN0ZXI	VEVNUDCCASIwDQYJKoZIhvcNAQEBE	BQAD
gEPADCCAQoCggEBAKVp0982yi05tcny	/paTujsFBe9jwOyRp+c5N00xf8OcN0	Dyg
VMVTSU9s9rTMWmUDzP+zLumOmC6gCW	Co5RgiT+dLjOvq+Z6AUWC1H+WVUsa	/bJc
ktV8ut805gi46dkQ4MD71btX6mnjjUE	3294Xwf8yUVP1Be0dkfqjUVnn6EAYz	zHdS
czK1yUZmY576IBwf6LZMujXbNDD5ZX;	dhG3pggarNdzHvg0RIJvro4IJ0rM6	SEsJ
N2d0SZms4Utj21DekFde3BsENvcvk0	PHZk8b8Bww050+ya3tk7jDbvw0a1	/XE9
qL+Zy4pEP1jKnTwM1IyPmsXyw7gx6Cr	Tw8ntgECAwEAAaCCAS8wHAYKKwYBE	BAGC
w@CAzEOFgwxMC4wLjE0MzkzLjIwRQY	IKwYBBAGCNxUUMTgwNgIBBQwMQ2x1c	:3R1
jFURU1QDBpDTFVTVEVSMVRFTVBcQWRt	caW5pc3RyYXRvcgwHTU1DLkVYRTBgE	Bgkq
kiG9w0BCQ4xUzBRMBMGA1UdJQQMMAo(	GCCsGAQUFBwMBMBsGCSsGAQQBgjcVC	CgQ0
AwwCgYIKwYBBQUHAwEwHQYDVR00BBY	FOBsTd6/Hpi6c18h5HHq88hWc911M	IGYG
isGAQQBgjcNAgIxWDBWAgEAHk4ATQB	AGMAcgBvAHMAbwBmAHQAIABTAG8AZ	ZgBØ
isGAQQBgjcNAgIxWDBWAgEAHk4ATQBp HcAYQByAGUAIABLAGUAeQAgAFMAdAB	DAGMAcgBvAHMAbwBmAHQAIABTAG8AZ /AHIAYQBnAGUAIABQAHIAbwB2AGkAZ	ZgB0 ZAB1
isGAQQBgjcNAgIxWDBWAgEAHk4ATQB HcAYQByAGUAIABLAGUAeQAgAFMAdAB HIDAQAwDQYJKoZIhvcNAQELBQADggEE	DAGMAcgBvAHMAbwBmAHQAIABTAG8AZ AHIAYQBnAGUAIABQAHIAbwB2AGkAZ BAFGoQLCtyivOXG0T0U4MS9VnUS0sQ	ZgBØ ZAB1 QUnN
CisGAQQBgjcNAgIxWDBWAgEAHk4ATQB AHcAYQByAGUAIABLAGUAeQAgAFMAdAB AHIDAQAwDQYJKoZIhvcNAQELBQADggEB )APtDKNDGskV/dq6rqgpYEKiQfWZeSno	DAGMAcgBvAHMAbwBmAHQAIABTAG8AZ /AHIAYQBnAGUAIABQAHIAbwB2AGkAZ 3AFGoQLCtyivOXG0T0U4MS9VnUS0sQ 1EOzxieJtES/1I5hmVUm51TIVydzE8	ZgBØ ZAB1 QUnN BiyW
isGAQQBgjcNAgIxWDBWAgEAHk4ATQB McAYQByAGUAIABLAGUAeQAgAFMAdAB MIDAQAwDQYJKoZIhvcNAQELBQADggEB MAPtDKNDGskV/dq6rqgpYEKiQfWZeSno (jUze/+WIiZifGFnkMKYwrzKgx7qIr)	DAGMAcgBvAHMAbwBmAHQAIABTAG8AZ AHIAYQBnAGUAIABQAHIAbwB2AGkAZ BAFGoQLCtyivOXG0T0U4MS9VnUS0sQ HEOzxieJtES/1I5hmVUm51TIVydzE8 Undo	ZgBØ ZAB1 QUnN BiyW
isGAQQBgjcNAgIxWDBWAgEAHk4ATQB; HcAYQByAGUAIABLAGUAeQAgAFMAdAB HIDAQAwDQYJKoZIhvcNAQELBQADggEB APtDKNDGskV/dq6rqgpYEKiQfWZeSnc (jUze/+WIiZifGFnkMKYwrzKgx7qIr I3dWazix8dSVOQIRZ3Lr7yXg9iiF49	DAGMAcgBvAHMAbwBmAHQAIABTAG8AZ VAHIAYQBnAGUAIABQAHIAbwB2AGkAZ BAFGoQLCtyivOXG0T0U4MS9VnUS0sQ HEOzxieJtES/1I5hmVUm51TIVydzE8 Undo	ZgBØ ZAB1 QUnN BiyW t j
isGAQQBgjcNAgIxWDBWAgEAHk4ATQB McAYQByAGUAIABLAGUAeQAgAFMAdAB MIDAQAwDQYJKoZIhvcNAQELBQADggEB DAPtDKNDGskV/dq6rqgpYEKiQfWZeSno (jUze/+WIiZifGFnkMKYwrzKgx7qIr) M3dWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aH	DAGMAcgBvAHMAbwBmAHQAIABTAG8AZ /AHIAYQBnAGUAIABQAHIAbwB2AGkAZ 3AFGoQLCtyivOXGOT0U4MS9VnUSOsQ HEOzxieJtES/1I5hmVUm51TIVydzE8 Undo Cut	ZgB0 ZAB1 QUnN BiyW t j j
isGAQQBgjcNAgIxWDBWAgEAHk4ATQB HcAYQByAGUAIABLAGUAeQAgAFMAdAB HIDAQAwDQYJKoZIhvcNAQELBQADggEE APtDKNDGskV/dq6rqgpYEKiQfWZeSno jUze/+WIiZifGFnkMKYwrzKgx7qIr 3dWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0	DAGMAcgBvAHMAbwBmAHQAIABTAG8AZ /AHIAYQBnAGUAIABQAHIAbwB2AGkAZ BAFGoQLCtyivOXGOT0U4MS9VnUSOsQ HEOzxieJtES/1I5hmVUm51TIVydzE8 Undo Cut Copy	ZgB0 ZAB1 QUnN BiyW i j J J B
isGAQQBgjcNAgIxWDBWAgEAHk4ATQB HcAYQByAGUAIABLAGUAeQAgAFMAdAB WHIDAQAwDQYJKoZIhvcNAQELBQADggEB APtDKNDGskV/dq6rqgpYEKiQfWZeSno GJUze/+WIiZifGFnkMKYwrzKgx7qIr BdWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQOAF0BsTd6/Hpi6c18h5Hb	DAGMAcgBvAHMAbwBmAHQAIABTAG8AZ VAHIAYQBnAGUAIABQAHIAbwB2AGkAZ BAFGoQLCtyivOXG0T0U4MS9VnUS0sQ HEOzxieJtES/1I5hmVUm51TIVydzE8 Undo Cut Copy Paste	ZgB0 ZAB1 QUnN BiyW t j J B B
isGAQQBgjcNAgIxWDBWAgEAHk4ATQB HcAYQByAGUAIABLAGUAeQAgAFMAdAB HIDAQAwDQYJKoZIhvcNAQELBQADggEB APtDKNDGskV/dq6rqgpYEKiQfWZeSno (jUze/+WIiZifGFnkMKYwrzKgx7qIr) BdWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQOAFOBsTd6/Hpi6c18h5He wYJKoZIhvcNAQkDMQoGCCsGAQUFBw	DAGMAcgBvAHMAbwBmAHQAIABTAG8AZ /AHIAYQBnAGUAIABQAHIAbwB2AGkAZ 3AFGoQLCtyivOXGOT0U4MS9VnUSOsQ HEOzxieJtES/1IShmVUm51TIVydzE8 Undo Cut Copy Paste Dalata	ZgBØ ZAB1 QUnN BiyW t j B B K K K K K K K K K K K K K K K K K
isGAQQBgjcNAgIxWDBWAgEAHk4ATQB HcAYQByAGUAIABLAGUAeQAgAFMAdAB HIDAQAwDQYJKoZIhvcNAQELBQADggE APtDKNDGskV/dq6rqgpYEKiQfWZeSnc jUze/+WIiZifGFnkMKYwrzKgx7qIr 3dWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQOAF0BsTd6/Hpi6c18h5H wYJKoZIhvcNAQkDMQoGCCsGAQUFBw Y6dr8BzietMf5QwmoRNzq8MRGSQiN	DAGMAcgBvAHMAbwBmAHQAIABTAG8AZ AHIAYQBnAGUAIABQAHIAbwB2AGkAZ BAFGoQLCtyivOXGOT0U4MS9VnUSOsQ HEOzxieJtES/1IShmVUm51TIVydzE8 Undo Cut Copy Paste Delete	ZgB0 ZAB1 QUnN BiyW L j J B W I
isGAQQBgjcNAgIxWDBWAgEAHk4ATQB HcAYQByAGUAIABLAGUAeQAgAFMAdAB HIDAQAwDQYJKoZIhvcNAQELBQADggE APtDKNDGskV/dq6rqgpYEKiQfWZeSno jUze/+WIiZifGFnkMKYwrzKgx7qIr 3dWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQOAF0BsTd6/Hpi6c18h5H wYJKoZIhvcNAQkDMQoGCCsGAQUFBw Y6dr8BzietMf5QwmoRNzq8MRGSQiN q73I6NKKLzg7ROhm16Xj7tL4Id2iV	DAGMAcgBvAHMAbwBmAHQAIABTAG8AZ VAHIAYQBnAGUAIABQAHIAbwB2AGkAZ BAFGoQLCtyivOXG0T0U4MS9VnUS0sQ IEOzxieJtES/1IShmVUm51TIVydzE8 Undo Cut Copy Paste Delete Select All	ZgB0 ZAB1 QUnN BiyW t j a b S S V T
isGAQQBgjcNAgIxWDBWAgEAHk4ATQB HcAYQByAGUAIABLAGUAeQAgAFMAdAB HIDAQAwDQYJKoZIhvcNAQELBQADggEH APtDKNDGskV/dq6rqgpYEKiQfWZeSno jUze/+WIiZifGFnkMKYwrzKgx7qIr 3dWazix8dSVOQIRZ3Lr7yXg9iiF49- X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQOAF0BsTd6/Hpi6c18h5HH wYJKoZIhvcNAQkDMQoGCCsGAQUFBw Y6dr8BzietMf5QwmoRNzq8MRGSQiN q73I6NKKLzg7ROhm16Xj7tL4Id2iV WR7EktvnBLYuBQVPGYb+gwd8EfBh9H	AGMAcgBvAHMAbwBmAHQAIABTAG8AZ AHIAYQBnAGUAIABQAHIAbwB2AGkAZ BAFGoQLCtyivOXG0T0U4MS9VnUS0sQ IEOzxieJtES/1I5hmVUm51TIVydzE8 Undo Cut Copy Paste Delete Select All	ZgBØ ZAB1 QUnN BiyW L j ð S S V K
isGAQQBgjcNAgIxWDBWAgEAHk4ATQB HcAYQByAGUAIABLAGUAeQAgAFMAdAB HIDAQAwDQYJKoZIhvcNAQELBQADggE APtDKNDGskV/dq6rqgpYEKiQfWZeSno jUze/+WIiZifGFnkMKYwrzKgx7qIr 3dWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQOAFOBsTd6/Hpi6c18h5H wYJKoZIhvcNAQkDMQoGCCsGAQUFBw Y6dr8BzietMf5QwmoRNzq8MRGSQiN q73I6NKKLzg7ROhm16Xj7tL4Id2iV WR7EktvnBLYuBQVPGYb+gwd8EfBh9 +5Z7i0E2HZpsBrSld1+u89F0Pi+W/a	AGMAcgBvAHMAbwBmAHQAIABTAG8AZ AHIAYQBnAGUAIABQAHIAbwB2AGkAZ BAFGoQLCtyivOXGOTOU4MS9VnUSOsQ BEOzxieJtES/1IShmVUm51TIVydzE8 Undo Cut Copy Paste Delete Select All Right to left Reading order	ZgB0 ZAB1 QUnN BiyW E j B B W E S S S S S S S S S S S S S S S S S S
isGAQQBgjcNAgIxWDBWAgEAHk4ATQB McAYQByAGUAIABLAGUAeQAgAFMAdAB MIDAQAwDQYJKoZIhvcNAQELBQADggE OAPtDKNDGskV/dq6rqgpYEKiQfWZeSno (jUze/+WIiZifGFnkMKYwrzKgx7qIr) M3dWazix8dSVOQIRZ3Lr7yXg9iiF49 M3dWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe P4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQOAFOBsTd6/Hpi6c18h5H WYJKoZIhvcNAQkDMQoGCCsGAQUFBw WYGdr8BzietMf5QwmoRNzq8MRGSQiN G73I6NKKLzg7ROhm16Xj7tL4Id2iV WR7EktvnBLYuBQVPGYb+gwd8EfBh9 S77i0E2HZpsBrS1d1+u89F0Pi+W/a Mi7k+ce+EDoHhXkbSD+fHYFbUqaTV	AGMAcgBvAHMAbwBmAHQAIABTAG8AZ AHIAYQBnAGUAIABQAHIAbwB2AGkAZ BAFGoQLCtyivOXGOTOU4MS9VnUSOsQ BEOzxieJtES/1IShmVUm51TIVydzE8 Undo Cut Copy Paste Delete Select All Right to left Reading order Show Unicode control characters	ZgB0 ZAB1 QUnN SiyW t j a S S V T V S J
isGAQQBgjcNAgIxWDBWAgEAHk4ATQB HcAYQByAGUAIABLAGUAeQAgAFMAdAB HIDAQAwDQYJKoZIhvcNAQELBQADggEH APtDKNDGskV/dq6rqgpYEKiQfWZeSno jUze/+WIIZifGFnkMKYwrzKgx7qIr 3dWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQOAFOBsTd6/Hpi6c18h5HH wYJKoZIhvcNAQkDMQoGCCsGAQUFBw Y6dr8BzietMf5QwmoRNzq8MRGSQiN1 q73I6NKKLzg7ROhm16Xj7tL4Id2iVL WR7EktvnBLYuBQVPGYb+gwd8EfBh9H +5Z7i0E2HZpsBrS1d1+u89F0Pi+W/a Ii7k+ce+EDoHhXkbSD+fHYFbUqaTYL PmPVkUJGJEUMwfo8rb4xb9taP6ycUI 8XTFWM0JCPMykW2	AGMAcgBvAHMAbwBmAHQAIABTAG8AZ AHIAYQBnAGUAIABQAHIAbwB2AGkAZ BAFGoQLCtyivOXG0T0U4MS9VnUS0sQ IEOzxieJtES/1I5hmVUm51TIVydzE8 Undo Cut Copy Paste Delete Select All Right to left Reading order Show Unicode control characters Insert Unicode control character	ZgB0 ZAB1 QUnN BiyW t j a b S V L V C J V V S S
isGAQQBgjcNAgIxWDBWAgEAHk4ATQB AHCAYQByAGUAIABLAGUAeQAgAFMAdAB AHIDAQAwDQYJKoZIhvcNAQELBQADggEB DAPtDKNDGskV/dq6rqgpYEKiQfWZeSno (jUze/+WIiZifGFnkMKYwrzKgx7qIr) adWazix8dSVOQIRZ3Lr7yXg9iiF49- X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQOAFOBsTd6/Hpi6c18h5H wYJKoZIhvcNAQkDMQoGCCsGAQUFBw Y6dr8BzietMf5QwmoRNzq8MRGSQiN -q73I6NKKLzg7ROhm16Xj7tL4Id2iV WR7EktvnBLYuBQVPGYb+gwd8EfBh90 +5Z7i0E2HZpsBrS1d1+u89F0Pi+W/a Ii7k+ce+EDoHhXkbSD+fHYFbUqaTV PmPVkUJGJEUMwfo8rb4xb9taP6ycU 8XTFWM0JCPMykW2 END NEW CERTIFICATE REQUES	AGMAcgBvAHMAbwBmAHQAIABTAG8AZ AHIAYQBnAGUAIABQAHIAbwB2AGkAZ BAFGoQLCtyivOXGOT0U4MS9VnUS0sQ BOzxieJtES/1IShmVUm51TIVydzE8 Undo Cut Copy Paste Delete Select All Right to left Reading order Show Unicode control characters Insert Unicode control character Open IME	ZgB0 ZAB1 QUnN BiyW t j a B S V T V S S

- 2. Copy the entire contents of the file. This includes the dashed lines marking the beginning and the end of the Certificate Request.
- 3. Open a web browser and enter the address of the Domain CA.

Microsoft Active Directory Certif × +	0		-	~
← → C A Not secure   10.0.4.103/certsrv/	☆	:	Update	• 1)
Microsoft Active Directory Certificate Services – IP-0A000467-CA			ľ	lome

#### 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>

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

~	IVIICIO	DSOIL A	cuve L	Directory Cer		^	٦										
4	3	C	A	Not secur	2   1	10.0	.4.1	03	10	CE	rt	SIL	/c	ert	rqu	15,3	sp
			-			P	-				D.	٥/	00	0.4	67	CA	-
MICI	osofi	Active	Dire	ctory Certifi	ate	Sen	vice	S -			-	ur	100	104	01-	-	۰.
Mici	osofi	Active	Dire	ctory Certifi	cate	Serv	lce	S -			1	ur	100	104	01-	-Cor	
Req	uest	a Ce	ertifi	ctory Certifi cate	cate	Serv	VICE	S-			1	Ur	100	104	01-		
Req Sele	uest ect th	a Ce	ertifica	ctory Certin cate ite type:	cate	Serv	/ice	S -			2	Ur			01-		
Req Sele	uest ect th /eb E	a Ce e cer Brows	ertifica	cate cate te type: Certificate	ate	Sen	/ICe	S -									

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 Certificate S	ervices - CLUSTER2TEM	MP-CA	Home
ubmit a Cer	tificate Request o	Renewal Request		
o submit a sa enewal reque	aved request to the est generated by an	CA, paste a base-64- external source (such	-encoded CMC or PKCS #10 co h as a Web server) in the Saved	ertificate request or PKCS #7 d Request box.
ived Request:				
ase-64-encodec ertificate reques CMC or KCS #10 or KCS #7):	INKVERTURLING r+52710E2HZpaBrS nli7k+c+4ED0HhXk 2PmPVkUJGJEUMwfc TSXTFWMOJCPMykk2 END NEW CER	PGID+GWAUELBHUK9QGWU ldl+uB9FOP1+W/AB/YW bSD+fHYFbUgaTVDfgU4 8rb4xb9taP6ycUZwieL TIFICATE REQUEST	dormu 78hAl. uSPg6 rNWw31	
ditional Attrib	outes:			
Attributes	-k	, 0		

#### 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.

#### 15.5 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.
- 4. Select to install the certificate for the current user and click Next.

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

X

weicome	the Certin	ficate Impor	t Wizard	
This wizard helps lists from your di	; you copy certifica sk to a certificate	ates, certificate tru store.	ist lists, and certific	ate revocation
A certificate, whi and contains info connections. A c	ich is issued by a c rmation used to p ertificate store is	certification author protect data or to e the system area w	ty, is a confirmation stablish secure net here certificates are	n of your identit work e kept,
Store Location				
Current Us     O Local Mach	er ine			
To continue, click	Next.			

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

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

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

8	File	Action	View	Favorites	Window	Help	
4	-		KE		B 7		

Console Root	Issued To	~	Issued	і Ву	Expiration
<ul> <li>Questificates (Local Computer)</li> <li>Personal</li> </ul>	Cluster175	Open	CLUS	TER2TEMP-CA	10/26/202
Trusted Root Certification Authorit	tie	All Tasks	> 0	pen	
<ul> <li>Enterprise Trust</li> <li>Intermediate Certification Authori</li> </ul>	tie	Cut	Re	quest Certificate with New	v Key
<ul> <li>Trusted Publishers</li> <li>Untrusted Certificates</li> </ul>		Delete	M	anage Private Keys	Keym
<ul> <li>Third-Party Root Certification Aut</li> <li>Certificates</li> </ul>	ho	Properties	Ac	dvanced Operations	>
Trusted People		Help	Ex	port	

- 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.
- 9. 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.

#### 15.5.1 Enable server encryption for Management Servers and Recording Servers

- Once the certificate is installed with the correct properties and permissions, do the following.
  - 10. 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
  - 11. In the Server Configurator, under Server certificate, turn on Encryption.
  - 12. 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.
  - 13. Select a certificate to encrypt communication between the recording server, management server, failover server, and data collector server.
  - 14. 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.

	-		X
Encryption			
It is recommended to secure communication with encryption.	earn m	ore	
Server certificate Applies to: management server, recording server, failover server, data collector			
Encryption: On	0		
1		Detail	in a
Carolicate issued by MS-Grgaostation-P2H-Actess (2021), Explore 5/8/2021			
Streaming media certificate Applies to clients and servers that retrieve data streams from the recording server	g		
Encryption: On	0		
terrene v		Details	
Cartillinian Instant by MS-Degarezansis 929-Access (2023), Institut 5/8/2023			
	Encryption         It is recommended to secure communication with encryption.         Server certificate         Applies to: management server, recording server, failover server, data collector         Encryption: On         Certificate is to lenses by ME-Organization P2R-Access (2021), Explores 5/4/2021         Streaming media certificate         Applies to clients and servers that retrieve data streams from the recording server.         Encryption: On         Encryption: On	Encryption   Server certificate   Applies to: management server, recording server, failover server, data collector   Encryption: On   Control on the MSD-Organization P2P-Action (2021) Support SUR2001   Streaming media certificate   Agrees to clients and servers that retrieve data streams from the recording server.   Encryption: On   Control on the server of the Support SUR2001   Streaming media certificate   Agrees to clients and servers that retrieve data streams from the recording server.   Encryption: On   Control on the server SUR2001	Encryption   Server certificate   Applies to: management server, recording server, failover server, data   collector   Encryption: On   Certificate is used by MS-Degeneration #284 Access [0021], brainers \$48/2001   Streaming media certificate   Applies to clients and servers that retrieve data streams from the recording   Encryption: On   Certificate locients and servers that retrieve data streams from the recording   Encryption: On   Certificate locients and servers that retrieve data streams from the recording   Encryption: On   Certificate locients and servers that retrieve data streams from the recording   Encryption: On   Certificate locients and servers that retrieve data streams from the recording   Encryption: On   Certificate locients and servers that retrieve data streams from the recording   Encryption: On   Certificate locient and locients B(84 Access [2021], brainers \$48/2021

15. 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.

### 16 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 like both the domain and commercial CA scenarios.

#### 16.1 Add a CA certificate to the server

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

16. On the computer that hosts the MOBOTIX HUB server, open the Microsoft Management Console.

😅 Run	c .	×
Ð	Type the name of a program, folder, document resource, and Windows will open it for you.	, or Internet
Open:	mmd	×
	OK Cancel	Browse

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

Open C	trl+0 Name		Actions	
Save As	_tn+5	There are no items to show in this view.	Console Root	
Add/Remove Snap-in Ct	tri+M		More Actions	
Options				
Recent File				
Exit				

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

© MOBOTIX AG www.mobotix.com	N A		D	<b>~</b> '	ТІ	1
Mx_GL_MX_HUB_Certificates_V2-04_EN.docx • 04.03.2025 • Page 96/ 126Certificates guide - Milestone XProtect® VMSCertificates g	guide	Nilesto	<b>h</b> 2			1
XProtect <sup>®</sup> VMS						

19. Click **OK**.

allable snap-ins:		-		Selected shap-ins:	
Snap-in	Vendor	^		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor			Certificates (Local Computer)	
Authorization Manager	Microsoft Cor				Riemove
Certificates	Microsoft Cor	Ξ			
Component Services	Microsoft Cor				Move Lip
Computer Managem	Microsoft Cor				
Device Manager	Microsoft Cor		1		Moye 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	ш			
IP Security Policy M	Microsoft Cor	~		1	Advanced
scription:					
C. F. S.	the second de borning	-	materia - Film	with the stress for a world a second	an a summer day

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

onsole Root Certificates	Current User	Object T	Type Ficates	
Tri	Find Certificates			
En	All Tasks	>	Find Certificates	
Ac	View	>	Request New Certificate	
	New Window from Here		Import	
Th	New Taskpad View		Advanced Operations	Create Custom Request
🚞 Tri	Refresh			Enroll On Behalf Of
Cli	Export List			Manage Enrollment Policies
📄 Sn	Help			

- 21. Click Next in the Certificate Enrollment wizard and select Proceed without enrollment policy.
- 22. Click Next.

# MOBOTIX HUB – Certificates Guide - Install certificates in a Workgroup environment

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

Custom request			
Chose an option from	the list below and configure the certificate options as required.		
Template:	(No template) CNG key		
	Suppress default extensions		
Request format:	O <u>P</u> KCS #10		
	● <u>C</u> MC		
Note: Key archival is option is specified in	not available for certificates based on a custom certificate reques the certificate template.	t, even v	vhen t

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

# MOBOTIX HUB – Certificates Guide - Install certificates in a Workgroup environment

Click Next to use the options alread request, and then click Next.	y selected for this template, or click Details to cu	istomize the certificat
Custom request	i) STATUS: Available	Details ^
The following options describ Key usage: Application policies: Validity period (days):	e the uses and validity period that apply to this t	ype of certificate: Properties

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

# MOBOTIX HUB - Certificates Guide - Install certificates in a Workgroup environment

General	Subject	Extensions	Private Kev	Signature		
A friend Friendh	dly name / name:	and descript	tion will make	e it easier to identi	fy and use a cert	ificate.
TestLa	bDomain.	com				
Descrip	tion:					
TestLa	bDomain.	com				

- 26. On the **Subject** tab, enter the required parameters for the subject name.
- 27. In the subject name **Type**, enter in **Common Name** the host name of the computer where the certificate will be installed.

# MOBOTIX HUB - Certificates Guide - Install certificates in a Workgroup environment

General	Subject	Extensions	Private Key	Signature	
The sub can ent can be Subject The use	er inform used in a of certifi or or com	certificate is ation about certificate. cate puter that is	the user or ci the types of s receiving the	omputer to v subject name certificate	which the certificate is issued. You and alternative name values that
Subject	name:		Ti l		CN=MJT-12A
Type:				< bba	
Comn	non name	e	1 1 1	1	
Value			<	Remove	
Alternat	tive name	e	-1		
Type:	_				
Direct	ory name				
Value		_		≤ bbA	
			ĸ	Remove	

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

# MOBOTIX HUB – Certificates Guide - Install certificates in a Workgroup environment

General	Shiert	Extensions	Drivate Key	Sanahare			
General	Subject		Frivate Ney	Signature	a contra		_
The foll	owing are	e the certific	ate extension	s for this cer	tificate type.	-	^
Key us	sage					v	
Extend	led Key U	sage (applic	ation policies	5)		~	
An app certific certific Availab	olication p ate can b ates issue	oolicy (called e used. Selec ed by this ter is:	l enhanced k ct the applica nplate.	ey usage in l tion policy r	Windows 2000) defi equired for valid sig Selected options	nes how a gnatures of	10
Code S Secure Time S Micros IP secu IP secu IP secu	Email Email Contracts Cont	List Signii Stamping system el termina	< R.	dd > emove	C III	otion 2	
Mak	the Exte	ended Key U	sage critical				~

- 29. On the **Private Key** tab, expand the **Key options** menu.
- 30. Set the key size to 2048 and select the option to make the private key exportable. Click **OK**.

# MOBOTIX HUB – Certificates Guide - Install certificates in a Workgroup environment

Certificate F	ropert	ies				>
General S	ubject	Extensions	Private Key	Signature		
Cryptog	raphic !	Service Prov	ider			۷
Key optio	ons					*
Set the ke	ey lengt	th and expo	rt options for	the private key.		
Key size:	2048			~		
Make	orivate	key exporta	ble		4	
Allow	private	key to be an	chived			
Strong	private	e kev protec	tion			
	P	- ary proves				
Select Ha	ach Ala	orithm				
Select Ha	sh Algo	prithm to be	used for this	request		
Hash Alg	orithm	sha256			~	
Select Si	gnature	e Format				*
				_		
				OK	Cancel	Apply

- **31.** When all of the certificate properties have been defined, click **Next** on the **Certificate Enrollment**
- 32. wizard.
- 33. 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.
- 34. Click Finish.

ertificate Enrollment	
Where do you want to save the offline request?	
If you want to save a copy of your certificate request or want to prote your hard disk or removable media. Enter the location and nam click Finish.	ocess the request later, save the rea e of your certificate request, and th
File Name:	procession
File Name: C:\Users\Administrator\Desktop\CSR6.1.21	Browse
File Name: C:\Users\Administrator\Desktop\CSR6.1.21 File format:	Browse
File Name: C:\Users\Administrator\Desktop\CSR6.1.21 File format: Base 64 Binany	Browse
File Name: C:\Users\Administrator\Desktop\CSR6.1.21 File format: Base 64 Binary	Browse

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

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

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

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

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

Ì

ile Edit Format View Help	
BEGIN NEW CERTIFICATE RE	OUEST
IIIF2AYJKoZIhvcNAOcCoIIFyTCCB	CUCAOMxDzANBg1ghkgBZOMEAgEFADCCBB4G
C5GAOUFBwwCoIIEEASCBAwwggOIM	IGYWZAIBAgYKKWYBBAGCNWoKATFTMFECAOAW
wIBATFHMEUGCSsGA00BgicVFDE4M	1DYCA0UMDENsdXN0ZXIxVEVNUAwa00xVU1RF
jFURU10XEFkbWluaXN0cmF0b3IMB	301NOy5FWEUwggOYoIID1AIBATCCA40wggJ1
gEAMBcxFTATBgNVBAMMDENsdXN0Z	XIxVEVNUDCCASIwDQYJKoZIhvcNAQEBBQAD
gEPADCCAQoCggEBAKVp0982yi05t	cnypaTujsFBe9jwOyRp+c5N00xf8OcN0Dyg
VMVTSU9s9rTMWmUDzP+zLumOmC6g	cWIo5RgiT+dLjOvq+Z6AUWC1H+WVUsaVbJc
ktV8ut805gi46dkQ4MD71btX6mnj	jUB294Xwf8yUVP1Be0dkfqjUVnn6EAYzHdS
czK1yUZmY576IBwf6LZMujXbNDD5	ZXzdhG3pggarNdzHvg0RIJvro4IJ0rM6EsJ
N2d0SZms4Utj21DekFde3BsENvcv	/k0/PHZk8b8Bww050+ya3tk7jDbvw0a1VXE9
qL+Zy4pEP1jKnTwM1IyPmsXyw7gx	c6CrTw8ntgECAwEAAaCCAS8wHAYKKwYBBAGC
w@CAzEOFgwxMC4wLjE0MzkzLjIwR	QYJKwYBBAGCNxUUMTgwNgIBBQwMQ2x1c3R1
jFURU1QDBpDTFVTVEVSMVRFTVBcQ	WRtaW5pc3RyYXRvcgwHTU1DLkVYRTBgBgkq
kiG9w0BCQ4xUzBRMBMGA1UdJQQMM	AoGCCsGAOUFBwMBMBsGCSsGA00BgicVCg00
AwwCgYIKwYBBQUHAwEwHQYDVRØOB	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG
AwwCgYIKwYBBQUHAwEwHQYDVR0OB isGAQQBgjcNAgIxWDBWAgEAHk4AT	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG FQBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0
AwwCgYIKwYBBQUHAwEwHQYDVR0OB isGAQQBgjcNAgIxWDBWAgEAHk4AT HcAYQByAGUAIABLAGUAeQAgAFMAd	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG TQBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 MABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1
AwwCgYIKwYBBQUHAwEwHQYDVR0OB isGAQQBgjcNAgIxWDBWAgEAHk4AT HcAYQByAGUAIABLAGUAeQAgAFMAd HIDAQAwDQYJKoZIhvcNAQELBQADg	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG TQBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 ggEBAFGoQLCtyiv0XG0T0U4MS9VnUS0sQUnN
AwwCgYIKwYBBQUHAwEwHQYDVR0OB isGAQQBgjcNAgIxWDBWAgEAHk4AT HcAYQByAGUAIABLAGUAeQAgAFMAd HIDAQAwDQYJKoZIhvcNAQELBQADg APtDKNDGskV/dq6rqgpYEKiQfWZe	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG TQBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 ggEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN SndEOzxieJtES/1I5hmVUm51TIVydzE8iyW
AwwCgYIKwYBBQUHAwEwHQYDVR0OB isGAQQBgjcNAgIxWDBWAgEAHk4AT HcAYQByAGUAIABLAGUAeQAgAFMAd HIDAQAwDQYJKoZIhvcNAQELBQADg APtDKNDGskV/dq6rqgpYEKiQfWZe jUze/+WIiZifGFnkMKYwrzKgx7qI	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG TQBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 IABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 ggEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN SndEOzxieJtES/1I5hmVUm51TIVydzE8iyW
AwwCgYIKwYBBQUHAwEwHQYDVR0OB isGAQQBgjcNAgIxWDBWAgEAHk4AT HcAYQByAGUAIABLAGUAeQAgAFMAd HIDAQAwDQYJKoZIhvcNAQELBQADg APtDKNDGskV/dq6rqgpYEKiQfWZe jUze/+WIiZifGFnkMKYwrzKgx7qI 3dWazix8dSVOQIRZ3Lr7yXg9iiF4	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG TQBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 IABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 ggEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN SndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Invundo
AwwCgYIKwYBBQUHAwEwHQYDVR0OB isGAQQBgjcNAgIxWDBWAgEAHk4AT HcAYQByAGUAIABLAGUAeQAgAFMAd HIDAQAwDQYJKoZIhvcNAQELBQADg APtDKNDGskV/dq6rqgpYEKiQfWZe jUze/+WIIZifGFnkMKYwrzKgx7qI 3dWazix8dSVOQIRZ3Lr7yXg9iiF4 X7yVZFyEAs/6uoApcKXc2KPgBP8a	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG TQBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 AABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 ggEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN eSndEOzxieJtES/1I5hmVUm51TIVydzE8iyW In Undo j aH Cut 9
AwwCgYIKwYBBQUHAwEwHQYDVR0OB isGAQQBgjcNAgIxWDBWAgEAHk4AT HcAYQByAGUAIABLAGUAeQAgAFMAd HIDAQAwDQYJKoZIhvcNAQELBQADg APtDKNDGskV/dq6rqgpYEKiQfWZe jUze/+WIiZifGFnkMKYwrzKgx7qI 3dWazix8dSVOQIRZ3Lr7yXg9iiF4 X7yVZFyEAs/6uoApcKXc2KPgBP8a p4XCYYiuyw/+iHqyNca2fvIIm8Hp	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG TQBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 IABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 gEBAFGoQLCtyiv0XG0T0U4MS9VnUS0sQUnN eSndEOzxieJtES/1I5hmVUm51TIVydzE8iyW In Undo Jahk Cut Jahk Copy
AwwCgYIKwYBBQUHAwEwHQYDVR0OB isGAQQBgjcNAgIxWDBWAgEAHk4AT HcAYQByAGUAIABLAGUAeQAgAFMAd HIDAQAwDQYJKoZIhvcNAQELBQADg APtDKNDGskV/dq6rqgpYEKiQfWZe jUze/+WIIZifGFnkMKYwrzKgx7qI 3dWazix8dSVOQIRZ3Lr7yXg9iiF4 X7yVZFyEAs/6uoApcKXc2KPgBP8a p4XCYYiuyw/+iHqyNca2fvIIm8Hp zCCAYcCAQOAF0BsTd6/Hpi6c18h5	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG TQBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 AABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 ggEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN SndEOzxieJtES/1I5hmVUm51TIVydzE8iyW In Undo 19- aHe Cut bbl Copy Hi Paste
AwwCgYIKwYBBQUHAwEwHQYDVR0OB isGAQQBgjcNAgIxWDBWAgEAHk4AT HCAYQByAGUAIABLAGUAeQAgAFMAd HIDAQAwDQYJKoZIhvcNAQELBQADg APtDKNDGskV/dq6rqgpYEKiQfWZe jUze/+WIIZifGFnkMKYwrzKgx7qI 3dWazix8dSVOQIRZ3Lr7yXg9iiF4 X7yVZFyEAs/6uoApcKXc2KPgBP8a p4XCYYiuyw/+iHqyNca2fvIIm8Hp zCCAYcCAQOAFOBsTd6/Hpi6c18h5 wYJKoZIhvcNAQkDMQoGCCsGAQUFB	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG TQBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 ggEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN eSndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Cn Undo i aHc Cut Delete Delete
AwwCgYIKwYBBQUHAwEwHQYDVR0OB isGAQQBgjcNAgIxWDBWAgEAHk4AT HcAYQByAGUAIABLAGUAeQAgAFMAd HIDAQAwDQYJKoZIhvcNAQELBQADg APtDKNDGskV/dq6rqgpYEKiQfWZe jUze/+WIIZifGFnkMKYwrzKgx7qI 3dWazix8dSVOQIRZ3Lr7yXg9iiF4 X7yVZFyEAs/6uoApcKXc2KPgBP8a p4XCYYiuyw/+iHqyNca2fvIIm8Hp zCCAYcCAQOAFOBsTd6/Hpi6c18h5 wYJKoZIhvcNAQkDMQoGCCsGAQUFB Y6dr8BzietMf5QwmoRNzq8MRGSQi	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG TQBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 IABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 ggEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN SndEOzxieJtES/1I5hmVUm51TIVydzE8iyW In Undo I9 aHe Cut bbl Copy HI Paste IN Delete
AwwCgYIKwYBBQUHAwEwHQYDVR0OB isGAQQBgjcNAgIxWDBWAgEAHk4AT HCAYQByAGUAIABLAGUAeQAgAFMAd HIDAQAwDQYJKoZIhvcNAQELBQADg APtDKNDGskV/dq6rqgpYEKiQfWZe jUze/+WIIZifGFnkMKYwrzKgx7qI 3dWazix8dSV0QIRZ3Lr7yXg9iiF4 X7yVZFyEAs/6uoApcKXc2KPgBP8a p4XCYYiuyw/+iHqyNca2fvIIm8Hp zCCAYcCAQOAFOBsTd6/Hpi6c18h5 wYJKoZIhvcNAQkDMQoGCCsGAQUFB Y6dr8BzietMf5QwmoRNzq8MRGSQi q7316NKKLzg7ROhm16Xj7tL4Id2i	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG TQBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 ggEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN SndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Ln Undo 19- aHc Cut bb Copy Paste N Delete Select All
AwwCgYIKwYBBQUHAwEwHQYDVR00B isGAQQBgjcNAgIxWDBWAgEAHk4AT HCAYQByAGUAIABLAGUAeQAgAFMAd HIDAQAwDQYJKoZIhvcNAQELBQADg APtDKNDGskV/dq6rqgpYEKiQfWZe jUze/+WIIZifGFnkMKYwrzKgx7qI 3dWazix8dSVOQIRZ3Lr7yXg9iiF4 X7yVZFyEAs/6uoApcKXc2KPgBP8a p4XCYYiuyw/+iHqyNca2fvIIm8Hp zCCAYcCAQOAFOBsTd6/Hpi6c18h5 wYJKoZIhvcNAQkDMQoGCCsGAQUFB Y6dr8BzietMf5QwmoRNzq8MRGSQi q73I6NKKLzg7ROhm16Xj7tL4Id2i	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG TQBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 ggEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN eSndEOzxieJtES/1I5hmVUm51TIVydzE8iyW C Undo H Cut Delete N Delete Select All Distant of Baseding and a
AwwCgYIKwYBBQUHAwEwHQYDVR00B isGAQQBgjcNAgIxWDBWAgEAHk4AT HCAYQByAGUAIABLAGUAeQAgAFMAd HIDAQAwDQYJKoZIhvcNAQELBQADg APtDKNDGskV/dq6rqgpYEKiQfWZe jUze/+WIIZifGFnkMKYwrzKgx7qI 3dWazix8dSVOQIRZ3Lr7yXg9iiF4 X7yVZFyEAs/6uoApcKXc2KPgBP8a p4XCYYiuyw/+iHqyNca2fvIIm8Hp zCCAYcCAQOAF0BsTd6/Hpi6c18h5 wYJKoZIhvcNAQkDMQoGCCsGAQUFB Y6dr8BzietMf5QwmoRNzq8MRGSQi q73I6NKKLzg7ROhm16Xj7tL4Id2i wR7EktvnBLYuBQVPGYb+gwd8EfBh +527i0E2HZpsBrS1d1+u89F0Pi+W	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG QBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 gEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN SndEOzxieJtES/1I5hmVUm51TIVydzE8iyW LPUNdo Undo Pate Cut Delete NI Delete Select All NI Right to left Reading order
AwwCgYIKwYBBQUHAwEwHQYDVR00B isGAQQBgjcNAgIxWDBWAgEAHk4AT HCAYQByAGUAIABLAGUAeQAgAFMAd HIDAQAwDQYJKoZIhvcNAQELBQADg APtDKNDGskV/dq6rqgpYEKiQfWZe jUze/+WIIZifGFnkMKYwrzKgx7qI 3dWazix8dSV0QIRZ3Lr7yXg9i1F4 X7yVZFyEAs/6uoApcKXc2KPgBP8a p4XCYYiuyw/+iHqyNca2fvIIm8Hp zCCAYcCAQ0AF0BsTd6/Hpi6c18h5 wYJKoZIhvcNAQkDMQoGCCsGAQUFB Y6dr8BzietMf5QwmoRNzq8MRGSQi q7316NKKLzg7ROhm16Xj7tL4Id2i wR7EktvnBLYuBQVPGYb+gwd8EfBh +5Z7i0E2HZpsBrS1d1+u89F0Pi+W Ii7k+ce+EDoHhXkbSD+fHYFbUqaT	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG QBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 gEBAFGoQLCtyiv0XG0T0U4MS9VnUS0sQUnN SndEOzxieJtES/1I5hmVUm51TIVydzE8iyW L Undo Undo Cut Copy Paste Delete Select All Select All Right to left Reading order Show Unicode control characters
AwwCgYIKwYBBQUHAwEwHQYDVR00B isGAQQBgjcNAgIxWDBWAgEAHk4AT HcAYQByAGUAIABLAGUAeQAgAFMAd HIDAQAwDQYJKoZIhvcNAQELBQADg APtDKNDGskV/dq6rqgpYEKiQfWZe jUze/+WIIZifGFnkMKYwrzKgx7qI 3dWazix8dSVOQIRZ3Lr7yXg9iiF4 K7yVZFyEAs/6uoApcKXc2KPgBP8a p4XCYYiuyw/+iHqyNca2fvIIm8Hp zCCAYcCAQOAF0BsTd6/Hpi6c18h5 wYJKoZIhvcNAQkDMQoGCCsGAQUFB Y6dr8BzietMf5QwmoRNzq8MRGSQi q73I6NKKLzg7R0hm16Xj7tL4Id2i WR7EktvnBLYuBQVPGYb+gwd8EfBh +5Z7i0E2HZpsBrS1d1+u89F0Pi+W Ii7k+ce+EDoHhXkbSD+fHYFbUqaT PmPVkUJGJEUMwfo8rb4xb9taP6yc 8XTFWM0JCPMvkW2	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG QBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 gEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN SndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Cut Undo Undo Cut Copy Paste Delete Select All Right to left Reading order Show Unicode control characters Insert Unicode control character > 3
AwwCgYIKwYBBQUHAwEwHQYDVR00B isGAQQBgjcNAgIxWDBWAgEAHk4AT HcAYQByAGUAIABLAGUAeQAgAFMAd HIDAQAwDQYJKoZIhvcNAQELBQADg APtDKNDGskV/dq6rqgpYEKiQfWZe jUze/+WIIZifGFnkMKYwrzKgx7qI 3dWazix8dSVOQIRZ3Lr7yXg9iiF4 X7yVZFyEAs/6uoApcKXc2KPgBP8a p4XCYYiuyw/+iHqyNca2fvIIm8Hp zCCAYcCAQOAFOBsTd6/Hpi6c18h5 wYJKoZIhvcNAQkDMQoGCCsGAQUFB Y6dr8BzietMf5QwmoRNzq8MRGSQi q73I6NKKLzg7ROhm16Xj7tL4Id2i WR7EktvnBLYuBQVPGYb+gwd8EfBh +5Z7i0E2HZpsBrS1d1+u89F0Pi+W Ii7k+ce+EDoHhXkbSD+fHYFbUqaT PmPVkUJGJEUMwfo8rb4xb9taP6yc 8XTFWMOJCPMykW2 END NEW CERTIFICATE REOU	BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG QBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 gEBAFGoQLCtyiv0XG0T0U4MS9VnUS0sQUnN SndEOzxieJtES/1I5hmVUm51TIVydzE8iyW C Undo Undo Cut Copy Paste Delete Select All Select All Right to left Reading order Show Unicode control characters Insert Unicode control character > Den IME

- 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.

© MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 105/ 126Certificates guide - Milestone XProtect® VMSCertificates SM OBSECTIX XProtect<sup>®</sup> VMS

#### MOBOTIX HUB – Certificates Guide - Install certificates in a Workgroup environment

Microsoft Active Directory Certif × +	0	-	^
← → C ▲ Not secure   10.0.4,103/certsrv/	4	Lupdat	ie :)
Microsoft Active Directory Certificate Services - IP-0A000467-CA			Ног

#### 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>

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

0	Micr	osoft A	ctive Directory Certi	F × +
4	÷	C	A Not secure	10.0.4.103/certsrv/certrqus.asp
Micr	rosof	t Active	Directory Certific	ate Services - IP-0A000467-CA
Req	ues	t a Ce	ertificate	
Sele	ect th	ne cer	tificate type:	

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.

# MOBOTIX HUB - Certificates Guide - Install certificates in a Workgroup environment

crosoft Active Directory Certificate Services - CLUSTER2TEMP-CA	Home
Ivanced Certificate Request	
e policy of the CA determines the types of certificates you can request. Click one	of the following options to:
Create and submit a request to this CA.	
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file.	or submit a renewal request by
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, using a base-64-encoded PKCS #7 file.	or submit a renewal request by
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, using a base-64-encoded PKCS #7 file.	or submit a renewal request by
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, using a base-64-encoded PKCS #7 file.	or submit a renewal request by

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

	110, 100, 100, 100, 100, 100, 100, 100,	Microsoft Active Directory	
Nicrosoft Activ	ve Directory Certificate Serv	ices - CLUSTER2TEMP-CA	Home
ubmit a Ce	ertificate Request or F	Renewal Request	
o submit a s newal requ	saved request to the C lest generated by an e	A, paste a base-64-encoded CMC or PKCS #10 ce xternal source (such as a Web server) in the Saved	ntificate request or PKCS #7 I Request box.
ived Reques	1WR7EktynBLYuBOVPO	Yb+awd8Ef8b9K9Qayd5fMu	
ase-64-encode	ed r+52710E2H2psBrS1c	ll+u89F0Pi+W/a8/YV7BhAl:^	
MC or	2PmPVkUJGJEUMwfo81 T8XTFWM0JCPMvkW2	b4xb9taP6ycUZwieLrNWw3)	
(CS #7):	END NEW CERTI	FICATE REQUEST	
dditional Attr	ibutes:		
	es:	0	
Attribute	1 St 1	->	
Attribute			
Attribute		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

#### MOBOTIX HUB - Certificates Guide - Install certificates in a Workgroup environment

0	Micr	osoft A	Active !	Directory Certif	×	+	0		+		×
4	>	C	A	Not secure	10.0	0.4.103/certsrv/certfnsh.asp		¢	4	Update	: :)
Mica	rosof	t Activ	e Dire	ctory Certificat	e Ser	rvices - IP-0A000467-CA				Į	lome

#### Certificate Pending

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

Your Request Id is 6.

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

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

#### 16.1.2 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.
- 4. In the **Pending Requests** folder, right-click on the matching Request ID, and from the **All Tasks** list, select **Issue**.
- 5. Open a browser and go to the Internal CA IIS site located at [ ip.ad.dr.ess/certsrv ].

Console1 - [Console Root\Certification Authority (Local)\IP-0A000467-CA\Pending Requests]



6. Click the View the status of a pending certificate request link.
# MOBOTIX HUB - Certificates Guide - Install certificates in a Workgroup environment

0	Micr	osoft A	ctive l	Directory Certif	×	+	0	-		×
4	÷	C		Not secure	10.0	0.4.103/certsrv/	4	8	Updat	te :)
Micr	rosof	t Active	e Dire	ctory Certificat	e Se	rvices - IP-0A000467-CA			1	Home

#### Welcome

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

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

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

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

0	Micro	osoft A	ctive [	Directory Certit	×	+		•	-		×
÷	7	C	A	Not secure	10.0	0.4.103/certsrv/ce	ertckpn.asp	☆	4	Update	• •)
Micr	osofi	Active	e Dire	ctory Certifica	te Ser	rvices - IP-0A000	0467-CA			ł	<u>lome</u>
Viev	v the	e Stat	tus c	of a Pendin	g Ce	ertificate Requ	est				_
Sele S	ect th avec	le cer d-Rec	tifica uest	te request	you v (6/1/	want to view: /2021 1:36:18	<u>PM</u> )				

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

- Ouiskasser		Name	~	Date modified	Туре
Desktop Downloads	* * * *	л	Open Install Certificate Scan with Windows Defender Open with		

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

- 9. Accept the security warning if it appears.
- 10. Select to install the certificate for the current user and click Next.

		×
4	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 Cance	1

- 11. Choose a store location. Select **Place all certificates in the following store**, and click the **Browse** button to open the **Select Certificate Store** window. Navigate to the **Personal** certificate store and click **OK**.
- 12. Click Next.

# MOBOTIX HUB – Certificates Guide - Install certificates in a Workgroup environment

🗧 🌛 Certificate Import Wizard	
Certificate Store Certificate stores are system areas where certificates are kept.	
Windows can automatcally select a certificate store, or you can specify a location for the certificate. <ul> <li>Automatically select the certificate store based on the type of certificate</li> <li>Place all certificates in the following store</li> <li>Certificate store:</li> <li>Browse</li> </ul>	Select Certificate Store × Select the certificate store you want to use.

- 13. Finish the Certificate Import Wizard.
- 14. Go to the Microsoft Management Console (MMC) certificates snap-in.

15. 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.



- 16. 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.
- 17. Make sure that the user has both Full Control and Read permissions enabled.
- By default, MOBOTIX HUB software uses the NETWORK SERVICE account.

up of user names.		
CREATOR OWNER		
NETWORK SERVICE		
SYSTEM		1
Preminadatora (GEGG) ENTI		01
	Add	Remove
missions for NETWORK RVICE	Allow	Deny
full control		
Read		
Special permissions		
special permissions or advance	ced settings,	Advanced

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 113/ 126Certificates guide - Milestone XProtect® VMSCertificates XProtect<sup>®</sup> VMS

# 16.1.3 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.
- 5. 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.

	-		×
Encryption			
It is recommended to secure communication with end	cryption. Learn I	more	
Server certificate Applies to: management server, recording server, failover server collector	er, data		
Encryption: On	0		
Concession in the local division of the loca	9	Detail	s
Camplicate issued by MS-Organization-P28-Actesh (2021), Expires 5/8/20	23 -		
Streaming media certificate Applies to clients and servers that retrieve data streams from t server	he recording		
Encryption: On	0		
Tearran .	Ŷ	Detail	s
Certificate instead by MS-Deganization 9/9-Access (2021), Explore 5/0/20	23		
	1.00		
		Apply	
	Encryption: On Control on Server certificate Applies to: management server, recording server, failover server, Particular in an agement server, recording server, failover server, Encryption: On Control on Server of MS-Organization PDS-Access (2021), Spriver SM200 Streaming media certificate Applies to clients and servers that retrieve data streams from the Streaming media certificate Applies to clients and servers that retrieve data streams from the Streaming media certificate Applies to clients and servers that retrieve data streams from the Encryption: On Encryption: On	Force point of the secure communication with encryption. Learn of the secure communication with encryption of the secure communication with encryption. Learn of the secure communication with encryption of the secure communication with encryption. Learn of the secure communication with encryption of the secure communication with encryption of the secure communication with encryption of the secure communication of the secure communicat	Control of the second second communication with encryption. Learn more     Server certificate     Applies to: management server, recording server, failover server, data     Control of the second server recording server, failover server, data     Control of the second server second server server data     Control of the second server server, data streams from the recording     Encryption: On     Control of the server set server set set retrieve data streams from the recording     Encryption: On     Control of the server set set retrieve data streams from the recording     Control of the server set set retrieve data streams from the recording     Control of the server set set retrieve data streams from the recording     Control of the server set set retrieve data streams from the recording     Control of the server set set retrieve data streams from the recording     Control of the server set set retrieve data streams from the recording     Control of the server set set retrieve data streams from the recording     Control of the server set set retrieve data streams from the recording     Control of the server set set retrieve data streams from the recording     Control of the server set set retrieve data streams from the recording     Control of the server set set retrieve data streams from the recording     Control of the server set

#### 6. 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.

# 16.2 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



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.

#### components.

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

# 16.3 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.

#### 16.3.1 Prerequisites:

A server authentication certificate is trusted on the computer that hosts the event server First, enable encryption on the event server.

Steps:

7. On a computer with an event server installed, open the **Server Configurator** from:

© MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 115/ 126Certificates guide - Milestone XProtect® VMSCertificates XProtect<sup>®</sup> VMS

- The Windows Start menu • or
- The Event Server by right-clicking the Event Server icon on the computer task bar
- 8. In the Server Configurator, under Event server and add-ons, turn on Encryption.
- 9. 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.
- 10. Select a certificate to encrypt communication between the event server and related add-ons.
- 11. Select **Details** to view Windows Certificate Store information about the selected certificate.

Server Configurator	100	( <del>) (</del> )		×
Encryption	S Encryption configuration successful			×
Registering servers Language selection	Encryption It is recommended to secure communicat Streaming media certificate Applies to clients and servers that retrieve data st	ion with encryption. <u>Learn r</u> treams from the recording	nore	
	server Encryption: Off Select-certificate No certificate selected	•		Ì
	Event server and add-ons Applies to: event server, LPR server Encryption: On	0		
	Certificate issued by I	Expires 1/8/2022	Details	
			Apply	

#### 12. Click Apply.

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

# 16.3.2 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:

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 116/ 126Certificates guide - Milestone XProtect® VMSCertificates XProtect<sup>®</sup> VMS

S Microsoft Active Directory Certif × +			-		×
← → C ▲ Not secure   10.0.4.103/certsrv/			4	-	ŧ
Microsoft Active Directory Certificate Services - IP-0A000467-CA					lome
Welcome					
Use this Web site to request a certificate for your Web browser, certificate, you can verify your identity to people you communica messages, and, depending upon the type of certificate you requ You can also use this Web site to download a certificate authori certificate revocation list (CRL), or to view the status of a pendir	e-mail client, or other pro ate with over the Web, sig uest, perform other securi ity (CA) certificate, certific ng request.	gra in a ty ta ate	m. By nd end isks. chain,	using crypt , or	a
For more information about Active Directory Certificate Services Documentation	s, see <u>Active Directory Ce</u>	rtific	cate S	ervices	5
Select a task: <u>Request a certificate</u> View the status of a pending certificate request					
Download a CA certificate, certificate chain, or CRL					

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

- 2. Click Download a CA certificate, certificate chain, or CRL.
- 3. In the CA certificate field, select the CA certificate to be used with the MOBOTIX HUB system, and click

<b>1.</b> Download CA certificate chain.	
--	--



To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [IP-0A000467-CA]

Encoding method:

**DER** OBase 64

Install CA certificate Download CA certificate Download CA certificate chain Download latest base CRL

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_EN.docx • 04.03.2025 • Page 117/ 126Certificates guide - Milestone XProtect® VMSCertificates XProtect<sup>®</sup> VMS

- 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.
- 7. Click Next.

÷

- 11	Certificate	Import	Wizard	
------	-------------	--------	--------	--

Inis wizard helps you copy certificates, certificate trust lists, and certificate lists from your disk to a certificate store.	revocation
A certificate, which is issued by a certification authority, is a confirmation o and contains information used to protect data or to establish secure netwo connections. A certificate store is the system area where certificates are ke	f your iden rk ept,
To continue, dick Next.	

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

9. Navigate to the Third-Party Root Certification Authorities certificate store and click OK. Click Next.



10. 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.

# 16.4 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	15
	146
Host name:	
North Toronto and Annual State	
Local web server address:	
https://ik:7563/	
Web server address:	
https://www.recordingserver1.dk:89/	
Time zone:	
(UTC+01:00) Brussels, Copenhagen, Madrid, Paris	

# 16.4.1 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.

# Certificates guide | MOBOTIX HUB®

allover server information	
Name:	
Failover recording server 1	
Description:	
Failover for Recording server 1	
	1
Host name:	
local	
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	

Appendix A | Create CA Certificate script

# 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) #Promptuser 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")

# 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'

#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 Heat, ForegroundColor Red 'At least one day name should be specified' evit

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"
}
for while the provided the second terms of terms of
```

\$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"

 ${\tt \# The only required purpose of the sertificate is "Server Authentication"}$ 

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

#### #Now-create the management server certificate

# $\# {\sf Export\, certificate\, to\, disk-protect\, with\, a \, password}$

\$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\_03/25

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 2025