

MOBOTIX HUB – Leitfaden für Zertifikate

V2.04

Inhaltsverzeichnis

	1	URHEBERRECHT, MARKEN UND HAFTUNGSAUSSCHLUSS4
	2	ÜBER DIESEN LEITFADEN
	3	WANN MÜSSEN SIE ZERTIFIKATE INSTALLIEREN?
	4	EINFÜHRUNG IN ZERTIFIKATE
	4.1	Zertifikat Verteilung
	5	ÜBERBLICK ÜBER DIE SZENARIEN UND VORGEHENSWEISEN, DIE MIT ATTESTE
	5.1 5.2 5.3 5.4 5.5 5.6 5.7	MOBOTIX HUB Mobiler Server10MOBOTIX HUB MANAGEMENT SERVER UND RECORDING SERVER10Zertifikat einer Drittanbieter- oder kommerziellen Zertifizierungsstelle11Domäne11Arbeitsgruppe11MOBOTIX HUB Ereignisserver11Kunde11
	6	WELCHE CLIENTS BENÖTIGEN ZERTIFIKATE? 13
	7	SERVER-KONFIGURATOR (ERKLÄRT) 15
	7.1 7.2 7.3 7.4	Server-Zertifikat
	8	POWERSHELL-SKRIPTS 18
	9	MANUELLES ERSTELLEN UND VERTEILEN VON ZERTIFIKATEN
	9.1 9.2	WICHTIG ZU WISSEN:
	10	INSTALLIEREN VON ZERTIFIKATEN AUF DEN CLIENTS 22
© MOBO Mx GI	11 DTIX A MX H	SSL-ZERTIFIKAT ERSTELLEN
	Miles	stone XProtect® VMS

MOBOTIX HUB – Leitfaden für Zertifikate - Error! Use the Home tab to apply

12 SSL-ZERTIFIKAT IMPORTIEREN
12.1 VERWALTEN SIE PRIVATE SCHLÜSSEL
13 ERSTELLEN EINES SSL-ZERTIFIKATS FÜR DEN FAILOVER-MANAGEMENT-SERVER
14 INSTALLIEREN ATTESTE FÜR DIE KOMMUNIKATION MIT DEM MOBILE SERVER
14.1 HINZUFÜGEN EINER ZERTIFIZIERUNGSSTELLE ZERTIFIKAT ZUM SERVER 42 14.2 LADEN SIZ DIE DED DATELLOGU UND GEGENZUG EIN GIGUERDEG ZERTIFIKAT ZU ERUNATERU 51
14.2 Laden Sie Die .Reg-Datei Hoch, om im Gegenzög ein Signiertes Zertifikat zu erhalten
15 INSTALLIEREN VON ZERTIFIKATEN VON DRITTANBIETERN ODER KOMMERZIELLEN ZERTIFIZIERUNGSSTELLEN FÜR DIE KOMMUNIKATION MIT DEM MANAGEMENT SERVER ODER RECORDING SERVER
15.1 HINZUFÜGEN EINES ZERTIFIZIERUNGSSTELLENZERTIFIKATS ZUM SERVER
15.2 LADEN SIE DIE .REQ-DATEI HOCH, UM IM GEGENZUG EIN SIGNIERTES ZERTIFIKAT ZU ERHALTEN
15.3 AKTIVIEREN DER VERSCHLÜSSELUNG ZUM UND VOM MANAGEMENT-SERVER
15.3.1 VORAUSSETZUNGEN:
15.3.2 SO INSTALLIEREN SIE AD CS:
15.4 INSTALLIEREN VON ZERTIFIKATEN IN EINER DOMÄNE FÜR DIE KOMMUNIKATION MIT DER MANAGEMENT-SERVER
ODER DER AUFZEICHNUNGSSERVER
15.4.1 HINZUFÜGEN EINES ZERTIFIZIERUNGSSTELLENZERTIFIKATS ZUM SERVER
15.4.2 LADEN SIE DIE .REQ-DATEI HOCH, UM IM GEGENZUG EIN SIGNIERTES ZERTIFIKAT ZU ERHALTEN
15.5 MANUELLES INSTALLIEREN DES ZERTIFIKATS
15.5.1 AKTIVIEREN DER SERVERVERSCHLÜSSELUNG FÜR MANAGEMENT-SERVER UND AUFZEICHNUNGSSERVER100
16 INSTALLIEREN ZERTIFIKATE IN EINER WORKGROUP-UMGEBUNG FÜR DIE KOMMUNIKATION MIT DEM MANAGEMENT SERVER ODER RECORDING SERVER
16.1 HINZUFÜGEN EINES ZERTIFIZIERUNGSSTELLENZERTIFIKATS ZUM SERVER
16.1HINZUFÜGEN EINES ZERTIFIZIERUNGSSTELLENZERTIFIKATS ZUM SERVER10216.1.1LADEN SIE DIE .REQ-DATEI HOCH, UM IM GEGENZUG EIN SIGNIERTES ZERTIFIKAT ZU ERHALTEN.111
16.1HINZUFÜGEN EINES ZERTIFIZIERUNGSSTELLENZERTIFIKATS ZUM SERVER10216.1.1LADEN SIE DIE .REQ-DATEI HOCH, UM IM GEGENZUG EIN SIGNIERTES ZERTIFIKAT ZU ERHALTEN11116.1.2MANUELLES AUSSTELLEN VON ZERTIFIKATEN115
16.1HINZUFÜGEN EINES ZERTIFIZIERUNGSSTELLENZERTIFIKATS ZUM SERVER10216.1.1LADEN SIE DIE .REQ-DATEI HOCH, UM IM GEGENZUG EIN SIGNIERTES ZERTIFIKAT ZU ERHALTEN.11116.1.2MANUELLES AUSSTELLEN VON ZERTIFIKATEN11516.1.3AKTIVIEREN DER SERVERVERSCHLÜSSELUNG FÜR MANAGEMENT-SERVER UND AUFZEICHNUNGSSERVER121
16.1HINZUFÜGEN EINES ZERTIFIZIERUNGSSTELLENZERTIFIKATS ZUM SERVER10216.1.1LADEN SIE DIE .REQ-DATEI HOCH, UM IM GEGENZUG EIN SIGNIERTES ZERTIFIKAT ZU ERHALTEN11116.1.2MANUELLES AUSSTELLEN VON ZERTIFIKATEN11516.1.3AKTIVIEREN DER SERVERVERSCHLÜSSELUNG FÜR MANAGEMENT-SERVER UND AUFZEICHNUNGSSERVER12116.2INSTALLIEREN VON ZERTIFIKATEN FÜR DIE KOMMUNIKATION MIT DEM EREIGNIS SERVER122
16.1HINZUFÜGEN EINES ZERTIFIZIERUNGSSTELLENZERTIFIKATS ZUM SERVER.10216.1.1LADEN SIE DIE .REQ-DATEI HOCH, UM IM GEGENZUG EIN SIGNIERTES ZERTIFIKAT ZU ERHALTEN.11116.1.2MANUELLES AUSSTELLEN VON ZERTIFIKATEN.11516.1.3AKTIVIEREN DER SERVERVERSCHLÜSSELUNG FÜR MANAGEMENT-SERVER UND AUFZEICHNUNGSSERVER.12116.2INSTALLIEREN VON ZERTIFIKATEN FÜR DIE KOMMUNIKATION MIT DEM EREIGNIS SERVER12216.3ERMÖGLICHEN MOBOTIX HUB EVENT SERVER-VERSCHLÜSSELUNG.122
16.1HINZUFÜGEN EINES ZERTIFIZIERUNGSSTELLENZERTIFIKATS ZUM SERVER.10216.1.1LADEN SIE DIE .REQ-DATEI HOCH, UM IM GEGENZUG EIN SIGNIERTES ZERTIFIKAT ZU ERHALTEN.11116.1.2MANUELLES AUSSTELLEN VON ZERTIFIKATEN.11516.1.3AKTIVIEREN DER SERVERVERSCHLÜSSELUNG FÜR MANAGEMENT-SERVER UND AUFZEICHNUNGSSERVER12116.2INSTALLIEREN VON ZERTIFIKATEN FÜR DIE KOMMUNIKATION MIT DEM EREIGNIS SERVER12216.3ERMÖGLICHEN MOBOTIX HUB EVENT SERVER-VERSCHLÜSSELUNG12216.3.1VORAUSSETZUNGEN:122
16.1HINZUFÜGEN EINES ZERTIFIZIERUNGSSTELLENZERTIFIKATS ZUM SERVER.10216.1.1LADEN SIE DIE .REQ-DATEI HOCH, UM IM GEGENZUG EIN SIGNIERTES ZERTIFIKAT ZU ERHALTEN.11116.1.2MANUELLES AUSSTELLEN VON ZERTIFIKATEN.11516.1.3AKTIVIEREN DER SERVERVERSCHLÜSSELUNG FÜR MANAGEMENT-SERVER UND AUFZEICHNUNGSSERVER.12116.2INSTALLIEREN VON ZERTIFIKATEN FÜR DIE KOMMUNIKATION MIT DEM EREIGNIS SERVER12216.3ERMÖGLICHEN MOBOTIX HUB EVENT SERVER-VERSCHLÜSSELUNG12216.3.1VORAUSSETZUNGEN:12216.3.2IMPORTIEREN VON CLIENTZERTIFIKATEN124
16.1HINZUFÜGEN EINES ZERTIFIZIERUNGSSTELLENZERTIFIKATS ZUM SERVER.10216.1.1LADEN SIE DIE .REQ-DATEI HOCH, UM IM GEGENZUG EIN SIGNIERTES ZERTIFIKAT ZU ERHALTEN.11116.1.2MANUELLES AUSSTELLEN VON ZERTIFIKATEN.11516.1.3AKTIVIEREN DER SERVERVERSCHLÜSSELUNG FÜR MANAGEMENT-SERVER UND AUFZEICHNUNGSSERVER.12116.2INSTALLIEREN VON ZERTIFIKATEN FÜR DIE KOMMUNIKATION MIT DEM EREIGNIS SERVER12216.3ERMÖGLICHEN MOBOTIX HUB EVENT SERVER-VERSCHLÜSSELUNG12216.3.1VORAUSSETZUNGEN:12216.3.2IMPORTIEREN VON CLIENTZERTIFIKATEN1241.LADEN SIE DIE CA-ZERTIFIKATSKETTE HERUNTER.125
16.1HINZUFÜGEN EINES ZERTIFIZIERUNGSSTELLENZERTIFIKATS ZUM SERVER10216.1.1LADEN SIE DIE .REQ-DATEI HOCH, UM IM GEGENZUG EIN SIGNIERTES ZERTIFIKAT ZU ERHALTEN.11116.1.2MANUELLES AUSSTELLEN VON ZERTIFIKATEN.11516.1.3AKTIVIEREN DER SERVERVERSCHLÜSSELUNG FÜR MANAGEMENT-SERVER UND AUFZEICHNUNGSSERVER.12116.2INSTALLIEREN VON ZERTIFIKATEN FÜR DIE KOMMUNIKATION MIT DEM EREIGNIS SERVER12216.3ERMÖGLICHEN MOBOTIX HUB EVENT SERVER-VERSCHLÜSSELUNG.12216.3.1VORAUSSETZUNGEN:12216.3.2IMPORTIEREN VON CLIENTZERTIFIKATEN1241.LADEN SIE DIE CA-ZERTIFIKATSKETTE HERUNTER.12516.4ANZEIGEN DES VERSCHLÜSSELUNGSSTATUS FÜR CLIENTS129

1 Urheberrecht, Marken und Haftungsausschluss

Copyright © 2025 MOBOTIX AG

Handelsmarken

MOBOTIX HUB ist eine eingetragene Marke der MOBOTIX AG. Microsoft und Windows sind eingetragene Marken der Microsoft Corporation. App Store ist eine Dienstleistungsmarke von Apple Inc. Android ist eine Marke von Google Inc. Alle anderen Marken, die in diesem Dokument erwähnt werden, sind Marken ihrer jeweiligen Eigentümer.

Verzichtserklärung

Dieser Text dient nur zu allgemeinen Informationszwecken und wurde mit der gebotenen Sorgfalt erstellt. Jedes Risiko, das sich aus der Verwendung dieser Informationen ergibt, liegt beim Empfänger, und nichts in diesem Dokument sollte so ausgelegt werden, dass es irgendeine Art von Garantie darstellt.

Die MOBOTIX AG behält sich das Recht vor, ohne vorherige Ankündigung Anpassungen vorzunehmen.

Alle Namen von Personen und Organisationen, die in den Beispielen in diesem Text verwendet werden, sind fiktiv. Jede Ähnlichkeit mit einer tatsächlichen Organisation oder Person, ob lebendig oder tot, ist rein zufällig und unbeabsichtigt.

Dieses Produkt kann Software von Drittanbietern verwenden, für die möglicherweise besondere Bedingungen gelten. Wenn dies der Fall ist, finden Sie weitere Informationen in der Datei

3rd_party_software_terms_and_conditions.txt, die sich in Ihrem Installationsordner für das MOBOTIX HUB-System befindet.

2 Über diesen Leitfaden

In diesem Leitfaden erhalten Sie eine Einführung in Verschlüsselung und Zertifikate sowie Schritt-für-Schritt-Verfahren zum Installieren von Zertifikaten in einer Windows Workgroup-Umgebung.

MOBOTIX empfiehlt, eine Public Key Infrastructure (PKI) für die Erstellung und Verteilung von Zertifikaten einzurichten. Eine PKI ist eine Reihe von Rollen, Richtlinien, Hardware, Software und Verfahren, die zum Erstellen, Verwalten, Verteilen, Verwenden, Speichern und Widerrufen digitaler Zertifikate sowie zum Verwalten der Public-Key-Verschlüsselung erforderlich sind. In einer Windows-Domäne wird empfohlen, eine PKI mithilfe der Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS) einzurichten.

Wenn Sie keine PKI erstellen können, entweder weil verschiedene Domänen nicht vertrauenswürdig sind oder weil Domänen überhaupt nicht verwendet werden, ist es möglich, Zertifikate manuell zu erstellen und zu verteilen.

WARNUNG: Das manuelle Erstellen und Verteilen von Zertifikaten wird als sichere Methode zum Verteilen von Zertifikaten nicht empfohlen. Wenn Sie sich für die manuelle Verteilung entscheiden, sind Sie dafür verantwortlich, die privaten Zertifikate immer sicher aufzubewahren. Wenn Sie die privaten Zertifikate sicher aufbewahren, sind die Clientcomputer, die den Zertifikaten vertrauen, weniger anfällig für Angriffe.

3 Wann müssen Sie Zertifikate installieren?

Entscheiden Sie zunächst, ob Ihr System eine verschlüsselte Kommunikation benötigt.

Verwenden Sie keine Zertifikate mit Aufzeichnungsserververschlüsselung, wenn Sie eine oder mehrere Integrationen verwenden, die die HTTPS-Kommunikation nicht unterstützen. Dies sind z. B. MIP SDK-Integrationen von Drittanbietern, die HTTPS nicht unterstützen.

Sofern die Installation nicht in einem physisch isolierten Netzwerk erfolgt, wird empfohlen, die Kommunikation mithilfe von Zertifikaten zu sichern.

In diesem Dokument wird beschrieben, wann Zertifikate verwendet werden sollten:

- Wenn Ihr MOBOTIX HUB VMS-System in einer Windows Workgroup-Umgebung eingerichtet ist
- Bevor Sie MOBOTIX HUB VMS 2019 R1 oder höher installieren oder aktualisieren, wenn Sie die Verschlüsselung während der Installation aktivieren möchten.
- Bevor Sie die Verschlüsselung aktivieren, wenn Sie MOBOTIX HUB VMS 2019 R1 oder höher ohne Verschlüsselung installiert haben
- Wenn Sie Zertifikate aufgrund von Ablauf erneuern oder ersetzen

4 Einführung in Zertifikate

Hypertext Transfer Protocol Secure (HTTPS) ist eine Erweiterung des Hypertext Transfer Protocol (HTTP) für die sichere Kommunikation über ein Computernetzwerk. Bei HTTPS wird das Kommunikationsprotokoll mit Transport Layer Security (TLS) oder seinem Vorgänger Secure Sockets Layer (SSL) verschlüsselt.

In MOBOTIX HUB VMS wird eine sichere Kommunikation durch die Verwendung von TLS/SSL mit asymmetrischer Verschlüsselung (RSA) erreicht. TLS/SSL verwendet ein Schlüsselpaar – einen privaten, einen öffentlichen – um sichere Verbindungen zu authentifizieren, zu sichern und zu verwalten.

Eine Zertifizierungsstelle (Certificate Authority, CA) ist jeder, der Stammzertifikate ausstellen kann. Dabei kann es sich um einen Internetdienst handeln, der Stammzertifikate ausstellt, oder um eine Person, die ein Zertifikat manuell generiert und verteilt. Eine Zertifizierungsstelle kann Zertifikate für Webdienste ausstellen, d. h. für jede Software, die HTTPS-Kommunikation verwendet. Dieses Zertifikat enthält zwei Schlüssel, einen privaten Schlüssel und einen öffentlichen Schlüssel. Der öffentliche Schlüssel wird auf den Clients eines Web-Service (Service-Clients) installiert, indem ein öffentliches Zertifikat installiert wird. Der private Schlüssel wird zum Signieren von Serverzertifikaten verwendet, die auf dem Server installiert werden müssen.

Jedes Mal, wenn ein Dienstclient den Webdienst aufruft, sendet der Webdienst das Serverzertifikat einschließlich des öffentlichen Schlüssels an den Client. Der Dienstclient kann das Serverzertifikat mithilfe des bereits installierten Zertifikats der öffentlichen Zertifizierungsstelle validieren. Der Client und der Server können nun über die öffentlichen und privaten Serverzertifikate einen geheimen Schlüssel austauschen und so eine sichere TLS/SSL-Verbindung aufbauen.

Bei manuell verteilten Zertifikaten müssen Zertifikate installiert werden, bevor der Client eine solche Überprüfung durchführen kann .

Weitere Informationen zu TLS finden Sie unter Transport Layer Security.

In MOBOTIX HUB-VMS können Sie die TLS/SSL-Verschlüsselung an den folgenden Speicherorten aktivieren:

- Bei der Kommunikation zwischen dem Management-Server und den Aufzeichnungsservern, Ereignisservern und mobilen Servern
- Auf dem Aufzeichnungsserver in der Kommunikation mit Clients, Servern und Integrationen, die Datenströme vom Aufzeichnungsserver abrufen.

In der Kommunikation zwischen Clients und dem mobilen Server In diesem Handbuch werden die folgenden Personen als Clients bezeichnet:

- MOBOTIX HUB Desk Client
- Management-Client
- Management Server (für System Monitor und für Bilder und AVI-Videoclips in E-Mail-Benachrichtigungen)
- MOBOTIX HUB Mobiler Server
- MOBOTIX HUB Ereignisserver
- MOBOTIX HUB LPR
- MOBOTIX Open Network Bridge
- MOBOTIX HUB DLNA Server
- Sites, die Datenströme vom Aufzeichnungsserver über Milestone Interconnect abrufen
- MIP SDK-Integrationen von Drittanbietern, die HTTPS unterstützen

Für Lösungen, die mit MIP SDK 2018 R3 oder früher erstellt wurden und auf Aufzeichnungsserver zugreifen:-Wenn die Integrationen mithilfe von MIP SDK-Bibliotheken erstellt werden, müssen sie mit MIP SDK 2019 R1 neu erstellt werden- Wenn die Integrationen direkt mit den Aufzeichnungsserver-APIs kommunizieren, ohne MIP SDK-Bibliotheken zu verwenden, müssen die Integratoren selbst HTTPS-Unterstützung hinzufügen- Im Zweifelsfall Fragen Sie Ihren Anbieter, der die Integration bereitgestellt hat.

4.1 Verteilung von Zertifikaten

Die Grafik veranschaulicht das grundlegende Konzept, wie Zertifikate in MOBOTIX HUB VMS signiert, vertrauenswürdig und verteilt werden, um die Kommunikation mit dem Management-Server zu sichern.



❶ Ein CA-Zertifikat fungiert als vertrauenswürdiger Dritter, dem sowohl der Betreff/Eigentümer (Management-Server) als auch die Partei, die das Zertifikat überprüft (Aufzeichnungsserver), vertrauen

🕑 Das CA-Zertifikat muss auf allen Aufzeichnungsservern als vertrauenswürdig eingestuft werden. Auf diese Weise können die Aufzeichnungsserver die Gültigkeit der von der Zertifizierungsstelle ausgestellten Zertifikate überprüfen

³ Das CA-Zertifikat wird verwendet, um eine sichere Verbindung zwischen dem Management-Server und den Aufzeichnungsservern herzustellen

🔮 Das Zertifikat der Zertifizierungsstelle muss auf dem Computer installiert sein, auf dem der Verwaltungsserver ausgeführt wird

Anforderungen an das Zertifikat des privaten Verwaltungsservers:

- Wird für den Management-Server ausgestellt, sodass der Hostname des Management-Servers im Zertifikat enthalten ist, entweder als Antragsteller (Besitzer) oder in der Liste der DNS-Namen, für die das Zertifikat ausgestellt wird
- Vertrauenswürdig auf dem Management-Server selbst, indem das CA-Zertifikat als vertrauenswürdig eingestuft wird, das zum Ausstellen des Management-Server-Zertifikats verwendet wurde

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 8/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfader für Zertifikate - Milestone XProtect® VMSLeitfader Milestone XProtect® VMS

MOBOTIX HUB – Leitfaden für Zertifikate - Einführung in Zertifikate

• Vertrauenswürdig auf allen Aufzeichnungsservern, die mit dem Management-Server verbunden sind, indem das Zertifikat der Zertifizierungsstelle als vertrauenswürdig eingestuft wird, das zum Ausstellen des Management-Server-Zertifikats verwendet wurde



Zertifikate haben ein Ablaufdatum. Sie erhalten keine Warnung, wenn ein Zertifikat kurz vor dem Ablauf steht. Wenn ein Zertifikat abläuft, vertrauen die Clients dem Server nicht mehr mit dem abgelaufenen Zertifikat und können daher nicht mehr mit ihm kommunizieren.

Um die Zertifikate zu erneuern, führen Sie die Schritte in diesem Leitfaden wie beim Erstellen von

5 Übersicht über die Szenarien und Verfahren, die mit Zertifikaten verwendet werden

Die Verfahren für die Konfiguration der sicheren Kommunikation in einer MOBOTIX HUB VMS-Umgebung sind unterschiedlich, je nachdem, welche Art von Servern eine sichere Kommunikation erfordert. Die Vorgehensweisen unterscheiden sich auch in einem WORKGROUP-Netzwerk von einem DOMAIN-Netzwerk. Die Typen der MOBOTIX HUB VMS-Client-Anwendungen, die im System verwendet werden, bestimmen auch einige der erforderlichen Verfahren für eine sichere Kommunikation.



Die Verwendung von Zertifikaten für die Serverkommunikation kann in der Regel bei einer einzelnen Serverinstallation ignoriert werden , es sei denn, sie dienen als zusätzliche Sicherheit bei der Kommunikation mit dem Management-Server.

Diese Liste zeigt die verschiedenen Szenarien:

5.1 MOBOTIX HUB Mobiler Server

In MOBOTIX HUB-VMS wird die Verschlüsselung pro Mobile Server aktiviert oder deaktiviert. Sie aktivieren oder deaktivieren die Verschlüsselung entweder während der Installation des Produkts MOBOTIX HUB VMS oder mithilfe des Server-Konfigurators. Wenn Sie die Verschlüsselung auf einem Mobile Server aktivieren, verwenden Sie eine verschlüsselte Kommunikation mit allen Clients, Diensten und Integrationen, die Datenströme abrufen.

Der Mobile Server verbindet sich mit dem MOBOTIX HUB Mobile Client und dem MOBOTIX HUB Web Client. Browser, Betriebssysteme und mobile Geräte, die diese Clients hosten, verwalten eine Liste vertrauenswürdiger CA-Stammzertifikate. Nur die Autorität kennt ihren privaten Schlüssel, aber jeder kennt ihren öffentlichen Schlüssel, der einem bestimmten Zertifikat ähnelt.

Auf diesen Clients sind dann bereits Zertifikatschlüssel installiert, und sie funktionieren mit den meisten Zertifikaten von Drittanbietern, die für die Installation auf dem Mobile Server selbst verfügbar sind. Da jede Drittanbieter-CA ihre eigenen Anforderungen für die Beantragung eines Zertifikats hat, ist es am besten, die einzelnen Anforderungen direkt mit der CA zu erörtern.

In diesem Dokument wird beschrieben, wie Sie eine Zertifikatsanforderung auf dem Mobile Server erstellen und das Zertifikat installieren, sobald es von der Zertifizierungsstelle ausgestellt wurde. Siehe:

Installieren von Zertifikaten für die Kommunikation mit dem Mobile Server auf Seite 40

⁵² MOBOTIX HUB Management Server und Recording Server

Sie können die bidirektionale Verbindung zwischen dem Management-Server und dem Aufzeichnungsserver verschlüsseln. Wenn Sie die Verschlüsselung auf dem Management-Server aktivieren, gilt sie für Verbindungen von allen Aufzeichnungsservern, die eine Verbindung zum Management-Server herstellen. Wenn Sie die Verschlüsselung auf dem Management-Server aktivieren, müssen Sie auch die Verschlüsselung auf allen Aufzeichnungsservern aktivieren. Bevor Sie die Verschlüsselung aktivieren, müssen Sie Sicherheitszertifikate auf dem Management-Server und allen Aufzeichnungsservern, einschließlich Failover-Aufzeichnungsservern, installieren.

Zertifikat einer Drittanbieter- oder kommerziellen Zertifizierungsstelle 5.3

Das Verfahren zum Anfordern von Zertifikaten von Zertifizierungsstellen von Drittanbietern für die Verwendung mit Management-Servern und Aufzeichnungsservern ist identisch mit dem für den Mobile Server. Der einzige Unterschied ist die Konfiguration mit dem Server Konfigurator. Siehe:

Installieren von Zertifikaten von Drittanbietern oder kommerziellen Zertifizierungsstellen für die Kommunikation mit dem Management Server oder Recording Server auf Seite 57

5.4 Domäne

Wenn Client- und Serverendpunkte alle in einer Domänenumgebung mit einer eigenen Zertifizierungsstelleninfrastruktur betrieben werden, ist es nicht erforderlich, CA-Zertifikate an Client-Workstations zu verteilen. Solange Sie über eine Gruppenrichtlinie innerhalb der Domäne verfügen, die die automatische Verteilung aller Zertifikate der vertrauenswürdigen Zertifizierungsstelle an alle Benutzer und Computer in der Domäne verarbeitet.

Das Anfordern eines Zertifikats und das Installieren eines Serverzertifikats ist identisch mit dem in einer Arbeitsgruppe.

Siehe:

Installieren von Zertifikaten in einer Domäne für die Kommunikation mit dem Management Server oder Recording Server auf Seite 86

5.5 Arbeitsgruppe

Beim Betrieb in einer Workgroup-Umgebung wird davon ausgegangen, dass keine Infrastruktur für Zertifizierungsstellen vorhanden ist. Zum Verteilen von Zertifikaten ist es erforderlich, eine Zertifizierungsstelleninfrastruktur zu erstellen. Es ist auch erforderlich, die Zertifikatsschlüssel an Client-Workstations zu verteilen. Abgesehen von diesen Anforderungen ähnelt der Prozess zum Anfordern und Installieren eines Zertifikats auf einem Server sowohl dem Domänen- als auch dem Drittanbieterszenario.

Siehe:

Installieren von Zertifikaten in einer Arbeitsgruppenumgebung für die Kommunikation mit dem Management-Server oder dem Aufzeichnungsserver auf Seite 104

MOBOTIX HUB Ereignisserver 5.6

Sie können die bidirektionale Verbindung zwischen dem Ereignisserver und den Komponenten, die mit dem Ereignisserver kommunizieren, einschließlich des LPR-Servers, verschlüsseln. Wenn Sie die Verschlüsselung auf dem Ereignisserver aktivieren, gilt sie für Verbindungen von allen Komponenten, die eine Verbindung mit dem Ereignisserver herstellen. Bevor Sie die Verschlüsselung aktivieren, müssen Sie Sicherheitszertifikate auf dem Ereignisserver und allen Verbindungskomponenten installieren. Siehe:

Installieren von Zertifikaten für die Kommunikation mit dem Ereignisserver auf Seite 126

Kunde 5.7

In den Szenarien Drittanbieter/Kommerziell und Domäne müssen Clients keine Zertifikatschlüssel installieren. Sie müssen Clientzertifikatschlüssel nur in einer Arbeitsgruppenumgebung installieren.

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 11/136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Guerrante VMSLeitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden für Zert Milestone XProtect® VMS

Wenn Sie die Verschlüsselung auf einem Aufzeichnungsserver aktivieren, wird die Kommunikation mit allen Clients, Servern und Integrationen, die Datenströme vom Aufzeichnungsserver abrufen, verschlüsselt. In diesem Dokument werden diese als "Clients" für den Aufzeichnungsserver bezeichnet:

- MOBOTIX HUB Desk Client
- Management-Client
- Management Server (für System Monitor und für Bilder und AVI-Videoclips in E-Mail-Benachrichtigungen)
- MOBOTIX HUB Mobiler Server
- MOBOTIX HUB Ereignisserver
- MOBOTIX HUB LPR
- MOBOTIX Netzwerkbrücke
- MOBOTIX HUB DLNA Server
- Standorte, die Datenströme vom Aufzeichnungsserver über MOBOTIX Interconnect abrufen
- Einige MIP SDK-Integrationen von Drittanbietern

Für Lösungen, die mit MIP SDK 2018 R3 oder früher erstellt wurden und auf
Aufzeichnungsserver zugreifen: Wenn die Integrationen mithilfe von MIP SDKBibliotheken erstellt werden, müssen sie mit MIP SDK 2019 R1 neu erstellt werden.
Wenn die Integrationen direkt mit den Aufzeichnungsserver-APIs kommunizieren, ohne
MIP SDK-Bibliotheken zu verwenden, müssen die Integratoren selbst HTTPS-

Siehe:

Welche Clients benötigen Zertifikate? auf Seite 11 Importieren von Client-Zertifikaten auf Seite 129

Welche Clients benötigen Zertifikate? 6

Auf welchen Clients müssen Zertifikate installiert werden? Wie planen wir das? Was können wir tun, um uns vorzubereiten?

Für webbrowserbasierte Clients und Clients, die über einen öffentlichen Anwendungsverteilungsdienst oder -store eines Drittanbieters, z. B. Google Play oder Apple AppStore, vertrieben werden, sollten Sie kein Zertifikat installieren müssen. MOBOTIX HUB Mobile verwendet keine installierten Zertifikate. MOBOTIX HUB Mobile kann nur vertrauenswürdige Zertifikate von Drittanbietern verwenden.

Wenn die MOBOTIX HUB-Server (Management Server und Recording Server) auf Computern installiert sind , die der Domäne beigetreten sind, und die Benutzer, die sich beim Desk Client anmelden, alle

Domänenbenutzer sind, übernimmt die Domäne die Verteilung und Authentifizierung öffentlicher Schlüssel, die für die Einrichtung einer sicheren Kommunikation erforderlich sind.

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

No Public Key Distribution Needed

Public Key Distribution Needed

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 13/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Guerrante VMSLeitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden für Zer Milestone XProtect® VMS

MOBOTIX HUB – Leitfaden für Zertifikate - Welche Clients benötigen Zertifikate?

Nur in einem Szenario, in dem Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS) zum Erstellen selbstsignierter Zertifikate verwendet werden und die Ressourcen (Benutzer und Computer) in einer Nicht-Domänenumgebung ausgeführt werden, besteht die Notwendigkeit, öffentliche Schlüssel an Clientarbeitsstationen zu verteilen.

Siehe auch Installieren von Zertifikaten auf den Clients auf Seite 19 und Importieren von Client-Zertifikaten auf Seite 129.

7 Server-Konfigurator (erklärt)

Verwenden Sie den Server-Konfigurator, um Zertifikate auf lokalen Servern für die verschlüsselte Kommunikation auszuwählen und Serverdienste zu registrieren, um sie für die Kommunikation mit den Servern zu qualifizieren. Die folgenden Servertypen in MOBOTIX HUB VMS benötigen Zertifikate für eine sichere Kommunikation:

- Verwaltungsserver
- Aufzeichnen von Servern
- Ereignisserver
- Mobile Server

Diese Server arbeiten mit dem Server-Konfigurator zusammen, um die sichere Kommunikation zu verwalten. Verwenden Sie den Server-Konfigurator, um festzulegen, ob die MOBOTIX HUB-Server eine sichere verschlüsselte Kommunikation verwenden oder nicht, und um die Zertifikate zu verwalten, die von den MOBOTIX HUB-Servern verwendet werden.

Der Server Configurator wird standardmäßig auf jedem Computer installiert, auf dem ein MOBOTIX HUB-Server gehostet wird. Öffnen Sie den Server-Konfigurator über:

• Das Windows-Startmenü

oder

• Den MOBOTIX HUB-Server-Manager, indem Sie mit der rechten Maustaste auf das Server-Manager-Symbol in der Taskleiste des Computers klicken und Server-Konfigurator auswählen

MOBOTIX HUB - Leitfaden für Zertifikate - Server-Konfigurator (erklärt)

Milestone Server Configurator		7	
Encryption	Encryption		
Registering servers	It is recommended to secure communication with encryption	. Learn mo	ore
Language selection	Server certificate Applies to: management server, recording server, failover server, data collector		
	DocCert1	~	Details
	Mobile streaming media certificate Applies to mobile and web clients that retrieve data streams from the r server	nobile	
	Encryption: On	e	Details
	Certificate issued by mjt-MiT-DC-CA, DC=mjt, DC=local. Expires 4/27/2022		
			Apply
			Арріу

Verwenden Sie den Server-Konfigurator, um die Zertifikate auszuwählen, die die MOBOTIX HUB-Server verwenden, um die Kommunikation mit ihren Client-Anwendungen zu sichern, und um zu überprüfen, ob die Verschlüsselungseinstellungen ordnungsgemäß konfiguriert sind.

Server-Zertifikat 7.1

Wählen Sie das Zertifikat aus, das zum Verschlüsseln der bidirektionalen Verbindung zwischen dem Management-Server und den folgenden Servern verwendet werden soll:

- Aufzeichnungsserver •
- Ereignisserver •
- Protokollserver .
- LPR-Server •
- Mobiler Server .

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 16/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Garage Control Contro Milestone XProtect® VMS

^{7.2} Ereignisserver und Add-ons

Wählen Sie das Zertifikat aus, das zum Verschlüsseln der bidirektionalen Verbindung zwischen dem Ereignisserver und den Komponenten, die mit dem Ereignisserver kommunizieren, einschließlich des LPR-Servers, verwendet werden soll.

73 Zertifikat für Streaming-Medien

Wählen Sie das Zertifikat aus, das zum Verschlüsseln der Kommunikation zwischen den Aufzeichnungsservern und allen Clients, Servern und Integrationen verwendet werden soll, die Datenströme von den Aufzeichnungsservern abrufen.

74 Zertifikat für mobile Streaming-Medien

Wählen Sie das Zertifikat aus, das zum Verschlüsseln der Kommunikation zwischen dem mobilen Server und den mobilen und Web-Clients verwendet werden soll, die Datenströme vom mobilen Server abrufen. Registrieren Sie im Abschnitt **Server Registering servers (Server registrieren**) des Server Configurator die Server, die auf dem Computer ausgeführt werden, mit dem angegebenen Management-Server.

Um die Server zu registrieren, überprüfen Sie die Adresse des Management-Servers, und wählen Sie **Registrieren** aus.

8 PowerShell-Skripts

Sie können PowerShell und das Milestone PSTools-Modul verwenden, um die laufende Wartung und die erforderlichen Konfigurationsprozesse von großen, komplexen und technisch fortschrittlichen MOBOTIX HUB VMS-Systemen zu installieren, zu integrieren, zu vereinfachen, zu überwachen und zu automatisieren. Nichtsdestotrotz empfiehlt MOBOTIX, dass Administratoren, Installateure und Techniker wissen, wie sie die MOBOTIX HUB VMS-Umgebung ihres Kunden manuell konfigurieren können. Sie lernen mit Erfahrung, wann Sie PowerShell-Skripte anstelle von manuellen Konfigurationen verwenden sollten. PowerShell-Skripts finden Sie an den folgenden Speicherorten:

- PowerShell-Prozess/Video für mobile Server und Lets Encrypt
- Github-Repository für Milestone PSTools Informationen, Dokumentation und Skripte.

9 Manuelles Erstellen und Verteilen von Zertifikaten

9.1 Wichtig zu wissen:

Das manuelle Erstellen und Verteilen von Zertifikaten wird als sichere Methode zum Verteilen von Zertifikaten nicht empfohlen. Wenn Sie sich für die manuelle Verteilung entscheiden, sind Sie dafür verantwortlich, die privaten Zertifikate jederzeit sicher zu halten. Wenn Sie die privaten Zertifikate sicher aufbewahren, sind die Clientcomputer, die den Zertifikaten vertrauen, weniger anfällig für Angriffe.

In einigen Situationen kann Windows Update in regelmäßigen Abständen Zertifikate entfernen, die nicht von einer "vertrauenswürdigen Zertifizierungsstelle eines Drittanbieters" stammen.

Um sicherzustellen, dass Ihre Zertifikate nicht von Windows Update entfernt werden, müssen Sie die Option Automatisches Update für Stammzertifikate deaktivieren aktivieren. Bevor Sie diese Änderung vornehmen, sollten Sie sicherstellen, dass die Änderung den Sicherheitsrichtlinien Ihres Unternehmens entspricht.

- 1. Aktivieren Sie dies, indem Sie den Editor für **lokale Gruppenrichtlinien** auf dem Computer öffnen (klicken Sie auf die Windows-Startleiste und geben Sie **gpedit.msc ein**).
- Navigieren Sie im Windows-Editor f
 ür lokale Gruppenrichtlinien zu Computerkonfiguration > Administrative Vorlagen > System > Internetkommunikationsverwaltung > Internetkommunikationseinstellungen.
- 3. Doppelklicken Sie auf **Automatische Aktualisierung des Stammzertifikats deaktivieren**, und wählen Sie **Aktiviert** aus.
- 4. Klicken Sie auf **OK.**

Beachten Sie, dass diese Einstellung möglicherweise durch eine Domänenrichtlinie gesteuert wird. In diesem Fall muss sie auf dieser Ebene deaktiviert werden.

Ihr Zertifikat verbleibt jetzt auf dem Computer, obwohl es nicht von einer "vertrauenswürdigen Zertifizierungsstelle eines Drittanbieters" stammt, da Windows Update die Windows Update-Website nicht kontaktiert, um zu überprüfen, ob Microsoft die Zertifizierungsstelle zu seiner Liste der vertrauenswürdigen Zertifizierungsstellen hinzugefügt hat.

9.2 Erstellen eines CA-Zertifikats

Führen Sie dieses Skript auf einem Computer mit eingeschränktem Zugriff, der nicht mit Ihrem MOBOTIX HUB-System verbunden ist, einmal aus, um ein CA-Zertifikat zu erstellen.



Auf dem Computer, den Sie zum Erstellen von Zertifikaten verwenden, muss Windows 10 oder Windows Server OS 2016 oder höher ausgeführt werden. Beachten Sie, dass beim Erstellen von Zertifikaten auf diese Weise die Zertifikate mit dem Computer verknüpft sind, auf dem sie installiert sind. Wenn sich der Computername ändert, kann der virtuelle Computer erst gestartet werden, wenn die Zertifikate erneut erstellt und auf dem Computer neu

Mit diesem Skript werden zwei Zertifikate erstellt:

- Ein privates Zertifikat: Nach dem Ausführen des Skripts ist nur im Speicher für persönliche Zertifikate für den aktuellen Benutzer vorhanden. Es wird empfohlen, eine Sicherung zu erstellen, die auf einem Medium (USB) an einem sicheren Ort aufbewahrt wird, und vorzugsweise zwei Sicherungen, die an physisch unterschiedlichen Orten aufbewahrt werden. Mit Ausnahme der Sicherungen sollte dieses Zertifikat niemals den Computer verlassen, auf dem Sie das Zertifikat erstellt haben
- Ein öffentliches Zertifikat, das als vertrauenswürdiges Zertifikat auf allen Clientcomputern importiert werden soll
- 1. In Anhang A am Ende dieses Handbuchs finden Sie ein Skript zum Erstellen des Zertifizierungsstellenzertifikats. Kopieren Sie den Inhalt.
- 2. Öffnen Sie Editor, und fügen Sie den Inhalt ein.

Es ist sehr wichtig, dass die Linien an den gleichen Stellen wie in Anhang A unterbrochen werden. Sie können die Zeilenumbrüche in Notepad hinzufügen oder alternativ diese PDF-Datei mit Google Chrome erneut öffnen , den Inhalt erneut kopieren und in Notepad

1	CreateCACertificate.ps1 - Notepad	- - ×
File Edit Format View Help		
<pre># Run this script once, to crea # Private certificate for sign Sca_certificate = New-SelFSign, KeyUsage CertSign, CRLSign, DJ # Thumbprint of private certifi Set-Content -Path "\$PSScriptRoc # Public CA certificate to trus Export-Certificate -Cert "Cert:</pre>	e a certificate that can sign multiple recording server certificates g other certificates (in certificate store) Certificate -CertStoreLocation cert:\CurrentUser\My -DnsName 'VMS Certificate Aut italSignature -FriendlyName 'VMS CA Certificate' ate used for signing other certificates \ca_thumbprint.txt" -Value \$ca_certificate.Thumbprint (Third-Party Root Certification Authorities) CurrentUser\My\\$(\$ca_certificate.Thumbprint)" -FilePath "\$PSScriptRoot\root-author	thority' -KeyusageProperty All ' ority-public.cer"
¢		3
		n 8, Col 130

 Klicken Sie im Editor auf Datei -> Speichern unter, nennen Sie die Datei CreateCACertificate.ps1, und speichern Sie sie lokal wie folgt:

 $C: \verb|Certificates\verb|CreateCACertificate.ps1.||$

4. Wechseln Sie im Datei-Explorer zu C:\Zertifikate, und wählen Sie die **Datei CreateCACertificate.ps1** aus.

5. Wählen Sie im Menü Datei die Option Windows PowerShell öffnen und dann Windows PowerShell als Administrator öffnen aus.

				Cert		
File Open <u>n</u> ew window	*	Open Windows PowerShell	Open •	Select all		
Open command prompt		Open Windows PowerShell as administrator	Properties History Open	Select:		
Open Windows Powe <u>r</u> Shell						
			Date modified	Туре	Size	
CX Delete matory			04-02-2019 11:31	File folder		
0			04-02-2019 11:31	File folder		
Eleip			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	Filefolder		
Carries 1		i CreateCACertificate.ps1	31-01-2019 15:01	Windows PowerShell Script		1 KB
📕 This PC						

 Geben Sie in PowerShell an der Eingabeaufforderung .\CreateCACertificate.ps1 ein, und drücken Sie die EINGABETASTE.

🛃 Admir	nistrator: Windows Pov	werShell				×
PS C:\Cer	tificates> .\Crea	ateCACertifi	cate.ps1			^
Direc	tory: C:\Certifi	cates				
Mode	LastW	riteTime	Length	Name		
-a	31-01-2019	09:29	844	root-authority-public.cer		
PS C:\Cer	tificates>					

7. Vergewissern Sie sich, dass die **root-authority-public.cer** Datei in dem Ordner angezeigt wird, in dem Sie das Skript ausgeführt haben.



Auf Ihrem Computer ist es möglicherweise erforderlich, dass Sie die PowerShell-Ausführungsrichtlinie ändern. Wenn ja, geben Sie **Set-ExecutionPolicy RemoteSigned**

10 Installieren von Zertifikaten auf den Clients

Nachdem Sie das Zertifikat der Zertifizierungsstelle erstellt haben, vertrauen Sie dem Zertifikat der öffentlichen Zertifizierungsstelle, indem Sie es auf allen Computern installieren, die als Clients für den Dienst fungieren, wie in den Beschreibungen unter Einführung in Zertifikate auf Seite 5 beschrieben.



Siehe Importieren von Client-Zertifikaten auf Seite 129 für ein alternatives Verfahren zur manuellen Installieren von Zertifikaten auf Clients.

8. Kopieren Sie die Datei root-authority-public.cer Datei von dem Computer aus, auf dem Sie das Zertifizierungsstellenzertifikat erstellt haben (C:\Zertifikate\root-authority-public.cer) auf den Computer, auf dem der MOBOTIX HUB-Client installiert ist.



Informationen darüber, welche Client- und Serverdienste und Integrationen Fordern Sie das Zertifikat an, siehe Einführung in die Zertifikate auf Seite 5.



9. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie Zertifikat installieren aus.

		×
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 Car	icel

- 10. Wählen Sie im **Zertifikatimport-Assistenten** aus, ob das Zertifikat im Speicher des lokalen Computers installiert werden soll, und klicken Sie auf **Weiter**.
- 11. Wählen Sie diese Option aus, um den Speicher, in dem das Zertifikat installiert werden soll, manuell zu suchen.

Certificate Store			
Certificate stores are sy	stem areas where certifi	cates are kept.	
Windows can automatic the certificate.	illy select a certificate st	ore, or you can spec ased on the type of	ify a location fo certificate
Place all certificat	es in the following store	7	
Certificate store:			1
			Browse

12. Klicken Sie auf Durchsuchen, wählen Sie Vertrauenswürdige Stammzertifizierungsstellen aus, und klicken Sie auf OK. Klicken Sie dann auf Weiter.



13. Klicken Sie im Dialogfeld Abschließen des Zertifikatimport-Assistenten auf Fertig stellen.



Wenn Sie eine Sicherheitswarnung erhalten, dass Sie ein Stammzertifikat installieren möchten, klicken Sie auf **Ja**, um fortzufahren.

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 24/136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Garage Context Milestone XProtect® VMSLeitfaden für Zertifikate - Milestone XProte Milestone XProtect® VMS

Completing th	e Certificate Import Wizard
The certificate will be in	nported after you click Finish.
You have specified the	following settings:
Certificate Store Sele Content	cted by User Trusted Root Certification Authorities Certificate

14. Sie erhalten einen Bestätigungsdialog über den erfolgreichen Import.



15. Um zu überprüfen, ob das Zertifikat importiert wurde, starten Sie die Microsoft Management Console.



16. Wählen Sie in der Microsoft Management Console im **Menü Datei** die Option **Snap-In hinzufügen/entfernen...**

Open Ctrl+O	Name	Actions
Save Ctrl+S	There are no items to show in this view	Console Root
Save As	THE CITE IS IN THE SHOW IT DIS STOR	More Actions
Add/Remove Snap-in Ctrl+M Options		
Recent File		
Exit		

17. Wählen Sie das Snap-In Zertifikate aus, und klicken Sie auf Hinzufügen.

nap-in ActiveX Control	Vendor Microsoft Cor	^		Console Root	Edit Extensions
Authorization Manager	Microsoft Cor	-			Feable
Component Services	Microsoft Cor				$(M) a \in \overline{P}()$
Computer Managem Device Manager	Microsoft Cor Microsoft Cor		<u>A</u> dd >	ľ	THEYE DEVIC
P Disk Management Event Viewer	Microsoft and Microsoft Cor	L.			
Folder	Microsoft Cor				
Internet Informatio	Microsoft Cor				
Internet Informatio IP Security Monitor	Microsoft Cor				Advanced
cription:					

18. Wählen Sie aus, dass das Snap-In Zertifikate für das **Computerkonto verwalten muss**.

Certificates snap-in		×
This snap in will always manage certificates for:		
<u>My</u> user account		
Computer account		

19. Wählen Sie Lokaler Computer als den Computer aus, den das Snap-In verwalten soll, und klicken Sie auf Fertig stellen.

ect Computer	
Select the computer you want this snap-in to manage.	
This snap-in will always manage: Cocal computer: (the computer this console is running on)	
O Another computer:	Bycase
	the command line. This

20. Klicken Sie auf **OK**, nachdem das Snap-In hinzugefügt wurde.

allable Sliabults.			Selected snap-ins:		
nap-in ActiveX Control	Vendor Microsoft Cor	^	Console Root	Edit E <u>x</u> te	ensions
Authorization Manager	Microsoft Cor			1.80	sole.
Component Services	Microsoft Cor			1 Méri	s th
Device Manager	Microsoft Cor	5	>	Here	Dave
Event Viewer	Microsoft Cor				
Group Policy Object	Microsoft Cor				
Internet Informatio	Microsoft Cor			_	
IP Security Monitor	Microsoft Cor	v		Ad <u>v</u> ar	nced

21. Stellen Sie sicher, dass das Zertifikat in der mittleren Ansicht der vertrauenswürdigen Stammzertifizierungsstellen aufgeführt ist.

Teilbaum.

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 28/136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Milestone XProtect® VMS

MOBOTIX HUB – Leitfaden für Zertifikate - Installieren von Zertifikaten auf den Clients

<mark>} E</mark> ile <u>A</u> ction <u>V</u> iew Fav <u>o</u> rites <u>W</u> indow <u>H</u> e ▶ ● ▲ 〒 1 ▲ ● 3 〒	lp				_ # :
Console Root	Issued To	Issued By	Exp ^	Actions	
 Certificates (Local Computer) 	[] 10.5.14.40	10.5.14.40	20:	Certificates	
 Personal Personal Trusted Root Certification Authorities Certificates Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Third-Party Root Certification Authorities Trusted People Client Authentication Issuers Preview Build Roots AAD Token Issuer eSIM Certificate Cartificates Remote Desktop Certificate Enrollment Requests Smart Card Trusted Roots Windows Live ID Token Issuer 	10.5.6.101 AddTrust External CA Root Baltimore CyberTrust Root CKMS Ckms 3 Public Primary Certificat Copyright (c) 1997 Microsoft C DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert Global Root CA GlobalSign Root CA Jor CyberTrust Global Root Hotspot 2.0 Trust Root CA - 03 Microsoft Root Certificate Auth Starfield Class 2 Certification A Starfield Services Root Certificate Symantec Enterprise Mobile Ro	10.5.6.101 AddTrust External CA Root Baltimore CyberTrust Root CKMS Class 3 Public Primary Certificatio Copyright (c) 1997 Microsoft Corp. DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert High Assurance EV Root DST Root CA X3 Equifax Secure Certificate Authority GeoTrust Global CA GlobalSign GlobalSign GlobalSign Root CA Go Daddy Class 2 Certification Au GTE CyberTrust Global Root Hotspot 2.0 Trust Root CA - 03 Microsoft Root Certificate Authori Microsoft Root Certificate Microsoft	20: 202 203 204 205 205 205 205 205 205 205 205	More Actions	

22. Wiederholen Sie die Schritte auf dem nächsten Computer, der als Client für den Dienst ausgeführt wird, für den die Verschlüsselung aktiviert ist , bis Sie das Zertifikat auf allen relevanten Computern installiert haben.

11 SSL-Zertifikat erstellen

Nachdem Sie das Zertifizierungsstellenzertifikat auf allen Clients installiert haben, können Sie Zertifikate erstellen, die auf allen Computern installiert werden, auf denen Server ausgeführt werden (Aufzeichnungsserver, Verwaltungsserver, mobile Server oder Failoverserver).



Führen Sie auf dem Computer, auf dem Sie das Zertifizierungsstellenzertifikat erstellt haben, in dem Ordner, in dem Sie das Zertifizierungsstellenzertifikat abgelegt haben, das Serverzertifikatskript aus, um SSL-Zertifikate für alle Server zu erstellen. In Anhang B am Ende dieses Handbuchs finden Sie ein Skript zum Erstellen von Serverzertifikaten.

1. Öffnen Sie Editor, und fügen Sie den Inhalt ein.



Es ist sehr wichtig, dass die Linien an den gleichen Stellen wie in Anhang B unterbrochen werden. Sie können die Zeilenumbrüche in Notepad hinzufügen oder alternativ diese PDF-Datei mit Google Chrome erneut öffnen , den Inhalt erneut kopieren und in Notepad

- 2. Klicken Sie im Editor auf Datei -> Speichern unter, nennen Sie die Datei CreateServerCertificate.ps1, und speichern Sie sie lokal im selben Ordner wie das Zertifizierungsstellenzertifikat, wie folgt: C:\Certificates\CreateServerCertificate.ps1.
- 3. Wechseln Sie im Datei-Explorer zu C:\Zertifikate, und wählen Sie die Datei CreateServerCertificate.ps1 aus.
- 4. Wählen Sie im Menü Datei die Option Windows PowerShell öffnen und dann Windows PowerShell als Administrator öffnen aus.

Open <u>n</u> ew window	*	2 Open Windows Powe <u>r</u> Shell	Open •	Select all			
Open command grompt	+	Open Windows PowerShell as administrator	Properties	Select	n		
Open Windows Powe <u>r</u> Shell							
D			Date modified	Туре		Size	
Delete history			04-02-2019 11	:31 File fold	er		
0.04			04-02-2019 11	:31 File fold	er		
Пер			04-02-2019 11	:31 File fold	er		
1			04-02-2019 11	:31 File fold	er		
Close			04-02-2019 11	53 File fold	er		
			04-02-2019 11	:31 File fold	er		
and a		CreateCACertificate.ps1	31-01-2019 15	:01 Window	s PowerShell Script		1 K
🖳 This PC		CreateServerCertificate.p	s1 25-01-2019 15	31 Window	s PowerShell Script		3 K

5. Geben Sie in PowerShell an der Eingabeaufforderung .\CreateServerCertificate.ps1 ein, und drücken Sie die EINGABETASTE.

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 30/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Milestone XProtect® VMS

 Geben Sie den DNS-Namen f
ür den Server ein. Wenn der Server mehrere Namen hat, z.B. f
ür den internen und externen Gebrauch, f
ügen Sie diese hier durch ein Leerzeichen getrennt hinzu. Dr
ücken Sie die Eingabetaste.



Um den DNS-Namen zu finden, öffnen Sie den Datei-Explorer auf dem Computer, auf dem der Aufzeichnungsserver-Dienst ausgeführt wird. Klicken Sie mit der rechten Maustaste auf **Dieser PC,** und wählen Sie **Eigenschaften aus**. Verwenden Sie den



Drücken Sie **die** Eingabetaste.



Um die IP-Adresse zu finden, können Sie die Eingabeaufforderung auf dem Computer öffnen, auf dem der Aufzeichnungsserverdienst ausgeführt wird. Geben Sie **ipconfig /all ein**. Wenn Sie das MOBOTIX HUB-System installiert haben, können Sie den Management Client öffnen, zum Server navigieren und die IP-Adresse auf der

8. Geben Sie ein Kennwort für das Zertifikat an, und drücken Sie **die Eingabetaste**, um die Erstellung abzuschließen.



Sie verwenden dieses Kennwort, wenn Sie das Zertifikat auf den Server importieren.

Die Datei Subjectname.pfx wird in dem Ordner angezeigt, in dem Sie das Skript ausgeführt haben.

9. Führen Sie das Skript aus, bis Sie über Zertifikate für alle Server verfügen.

12 SSL-Zertifikat importieren

Nachdem Sie die SSL-Zertifikate erstellt haben, installieren Sie sie auf den Computern, auf denen der Serverdienst



Denken Sie daran, dass jedes Zertifikat auf einem bestimmten Server erstellt wird.

ausgeführt wird.

- 10. Kopieren Sie die entsprechende Datei "Subjectname.pfx" von dem Computer, auf dem Sie das Zertifikat erstellt haben, auf den entsprechenden Serverdienstcomputer.
- 11. Starten Sie auf dem Serverdienstcomputer Computerzertifikate verwalten.
- 12. Klicken Sie auf **Persönlich**, klicken Sie mit der rechten Maustaste auf **Zertifikate** und wählen Sie **Alle Aufgaben** > **Importieren**.



13. Wählen Sie diese Option aus, um das Zertifikat in den Speicher des **lokalen Computers zu importieren,** und klicken Sie auf **Weiter**.

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

14. Navigieren Sie zur Zertifikatsdatei, und klicken Sie auf Weiter.

and the second		
Specify the file you war	nt to import.	
File name:		
C:\Users\gis\Document	its Wy Received Files (VMS-REC	Browse.
Note: More than one o	ertificate can be stored in a sir	ngle file in the following form
Personal Information	n Exchange-PKCS #12 (.PFX,.	P12)
Cryptographic Mess	age Syntax Standard-PKCS #	7 Certificates (.P7B)
Microsoft Serialized	Certificate Store (.SST)	

15. Geben Sie das Kennwort für den privaten Schlüssel ein, das Sie beim Erstellen des Serverzertifikats angegeben haben, und klicken Sie dann auf **Weiter**.

MOBOTIX HUB – Leitfaden für Zertifikate - SSL-Zertifikat importieren

Pr	ivate 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 Tack use all extended respective
	Indude all extended properties.

16. Legen Sie die Datei im Zertifikatsspeicher: Persönlich ab, und klicken Sie dann auf Weiter.

MOBOTIX HUB – Leitfaden für Zertifikate - SSL-Zertifikat importieren

Certificate Store				
Certificate	e stores are system	areas where cert	ificates are kept.	
Windows	can automatically se	lect a certificate	store, or you can si	pecify a location for
the certifi	cate.	al a n a str		
() Aut	tomatically select the	e certificate store	based on the type	of certificate
Place	ce all certificates in t	the following stor	ė	
Ce	rtificate store:			
P	ersonal			Browse

17. Überprüfen Sie die Informationen und klicken Sie auf **Fertig stellen**, um das Zertifikat zu importieren.
| ha cartificate will be imported after | r vou dick Einich |
|---------------------------------------|--------------------------------------|
| ne cel alcate vill de imported al te | |
| ou have specified the following se | ttings: |
| Certificate Store Selected by User | Personal |
| File Name | C: \Users\gis\Desktop\VMS-REC-01.pfx |
| | |
| | |
| | |
| | |

Das importierte Zertifikat wird in der Liste angezeigt.

Issued To	Issued By
VMS Certificate Authority	localhost VMS Certificate Authority VMS Certificate Authority
	VMS-REC-01

18. Um einem Dienst die Verwendung des privaten Schlüssels des Zertifikats zu gestatten, klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie **Alle Aufgaben** >

^{12.1} Verwalten Sie private Schlüssel.

3

1. Fügen Sie Leseberechtigungen für den Benutzer hinzu, der die MOBOTIX HUB-VMS-Dienste ausführt, die das Serverzertifikat verwenden müssen .

Administrators (Administrate	(and	
NETWORK SERVICE	515)	
	Add	Remove
ermissions for NETWORK ERVICE	Allow	Deny
Full control		
Read	J	
Special permissions		

2. Fahren Sie mit dem nächsten Computer fort, bis Sie alle Serverzertifikate installiert haben.

13 Erstellen eines SSL-Zertifikats für den Failover-Management-Server

MOBOTIX HUB Management Server Failover wird auf zwei Computern konfiguriert. Um sicherzustellen, dass die Clients dem ausgeführten Verwaltungsserver vertrauen, installieren Sie das SSL-Zertifikat auf dem primären und dem sekundären Computer.

Um das SSL-Zertifikat für den Failovercluster zu erstellen und zu installieren, müssen Sie zuerst das Zertifizierungsstellenzertifikat installieren.

Führen Sie auf dem Computer, auf dem Sie das Zertifizierungsstellenzertifikat erstellt haben, in dem Ordner, in dem Sie das Zertifizierungsstellenzertifikat abgelegt haben, das Skript für das

Failoververwaltungsserverzertifikat aus, um ein SSL-Zertifikat für den primären und den sekundären Computer zu erstellen.



Auf dem Computer, den Sie zum Erstellen von Zertifikaten verwenden, muss Windows 10 oder Windows Server 2016 oder höher ausgeführt werden.

- 3. Kopieren Sie in Anhang C dieses Handbuchs das Skript zum Erstellen von Zertifikaten für den Failover-Verwaltungsserver.
- 4. Öffnen Sie Editor, und fügen Sie das Skript ein.



Es ist sehr wichtig, dass die Linien an den gleichen Stellen brechen, wie im Anhang gezeigt C. Sie können die Zeilenumbrüche in Notepad hinzufügen oder alternativ diese PDF-Datei mit Google Chrome erneut öffnen, den Inhalt erneut kopieren und in Notepad

5. Wählen Sie im Editor Datei -> Speichern unter aus, nennen Sie die Datei CreateFailoverCertificate.ps1, und speichern Sie sie lokal im selben Ordner wie das Zertifizierungsstellenzertifikat:

Beispiel: C:\Certificates\CreateFailoverCertificate.ps1.

- 6. Wechseln Sie im Datei-Explorer zu C:\Zertifikate, und wählen Sie die Datei CreateFailoverCertificate.ps1 aus.
- 7. Wählen Sie im Menü Datei die Option Windows PowerShell öffnen und dann Windows PowerShell als Administrator öffnen aus.

Open <u>n</u> ew window	*	Open Windows PowerShell	Open •		Select all	ne		
Open command <u>p</u> rompt	*	Open Windows PowerShell as administrator	Properties History Open		Invert sel	ection		
Open Windows Powe <u>r</u> Shell	*							
Dalata biston			Date modifi	ied	Тур	e	Size	
Delete history			04-02-2019	11:	31 File	folder		
2 11-12			04-02-2019	11:	31 File	folder		
Пер			04-02-2019	116	31 File	folder		
S			04-02-2019	11:	31 File	folder		
Close			04-02-2019	11:	53 File	folder		
			04-02-2019	11:	31 File	folder		
1. J.		🧟 CreateCACertificate.ps1	31-01-2019	15:	01 Wir	dows PowerShell Script		1.6
🜉 This PC		CreateServerCertificate.p	s1 25-01-2019	15:	31 Wir	dows PowerShell Script		3 K

8. Geben Sie in PowerShell an der Eingabeaufforderung .\CreateFailoverCertificate.ps1 ein, und drücken Sie die EINGABETASTE.

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 40/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Milestone XProtect® VMS

9. Geben Sie die FQDNs und die Hostnamen für den primären und den sekundären Computer an, getrennt durch ein Komma.

Beispiel: pc1host,pc1host.domain,pc2host,pc2host.domain.

- 10. Drücken Sie **die** Eingabetaste.
- 11. Geben Sie die virtuelle IP-Adresse des Failoverclusters an. Drücken Sie **die** Eingabetaste.
- 12. Geben Sie ein Kennwort für das Zertifikat an, und drücken Sie **die Eingabetaste**, um die Erstellung abzuschließen.

, series and s

Sie verwenden dieses Kennwort, wenn Sie das Zertifikat auf den Server importieren.

Die Datei [virtualIP].pfx wird in dem Ordner angezeigt, in dem Sie das Skript ausgeführt haben. Importieren Sie das Zertifikat auf die gleiche Weise, wie Sie ein SSL-Zertifikat importieren würden, siehe Importieren eines SSL-Zertifikats auf Seite 29. Importieren Sie das Zertifikat auf dem primären und dem sekundären Computer.

14 Installieren von Zertifikaten f ür die Kommunikation mit dem Mobile Server

Um ein HTTPS-Protokoll zum Herstellen einer sicheren Verbindung zwischen dem mobilen Server und Clients und Diensten zu verwenden, müssen Sie ein gültiges Zertifikat auf dem Server anwenden. Das Zertifikat bestätigt, dass der Zertifikatsinhaber berechtigt ist, sichere Verbindungen herzustellen. In MOBOTIX HUB-VMS wird die Verschlüsselung pro Mobile Server aktiviert oder deaktiviert. Sie aktivieren oder deaktivieren die Verschlüsselung entweder während der Installation des Produkts MOBOTIX HUB VMS oder mithilfe des Server-Konfigurators. Wenn Sie die Verschlüsselung auf einem Mobile Server aktivieren, verwenden Sie eine verschlüsselte Kommunikation mit allen Clients, Diensten und Integrationen, die



٢

Wenn Sie die Verschlüsselung für eine Servergruppe konfigurieren, muss sie entweder mit einem Zertifikat aktiviert werden, das zum selben Zertifizierungsstellenzertifikat gehört, oder, wenn die Verschlüsselung deaktiviert ist, auf allen Computern in der Servergruppe deaktiviert

Datenströme abrufen.



14.1 Hinzufügen eines Zertifizierungsstellenzertifikats zum Server

Fügen Sie das Zertifizierungsstellenzertifikat zum Mobile Server hinzu, indem Sie wie folgt vorgehen: Öffnen Sie auf dem Computer, auf dem der Mobile Server gehostet wird, die Microsoft Management Console.

> Bestimmte Parameter hängen von der Zertifizierungsstelle ab. Lesen Sie die Dokumentation Ihrer Zertifizierungsstelle, bevor Sie fortfahren.

Ð	Type the name of a progressource, and Windows	gram, folder, docun will open it for you	nent, or Internet
Open:	mmd		Y

1. Wählen Sie in der Microsoft Management Console im Menü Datei die Option Snap-In hinzufügen/entfernen....

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 42/136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Milestone XProtect® VMS

MOBOTIX HUB – Leitfaden für Zertifikate - Installieren von Zertifikaten für die

Open Ctrl+O	1		
Save Ctrl+S	Name	Console Root	
Save As	i nere are no items to snow in this view.	More Actions	-
Add/Remove Snap-in Ctrl+M			
Options			
Recent File			
Exit			

- 2. Wählen Sie das Snap-In Zertifikate aus, und klicken Sie auf Hinzufügen.
- 3. Klicken Sie auf OK.

Available shaphilis.			5	elected snap-ins:	-
Snap-in	Vendor	^		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor			carrier uncates - currer	Remove
Authorization Manager	Microsoft Cor				I constant a
Certificate Templates	Microsoft Cor				1 hourseller
Certification Authority	Microsoft Cor				
Component Services	Microsoft Cor	1-2			Marias Crises
Computer Managem	Microsoft Cor	A	dd >		
📩 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:					
	hannes and the second		1. 54		(F)

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 43/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Gur A Context Milestone XProtect® VMSLeitfaden für Zertifikate - Milestone XProte

4. Erweitern Sie das Objekt Zertifikate. Klicken Sie mit der rechten Maustaste auf den Ordner Persönlich und wählen Sie Alle Aufgaben > Erweiterte Vorgänge > Benutzerdefinierte Anforderung erstellen.

) 🗖 🖬 🖬 🖓 🖬 🖬				
Certificates - Current User	Object T	lype ficates		
Tru Find Certificates				
En All Tasks	>	Find Certificates		
Ac View	*	Request New Certificate Import		
Th New Taskpad View		Advanced Operations	2	Create Custom Request
Cli Export List				Enroll On Behalf Of Manage Enrollment Policies
Sn Help				

- 5. Klicken Sie im Zertifikatregistrierungs-Assistenten auf Weiter, und wählen Sie Ohne Registrierungsrichtlinie fortfahren aus.
- 6. Klicken Sie auf Weiter.

- 🗆 X

Certificate Enrollment

Select Certificate Enrollment Policy

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

Configured by you	Add New
Custom Request	
Proceed without enrollment policy	
	Net Carca
	INEXT CANCE

7. Wählen Sie die Vorlage CNG-Schlüssel (keine Vorlage) und das CMC-Anforderungsformat aus und

Certificate Enrollment		
Custom request		
Chose an option from	the list below and configure the certificate options a	s required.
Template:	(No template) CNG key	3
	<u>Suppress</u> default extensions	
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 certifi the certificate template.	icate request, even when this
a barra barran		
		Next Canc
		and the second second

- 8. Erweitern Sie, um die Details der benutzerdefinierten Anforderung anzuzeigen, und klicken Sie auf Eigenschaften.
- 9. Füllen Sie auf der Registerkarte Allgemein die Felder Anzeigename und Beschreibung mit dem Domänennamen aus, der bei der Zertifizierungsstelle registriert ist.



Das Anforderungsformat hängt von der Zertifizierungsstelle ab. Wenn das falsche Format ausgewählt wird, gibt die Zertifizierungsstelle einen Fehler aus, wenn die Zertifikatsignieranforderung (Certificate Signing Request, CSR) übermittelt wird. Wenden

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 45/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Garage Context Milestone XProtect® VMSLeitfaden Seite 45/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Seite 45/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Seite 45/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Seite 45/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Seite 45/ 136Leitfaden Seite 45/ Milestone XProtect® VMS

MOBOTIX HUB – Leitfaden für Zertifikate - Installieren von Zertifikaten für die

ertificate	ePropen	185				
General	Subject	Extensions	Private Key	Signature		
A friend	ly name	and descript	tion will make	e it easier to ident	tify and use a certi	ificate.
Friendly	name:					
TestLab	Domain	.com				
Descript	ion:					
TestLab	Domain	.com				
				-		

10. Geben Sie auf der **Registerkarte Betreff** die Parameter ein, die für die jeweilige Zertifizierungsstelle erforderlich sind.

Beispielsweise sind der Antragstellername, der **Typ** und **der Wert** für jede Zertifizierungsstelle unterschiedlich. Ein Beispiel sind die folgenden erforderlichen Informationen:

- Trivialname:
- Organisation:
- Organisationseinheit :
- Stadt/Ort:
- Bundesland/Provinz:
- Land/Region:

ertificate	Propert	ies					×
General	Subject	Extensions	Private Key	Signature			
The subje can enter can be us	ect of a r inform sed in a	certificate is ation about certificate.	the user or c the types of :	omputer to w subject name	hich the c and alterr	ertificate is native name	issued. You values that
Subject o	of certifie	cate					
The user	or com	puter that is	receiving the	certificate			
Subject n	ame:						
Туре:					CN=T	est for Docs	R.
Country	i.	2	0	Add		UT Lab	
Value:			×	Remove	L=Map S=MN C=US/	ole Grove	
Alternativ	ve name	e:	1				
Туре:					1		
Director	y name	-					
Value:		_		Add >			
1			10	Remove			
				OK		Cancel	Apply

 Für einige Zertifizierungsstellen sind keine Erweiterungen erforderlich. Wechseln Sie jedoch bei Bedarf zur Registerkarte Erweiterungen, und erweitern Sie das Menü Schlüsselverwendung. Fügen Sie der Liste Ausgewählte Optionen die erforderlichen Optionen aus der Liste Verfügbare Optionen hinzu . 12. Erweitern Sie auf der Registerkarte Privater Schlüssel das Menü Schlüsseloptionen.

General Subject Extensions	Private Key Signature		
The following are the certific	ate extensions for this	certificate type.	1
Key usage			•
The key usage extension des	scribes the purpose of a	a certificate.	
Available options:		Selected options:	
CRL signing Data encipherment		Digital signature Key certificate signing	
Decipher only		Key encipherment	
Encipher only Key agreement	Add >		
Non repudiation	< Remove	T I	
Make these key usages cr	itical		. 1
☑ Make these key usages cr Extended Key Usage (applic	itical ation policies)		*
Make these key usages cr Extended Key Usage (applic Basic constraints	itical ation policies)		*

13. Legen Sie die Schlüsselgröße auf 2048 fest, und wählen Sie die Option aus, um den privaten Schlüssel exportierbar zu machen.

Ì

Die Variable für die Schlüsselgröße wird von der Zertifizierungsstelle bestimmt, daher kann ein Schlüssel mit höherer Größe erforderlich sein. Möglicherweise sind auch andere Optionen, wie z. B. ein bestimmter Hash-Algorithmus (sha256), erforderlich. Passen Sie

MOBOTIX HUB – Leitfaden für Zertifikate - Installieren von Zertifikaten für die

and the second se	>
General Subject Extensions Private Key Signature	2
Cryptographic Service Provider	۷
Key options	*
Set the key length and export options for the priva	te key.
Key size: 2048	~
Make private key exportable	
Allow private key to be archived	
Strong private key protection	
Select Hash Algorithm	*
Select Hash Algorithm to be used for this request	
11 / 11 St	~
Hash Algorithm: sha256	
Hash Algorithm: sha256	
Hash Algorithm: sha256 Select Signature Format	v
Hash Algorithm: sha256 Select Signature Format	v
Hash Algorithm: sha256 Select Signature Format	~

- 14. Sofern die Zertifizierungsstelle keine Signatur verlangt, besteht der nächste Schritt darin, auf **OK zu** klicken.
- 15. Wenn alle Zertifikateigenschaften definiert wurden, klicken Sie **im Zertifikatregistrierungs-**Assistenten auf Weiter.

- 🗆 X

	Certificate	Enrollment
- 14	Certificate	Etti oniti ente

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 Key encipherment	
Application polic	ties:	
Validity period (d	lays):	
		Properties

 Wählen Sie einen Speicherort für die Zertifikatanforderung und ein Format aus. Navigieren Sie zu diesem Speicherort, und geben Sie einen Namen für die REQ-Datei an. Das Standardformat ist Basis 64, einige Zertifizierungsstellen erfordern jedoch das Binärformat.

17. Klicke	en Sie auf Fertig stellen .	
		- 🗆 X
Ş	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 request me of your certificate request, and then
	File Name:	
	C:\Users\Administrator\Desktop\CSR6.1.21	Browse
	File format: Base 64	
	Obmary	
		Finish Cancel

Es wird eine .req-Datei generiert, die Sie zum Anfordern eines signierten Zertifikats verwenden müssen.

14.2 Laden Sie die .req-Datei hoch, um im Gegenzug ein signiertes Zertifikat zu erhalten.

Jede Zertifizierungsstelle hat einen anderen Prozess zum Hochladen von .req-Dateien, um im Gegenzug ein signiertes Zertifikat zu erhalten. In der Dokumentation Ihrer Zertifizierungsstelle finden Sie Informationen zum Abrufen eines signierten Zertifikats.

Bei der Arbeit mit dem Mobile Server wird empfohlen, eine Zertifizierungsstelle eines Drittanbieters zu verwenden. In den meisten Fällen ist es erforderlich, eine .ZIP Datei herunterzuladen und den Inhalt auf den Computer zu extrahieren, auf dem der Mobile Server gehostet wird.

Es gibt mehrere Dateitypen, die in den extrahierten .ZIP Dateiinhalten enthalten sein können.

. CER oder . CRT-Dateien können auf ähnliche Weise installiert werden. Klicken Sie mit der rechten Maustaste auf die Datei, und wählen Sie Zertifikat installieren aus.

aus dem Kontextmenü.

In den folgenden Schritten wird eine . CER-Datei von einer internen Zertifizierungsstelle.

Ihre Zertifizierungsstelle benötigt den Inhalt der REQ-Datei. Sie werden aufgefordert, den gesamten Text der REQ-Datei, einschließlich der Anfangs- und Endzeilen, zu kopieren und den Text in ein Feld einzufügen, das in einem von der Zertifizierungsstelle verwalteten Portal zur Verfügung gestellt wird.

© MOBOTIX AG www.mobotix.com

Ì

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 51/136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Milestone XProtect® VMS

1. Navigieren Sie zum Speicherort der REQ-Datei, öffnen Sie sie in Editor, und fügen Sie den Text in ein Feld ein, das in einem von Ihrer Zertifizierungsstelle verwalteten Portal zur Verfügung gestellt wird.

CSR6.1.21 - Notepad	-		×
File Edit Format View Help			
BEGIN NEW CERTIFICATE REQUEST			
MIIGBAYJKoZIhvcNAQcCoIIF9TCCBfECAQMxDzANBglghkgBZQMEA	gEFADO	CBEoG	
CCsGAQUFBwwCoIIEPASCBDgwggQ0MGQwYgIBAgYKKwYBBAGCNwoKA	TFRME	CAQAW	
AwIBATFFMEMGCSsGA00BgjcVFDE2MD0CA0UMC010LTBBMDAwNDY3D	BIJUCE	WOTAW	
MDQ2N1xBZG1pbm1zdHJhdG9yDAdNTUMuRVhFMIIDxqCCA8ICAQEwg	g07MII	CowIB	
ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAgMAk10MRQwEgYDVQQHD	AtNYXE	SZSBH	
cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UECgwDTUpUMRYwF	AYDVOC	DDA1U	
ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC	gKCAQE	A7G1/	
5z1YrUGOo4dW1/b3o35rpcQQbyOUE0K1NWjaIy4YrRPM9HjhKReTh	bcSnxd	ldj6eR	
Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ//Zi08bEPobL	v8YnWi	eNDuw	
lkaJWWRx3mb1/Yz0f1bwZrKFT3nkrXYOFYmZOR19W0J+Iin0Btziw	iC8DHt	+bxST	
nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9qC47RP9yMjyu	uEtpdR	9ERoR	
qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs18zBATRXkk/k	RI+Po6	cXNJp	
Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEAYI3DQIDMQ4WD	DEwLjA	uMTc3	
NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/wQEAwICpDAdB	gNVHQ4	IEFgQU	
vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCNxUUMTYwNAIBB	QwLSVA	TMEEW	
MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b3IMB01NQy5FW	EUwZgY	KKwYB	
BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFMAb	wBmAHQ	AdwBh	
AHIAZQAgAEsAZQB5ACAAUwB0AG8AcgBhAGcAZQAgAFAAcgBvAHYAa	QBkAGL	JAcgMB	
ADANBgkqhkiG9w0BAQsFAAOCAQEAqtKb5HCh2a1BD2QcKdFuhVQbN	xg+G5w	/cVkZt	
7bXdwVuzoAxd9BFd+uVy4D3TmvXtineT3GVWQbKJCcxRZeTKPBFnH	GØSeaY	upUrG	
cX4ySsKR1xGSuOhsfIVa/5NXiIYgYxMh1z3nt2CDw+RNqAp/1gLV2	cLsui0	1y5ib	
088po4/b9eiXV7A1DWFy7ecw/7Z20a07Sa0OaRbwzGJ8HelIiVEjf	yAt7KL	oufAq	
LkeSaJtjokkJuGPdr+ykjfuCmIF4hSbcOxzVkPCQbiHOwSxDGlkqY	HZ8Xru	1665Q6	
0L7QgBXCc7tcecDieqbYmp50LJPpqEQDQiYjzg57j3eYIFNYYjAAM	AAxgg	SLMIIB	
hwIBA4AUvruQxeU1yku5Cem3anpu1cbMEDAwDQYJYIZIAWUDBAIBB	QCgSjA	XBgkq	
hkiG9w0BCQMxCgYIKwYBBQUHDAIwLwYJKoZIhvcNAQkEMSIEICk1S	Kp5MUj	Ma+vr	
DU1UXU+V05r1F8bNdM0mDgYfmjCiMA0GCSqGSIb3DQEBAQUABIIBA	Ejqqe4	GSGE4	
oZQj0vbWrAP0Ab2u8epFm7ZIMZzsJSzR0z98m+R+1R2mCoqWC0SSa	fybJ70)1Jhly	
A3eqzDYxAu9p9drJft317sGAERE/i1D3BFvKZZQH0sz0JNRwDp3qB	yHHzVC	ULUEI	
JSOpYvI1s3S23ZYEedQLp35Xy87378zLLGLpgGKTK4teav1IitUJw	VCKikL	.47uyF	
uOY4XLagwI1WWALsPF1+5ZcVNZMvsgzsbuMEXvjBkFKyhMv49oisg	FcLJ1A	loMtWn	
7Mbq8K6ckbKkVpuvmWThkVTp1W3hIS/i/J0X7c2unA25LxAC/P/Ly	WhPt/V	/k/oqf	
06jNaHC/zBQ=			
END NEW CERTIFICATE REQUEST			

Windows (CRLF Ln 1, Col 1 100%

© MOBOTIX AG www.mobotix.com Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 52/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden f

MOBOTIX HUB – Leitfaden für Zertifikate - Installieren von Zertifikaten für die

 Wenn Sie das Zertifikat von Ihrer Zertifizierungsstelle erhalten, navigieren Sie zum Ordner "Downloads" (oder an einem anderen Ort, an dem Sie den Ordner auf dem Computer speichern möchten), klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie **"Zertifikat** installieren" aus.



3. Akzeptieren Sie die Sicherheitswarnung, wenn sie angezeigt wird.

4. Wählen Sie diese Option aus, um das Zertifikat für den lokalen Computer zu installieren, und klicken Sie auf

X

🚽 Certificate Import Wizard

We	lcome to the Certificate I	Import Wizard
This w lists fr	wizard helps you copy certificates, certi rom your disk to a certificate store.	ificate trust lists, and certificate revocation
A cert and conne	tificate, which is issued by a certificatio contains information used to protect dat actions. A certificate store is the system	n authority, is a confirmation of your identity ta or to establish secure network n area where certificates are kept.
Stor	re Location	
0	Current User	
۲	Local Machine	
To coi	ntinue, click Next.	

Weiter.

5. Wählen Sie einen Speicherort aus, navigieren Sie zum Speicher für persönliche Zertifikate, und klicken Sie auf **Weiter**.

Next:

Cancel

MOBOTIX HUB – Leitfaden für Zertifikate - Installieren von Zertifikaten für die

🗧 🔄 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 locati the certificate. Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Brows	Select Certificate Store X Select the certificate store you want to use.
	Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Intrusted Certificates Show physical stores
Next	OK Cancel

6. Beenden Sie den Assistenten zum Installieren von Zertifikaten.

14.3 Aktivieren der Verschlüsselung auf dem Mobile Server

Nachdem das Zertifikat auf dem Computer installiert wurde, auf dem der Mobile Server gehostet wird, gehen Sie wie folgt vor.

- 1. Öffnen Sie auf einem Computer, auf dem ein Mobile Server installiert ist, den **Server-Konfigurator** über:
- Das Windows-Startmenü oder
- Den Mobile Server Manager, indem Sie mit der rechten Maustaste auf das Mobile Server Manager-Symbol in der Taskleiste des Computers klicken
- 2. Aktivieren Sie im Server-Konfigurator unter Mobiles Streaming-Media-Zertifikat die Option Encryption.
- 3. Klicken Sie auf Zertifikat auswählen, um eine Liste mit eindeutigen Antragstellernamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und auf dem lokalen Computer im Windows-Zertifikatspeicher installiert sind.
- 4. Wählen Sie ein Zertifikat aus, um die Kommunikation zwischen dem MOBOTIX HUB Mobile Client und dem MOBOTIX HUB Web Client mit dem Mobile Server zu verschlüsseln.

Wählen Sie **Details** aus, um Informationen zum Windows-Zertifikatspeicher für das ausgewählte Zertifikat anzuzeigen. Dem Benutzer des Mobile Server-Dienstes wurde Zugriff auf den privaten Schlüssel gewährt. Es ist erforderlich, dass dieses Zertifikat auf allen Clients vertrauenswürdig ist.

MOBOTIX HUB – Leitfaden für Zertifikate - Installieren von Zertifikaten für die

Server Configurator		-		×
Encryption	Encryption			
Registering servers	It is recommended to secure communication with encryption. Le	arn m	ore	
anguage selection	Server certificate Applies to: management server, recording server, failover server, data collector			
	Encryption: On	0		
	-		Details	
	Carolificate innied by MS-Organization-P2P-Acona [2021], Expirer 3/8/2021			
	Mobile streaming media certificate Applies to mobile and web clients that retrieve data streams from the mobil server	le		
	Encryption: On	Ð		
	Normal V		Details	
	Certificate instead by Expires 5/3//H21			
		1	Apply	

5. Klicken Sie auf Übernehmen.

Wenn Sie Zertifikate anwenden, wird der Mobile Server-Dienst neu gestartet.

Weitere Informationen finden Sie unter:

Video zum Powershell-Prozess.

Whitepaper zu Zertifikaten mit dem Mobile Server.

15 Installieren von Zertifikaten von Drittanbietern oder kommerziellen Zertifizierungsstellen für die Kommunikation mit dem Management Server oder **Recording Server**

Management-Server und Aufzeichnungsserver benötigen keine vertrauenswürdigen Zertifikate von Drittanbietern oder kommerziellen Zertifizierungsstellen für die Verschlüsselung, aber Sie können diese Zertifikate verwenden, wenn dies Teil Ihrer Sicherheitsrichtlinie ist, und sie werden automatisch von Client-Workstations und -Servern als vertrauenswürdig eingestuft.

Der Vorgang ist identisch mit der Installation des Mobile Server-Zertifikats.



Ì

Wenn Sie die Verschlüsselung für eine Servergruppe konfigurieren, muss sie entweder mit einem Zertifikat aktiviert werden, das zum selben Zertifizierungsstellenzertifikat gehört, oder, wenn die Verschlüsselung deaktiviert ist, auf allen Computern in der Servergruppe deaktiviert

Zertifikate, die von einer Zertifizierungsstelle (CA) ausgestellt wurden, verfügen über eine Kette von Zertifikaten, und im Stammverzeichnis dieser Kette befindet sich das Stammzertifikat der Zertifizierungsstelle. Wenn ein Gerät oder Browser dieses Zertifikat sieht, vergleicht es sein Stammzertifikat mit den auf dem Betriebssystem (Android, iOS, Windows usw.) vorinstallierten Zertifikaten. Wenn das Stammzertifikat in der Liste der vorinstallierten Zertifikate aufgeführt ist, stellt das Betriebssystem dem Benutzer sicher, dass

15.1 Hinzufügen eines Zertifizierungsstellenzertifikats zum Server

Fügen Sie dem Server das Zertifizierungsstellenzertifikat hinzu, indem Sie wie folgt vorgehen. Öffnen Sie auf dem Computer, auf dem der MOBOTIX HUB-Server gehostet wird, die Microsoft Management Console.

> Bestimmte Parameter hängen von der Zertifizierungsstelle ab. Lesen Sie die Dokumentation Ihrer Zertifizierungsstelle, bevor Sie fortfahren.

1. Wählen Sie in der Microsoft Management Console im Menü Datei die Option Snap-In hinzufügen/entfernen....

💷 Run	×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	mmd
	OK Cancel <u>B</u> rowse

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 57/136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Milestone XProtect® VMS

MOBOTIX HUB – Leitfaden für Zertifikate - Installieren von Zertifikaten von

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

- 2. Wählen Sie das Snap-In Zertifikate aus, und klicken Sie auf Hinzufügen.
- 3. Klicken Sie auf **OK.**

Available shaphils.			Selected snap-ins:	-
Snap-in	Vendor	^	Console Root	Edit Extensions
ActiveX Control	Microsoft Cor		Certificates - Current User	Remove
Authorization Manager	Microsoft Cor			
Certificate Templates	Microsoft Cor			thusth
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor		10000	Manus Crown
Computer Managem	Microsoft Cor		dd >	
击 Device Manager	Microsoft Cor			
📅 Disk Management	Microsoft and			
Enterprise PKI	Microsoft Cor			
Event Viewer	Microsoft Cor			
Folder	Microsoft Cor			E CONTRACTOR
Group Policy Object	MICrosoft Cor	*		Advanced
Description:				
	the second second second			

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 58/136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Gur Context VMSLeitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden VMSLeitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden VMSLeitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden VMSLeitfaden VMSLeitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden VMSLeitfaden

4. Erweitern Sie das Objekt Zertifikate. Klicken Sie mit der rechten Maustaste auf den Ordner Persönlich und wählen Sie Alle Aufgaben > Erweiterte Vorgänge > Benutzerdefinierte Anforderung erstellen.

Console Root	- Current User	Object T	ype ficates		
Tri	Find Certificates				
> 📫 En	All Tasks	>	Find Certificates		
Ac	View New Window from Here	>	Request New Certificate Import		
Th	New Taskpad View		Advanced Operations	Cre	ate Custom Request
Tru Cli	Refresh Export List			Enro Mar	oll On Behalf Of nage Enrollment Policies
> 📄 Sn	Help				

- 5. Klicken Sie im Zertifikatregistrierungs-Assistenten auf Weiter, und wählen Sie Ohne Registrierungsrichtlinie fortfahren aus.
- 6. Klicken Sie auf Weiter.

	11
-	X

Certificate Enrollment

Select Certificate Enrollment Policy

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

Configured by you	Add Nev
Custom Request	
Proceed without enrollment policy	

7. Wählen Sie die Vorlage CNG-Schlüssel (keine Vorlage) und das CMC-Anforderungsformat aus und klicken Sie auf Weiter.

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 59/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Garage Context Milestone XProtect® VMSLeitfaden Seite Sei Milestone XProtect® VMS

MOBOTIX HUB – Leitfaden für Zertifikate - Installieren von Zertifikaten von

8. Erweitern Sie, um die **Details** der benutzerdefinierten Anforderung anzuzeigen, und klicken Sie auf

- 0

X

Certificate Enrollment

Custom request

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

Template:	(No template) CNG key -
	Suppress default extensions
Request format	○ <u>P</u> KCS #10
	● <u>C</u> MC
Note: Key archival option is specified	is not available for certificates based on a custom certificate request, even when this in the certificate template.
	<u>N</u> ext Cancel
Eigenschaften.	
Das Anforder ausgewählt	ungsformat hängt von der Zertifizierungsstelle ab. Wenn das falsche Format

9. Füllen Sie auf der **Registerkarte Allgemein** die Felder **Anzeigename** und **Beschreibung** mit dem Domänennamen aus, der bei der Zertifizierungsstelle registriert ist.

General	Subject	Extensions	Private Key	Signature		
A frienc	lly name	and descript	ion will make	e it easier to identi	fy and use a certi	ficate.
Friendly	name:					
TestLa	Domain	.com				
Descrip	tion:					
TestLa	Domain	.com				
				-	1	-

- 10. Geben Sie auf der **Registerkarte Betreff** die Parameter ein, die für die jeweilige Zertifizierungsstelle erforderlich sind.
- 11. Beispielsweise sind der Antragstellername, der **Typ** und **der Wert** für jede Zertifizierungsstelle unterschiedlich. Ein Beispiel sind die folgenden erforderlichen Informationen:
- Trivialname:
- Organisation:
- Organisationseinheit :
- Stadt/Ort:
- Bundesland/Provinz:
- Land/Region:

cremear	eriopeit	10			
General	Subject	Extensions	Private Key	Signature	
The sub can ente can be u	ject of a er inform used in a	certificate is ation about certificate.	the user or c the types of :	omputer to w subject name	which the certificate is issued. You and alternative name values that
Subject	of certifi	cate			
The use	r or com	puter that is	receiving the	certificate	
Subject	name:				
Туре:					CN=Test for Docs
Count	ry .			Add	OU=MJT Lab
Value:			<	Remove	L=Maple Grove S=MN C=USA
Alternat	ive name	2	4		
Туре:					
Directo	ory name	-	-		
Value:				Add >	
			10	Remiove	
_					

 Für einige Zertifizierungsstellen sind keine Erweiterungen erforderlich. Wechseln Sie jedoch bei Bedarf zur Registerkarte Erweiterungen, und erweitern Sie das Menü Schlüsselverwendung. Fügen Sie der Liste Ausgewählte Optionen die erforderlichen Optionen aus der Liste Verfügbare Optionen hinzu .

ertificat	e Propert	ties						>
General	Subject	Extensions	Private Key	Signature				
The foll	lowing ar	e the certific	ate extensior	is for this cer	tificate t	ype.	. 1	^
Key us	sage						~	
The ke	y usage e	extension des	cribes the pu	irpose of a ce	ertificate			
Availab	ole option	ns:			Select	ted options:		
CRL sig Data e	gning ncipherm	ient			Digita Key c	al signature ertificate signi	ng	
Deciph	ner only			11.	Key e	ncipherment		
Enciph Key ag	reement		A	dd >				
Non re	pudiation	n	20	emove				
			-					
Mak Mak	te these k	ey usages cr	itical					
Extend	ded Key U	lsage (applic	ation policie	s)			¥	
Basic	constrain	ts					*	
								V
				-				

13. Erweitern Sie auf der Registerkarte Privater Schlüssel das Menü Schlüsseloptionen.

Ì

14. Legen Sie die Schlüsselgröße auf 2048 fest, und wählen Sie die Option aus, um den privaten Schlüssel exportierbar zu machen.

Die Variable für die Schlüsselgröße wird von der Zertifizierungsstelle bestimmt, daher kann ein Schlüssel mit höherer Größe erforderlich sein. Möglicherweise sind auch andere Optionen, wie z. B. ein bestimmter Hash-Algorithmus (sha256), erforderlich. Passen Sie

Certificate P	properti	ies				×
General S	ubject	Extensions	Private Key	Signature		
Cryptog	raphic S	Service Prov	ider			۷
Key optio	ons					*
Set the ke	ey lengt	th and expor	t options for	the private key	te.	
Key size:	2048				~	
Make ;	orivate	key exportal	ble			
Allow	private	key to be ar	chived			
Strong	private	e key protect	tion			
Select H	ash Ala	orithm				
Select Ha	sh Alac	prithm to be	used for thi	s request		
Hash Alg	orithm:	sha256			~	
Select Sid	anature	e Format				~

- 15. Sofern die Zertifizierungsstelle keine Signatur verlangt, besteht der nächste Schritt darin, auf **OK zu** klicken.
- 16. Wenn alle Zertifikateigenschaften definiert wurden, klicken Sie im Zertifikatregistrierungs-Assistenten auf Weiter.

Certificate mormati	on	
Click Next to use the optio request, and then click Ne	ns already selected for this template, or click Details to cι xt.	ustomize the certificat
Custom request	i STATUS: Available	Details A
The following option	s describe the uses and validity period that apply to this t	ype of certificate:
Key usage:	Digital signature Key certificate signing Key engineerent	
Application polic	ies:	
Validity period (d	ays):	
validity period (d	126.1	Properties
validity period (d		
validity period (d		1
Validity Denou tu	-1-1-	Properties

- Wählen Sie einen Speicherort für die Zertifikatanforderung und ein Format aus. Navigieren Sie zu diesem Speicherort, und geben Sie einen Namen für die REQ-Datei an. Das Standardformat ist Basis 64, einige Zertifizierungsstellen erfordern jedoch das Binärformat.
- 18. Klicken Sie auf **Fertig stellen**.

	- 🗆 X
Certificate Enrollment	
Where do you want to save the offline request?	
If you want to save a copy of your certificate request or want to proces to your hard disk or removable media. Enter the location and name of click Finish.	ss the request later, save the request your certificate request, and then
File Name:	Browse
File format:	Englishing and a second s

Es wird eine .req-Datei generiert, die Sie zum Anfordern eines signierten Zertifikats verwenden müssen.

Finish

Cancel

15.2 Laden Sie die .req-Datei hoch, um im Gegenzug ein signiertes Zertifikat zu erhalten.

Jede Zertifizierungsstelle hat einen anderen Prozess zum Hochladen von .req-Dateien, um im Gegenzug ein signiertes Zertifikat zu erhalten. In der Dokumentation Ihrer Zertifizierungsstelle finden Sie Informationen zum Abrufen eines signierten Zertifikats.

In den meisten Situationen mit Zertifizierungsstellen von Drittanbietern ist es erforderlich, eine .ZIP

Datei herunterzuladen und den Inhalt auf den Computer zu extrahieren, auf dem der MOBOTIX HUB-Server gehostet wird.

Es gibt mehrere Dateitypen, die in den extrahierten .ZIP Dateiinhalten enthalten sein können.

. CER oder . CRT-Dateien können auf ähnliche Weise installiert werden. Klicken Sie mit der rechten Maustaste auf die Datei, und wählen Sie Zertifikat installieren aus.

aus dem Kontextmenü.

E

In den folgenden Schritten wird eine . CER-Datei von einer internen Zertifizierungsstelle.

Ihre Zertifizierungsstelle benötigt den Inhalt der REQ-Datei. Sie werden aufgefordert, den gesamten Text der REQ-Datei, einschließlich der Anfangs- und Endzeilen, zu kopieren und den Text in ein Feld einzufügen, das in einem von der Zertifizierungsstelle verwalteten Portal zur Verfügung gestellt wird.

Ì

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 66/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Milestone XProtect® VMS

1. Navigieren Sie zum Speicherort der REQ-Datei, öffnen Sie sie in Editor, und fügen Sie den Text in ein Feld ein, das in einem von Ihrer Zertifizierungsstelle verwalteten Portal zur Verfügung gestellt wird.

CSR6.1.21 - Notepad	-		×
File Edit Format View Help			
BEGIN NEW CERTIFICATE REQUEST			
MIIGBAYJKoZIhvcNAOcCoIIF9TCCBfECAOMxDzANBglghkgBZOM	EAgEFAD	CCBEoG	
CCsGAOUFBwwCoIIEPASCBDgwggO0MGOwYgIBAgYKKwYBBAGCNwol	KATERME	BCAOAW	
AWIBATEEMEMGCSsGA00BgicVEDE2MD0CA0UMC010LTBBMDAWNDY	3DB1 JUC	WOTAW	
MD02N1xBZG1pbm1zdHJhdG9vDAdNTUMuRVhFMIIDxaCCA8ICA0E	wgg07MI	ICOWIB	
ADBpMOwwCgYDV00GEwNVU0ExCzAJBgNVBAgMAk10MR0wEgYDV00	HDATNYX	BsZSBH	
cm927TEOMA4GA1UECwwHTUpUTExhY1EMMAoGA1UECgwDTUpUMRY	FAYDVO	DDDA1U	
ZXN0IGZvciBEb2NzMIIBIjANBgkahkiG9w0BA0EFAA0CA08AMII	BCgKCAO	EA7G1/	
5z1YrUG0o4dW1/b3o35rpc00bv0UE0K1NWiaIv4YrRPM9HihKRe	ThbcSnx	ddi6eR	
Ziz50dV7tJ0atds9GuaPYX7PrGfsUs5/4AvEK8nDJ//Zi08bEPol	bLv8YnW	ieNDuw	
<pre>lkaJWWRx3mb1/Yz0f1bwZrKFT3nkrXY0FYmZ0R19W0J+Iin0Btz</pre>	iwiC8DH	t+bxST	
nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9gC47RP9yMin	vuuEtpd	R9ERoR	
gJJoOK6CdrKLU5kZFiDTIVbs0F3mNgnHCyzs7cEEs18zBATRXkk	/kRI+Po	5cXNJp	
Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEAYI3DQIDM04	WDDEwLjA	AuMTc3	
NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/wQEAwICpDA	dBgNVHQ4	4EFgQU	
vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCNxUUMTYwNAI	BBQwLSV	AtMEEw	
MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b3IMB01NQy5	FWEUwZg	YKKwYB	
BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFM	AbwBmAH	QAdwBh	
AHIAZQAgAEsAZQB5ACAAUwB0AG8AcgBhAGcAZQAgAFAAcgBvAHY	AaQBkAG	JAcgMB	
ADANBgkqhkiG9w0BAQsFAAOCAQEAqtKb5HCh2a1BD2QcKdFuhVQ	bNxg+G5	vcVkZt	
7bXdwVuzoAxd9BFd+uVy4D3TmvXtineT3GVWQbKJCcxRZeTKPBF	nHG0Sea'	YupUrG	
cX4ySsKR1xGSuOhsfIVa/5NXiIYgYxMh1z3nt2CDw+RNqAp/1gL	V2cLsui	01y5ib	
088po4/b9eiXV7A1DWFy7ecw/7Z20a07Sa00aRbwzGJ8He1IiVE	jfyAt7KI	LoufAq	
LkeSaJtjokkJuGPdr+ykjfuCmIF4hSbcOxzVkPCQbiHOwSxDG1k	qYHZ8Xru	u665Q6	
0L7QgBXCc7tcecDieqbYmp50LJPpqEQDQiYjzg57j3eYIFNYYjA	AMAAxgg	GLMIIB	
hwIBA4AUvruQxeU1yku5Cem3anpu1cbMEDAwDQYJYIZIAWUDBAI	BBQCgSj	AXBgkq	
hkiG9w0BCQMxCgYIKwYBBQUHDAIwLwYJKoZIhvcNAQkEMSIEICk	1SKp5MU	jMa+vr	
DU1UXU+V05r1F8bNdM0mDgYfmjCiMA0GCSqGSIb3DQEBAQUABII	BAEjqqe	4GSGE4	
oZQj0vbWrAP0Ab2u8epFm7ZIMZzsJSzR0z98m+R+1R2mCoqWC05	SafybJ70	DlJhly	
A3eqzDYxAu9p9drJft317sGAERE/i1D3BFvKZZQH0sz0JNRwDp3	qByHHzV	CULUEI	
JSOpYvI1s3S23ZYEedQLp35Xy87378zLLGLpgGKTK4teav1IitU	JwVCKikl	L47uyF	
uOY4XLagwI1WWALsPF1+5ZcVNZMvsgzsbuMEXvjBkFKyhMv49oi	sgFcLJ1/	AoMtWn	
7Mbq8K6ckbKkVpuvmWThkVTp1W3hIS/i/J0X7c2unA25LxAC/P/	LyWhPt/	/k/oqf	
06jNaHC/zBQ=			
END NEW CERTIFICATE REQUEST			
1			

Windows (CRLF Ln 1, Col 1 100%

© MOBOTIX AG www.mobotix.com Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 67/136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Guerren Aufligen AufligenA

MOBOTIX HUB – Leitfaden für Zertifikate - Installieren von Zertifikaten von

 Wenn Sie das Zertifikat von Ihrer Zertifizierungsstelle erhalten, navigieren Sie zum Ordner "Downloads" (oder an einem anderen Ort, an dem Sie den Ordner auf dem Computer speichern möchten), klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie **"Zertifikat** installieren" aus.



3. Akzeptieren Sie die Sicherheitswarnung, wenn sie angezeigt wird.

4. Wählen Sie diese Option aus, um das Zertifikat für den lokalen Computer zu installieren, und klicken Sie auf

X

Certificate Import Wizard

Welcome to the Certific	ate Import Wizard
This wizard helps you copy certificates ists from your disk to a certificate stor	s, certificate trust lists, and certificate revocation re.
A certificate, which is issued by a certi and contains information used to prote connections. A certificate store is the	ification authority, is a confirmation of your identity ect data or to establish secure network system area where certificates are kept.
Store Location	
O Current User	
Local Machine	
To continue, click Next.	

Weiter.

5. Wählen Sie einen Speicherort aus, navigieren Sie zum Speicher für persönliche Zertifikate, und klicken Sie auf **Weiter**.

Next:

Cancel

MOBOTIX HUB – Leitfaden für Zertifikate - Installieren von Zertifikaten von

+	🚁 Certificate Import Wizard	*
	Certificate Store Certificate stores are system areas where certificates are kept.	
	Automatically select the certificate store based on the type of certificate Automatically select the certificate store based on the type of certificate Certificate store: Browse	Select Certificate Store × Select the certificate store you want to use.
		OK Cancel

6. Beenden Sie den Assistenten zum Installieren von Zertifikaten.

15.3 Aktivieren der Verschlüsselung zum und vom Management-Server

Sie können die bidirektionale Verbindung zwischen dem Management-Server und dem zugehörigen Datensammler verschlüsseln, wenn Sie über einen Remoteserver des folgenden Typs verfügen:

- Aufzeichnungsserver •
- Ereignisserver
- Protokollserver
- LPR-Server •
- Mobiler Server

Wenn Ihr System über mehrere Aufzeichnungsserver oder Remote-Server verfügt, müssen Sie die Verschlüsselung auf allen Servern aktivieren.

15.3.1 Voraussetzungen:

Wenn Sie die Verschlüsselung für eine Servergruppe konfigurieren, muss sie entweder mit einem Zertifikat aktiviert werden, das zum selben Zertifizierungsstellenzertifikat gehört, oder, wenn die Verschlüsselung deaktiviert ist, auf allen Computern in der Servergruppe deaktiviert

Auf dem Computer, auf dem der Verwaltungsserver gehostet wird, ist ein

Serverauthentifizierungszertifikat vertrauenswürdig Aktivieren Sie zunächst die Verschlüsselung auf dem Verwaltungsserver.

© MOBOTIX AG www.mobotix.com

J.

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 70/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden VMSLeitfaden Milestone XProtect® VMS

Schritte:

- 7. Öffnen Sie auf einem Computer, auf dem ein Management-Server installiert ist, den **Server-Konfigurator** über:
- Das Windows-Startmenü oder
- Den Management-Server-Manager, indem Sie mit der rechten Maustaste auf das Symbol Management-Server-Manager in der Taskleiste des Computers klicken.
- 1. Aktivieren Sie im Server-Konfigurator unter Serverzertifikat die Option Verschlüsselung.
- 2. Klicken Sie auf Zertifikat auswählen, um eine Liste mit eindeutigen Antragstellernamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und auf dem lokalen Computer im Windows-Zertifikatspeicher installiert sind.
- 3. Wählen Sie ein Zertifikat aus, um die Kommunikation zwischen dem Aufzeichnungsserver, dem Verwaltungsserver, dem Failover-Server und dem Datensammlerserver zu verschlüsseln.
- 4. Wählen Sie **Details** aus, um Informationen zum Windows-Zertifikatspeicher für das ausgewählte Zertifikat anzuzeigen.

Milestone Server Configura	or			
ncryption	Encryption			
egistering servers	It is recommended to secure communication	n with encryption. Learn r	more	
nguage selection	Server certificate Applies to: management server, recording server, fa collector, api gateway, log server	ilover 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 server	a streams from the mobile		
	Encryption: Off			
	Select certificate	~		
	No certificate selected			
			Apply	

5. Klicken Sie auf Übernehmen.

Um die Aktivierung der Verschlüsselung abzuschließen, besteht der nächste Schritt darin, die Verschlüsselungseinstellungen auf jedem Aufzeichnungsserver und jedem Server mit einem Datensammler (Ereignisserver, Protokollserver, LPR-Server und mobiler Server) zu aktualisieren. Installieren von Active Directory-Zertifikatdiensten

Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS) sind ein Microsoft-Produkt, das PKI-Funktionen (Public Key Infrastructure) ausführt. Es fungiert als Serverrolle, die es Ihnen ermöglicht, eine Public Key-Infrastruktur (PKI) zu erstellen und Open-Key-Kryptografie, computergestützte Authentifizierung und erweiterte Markierungsfunktionen für Ihre Zuordnung bereitzustellen.

In diesem Dokument wird AD CS beim Installieren von Zertifikaten verwendet:

- In einer Domänenumgebung (siehe Installieren von Zertifikaten in einer Domäne für die Kommunikation mit dem Management Server oder Recording Server auf Seite 86)
- In einer Arbeitsgruppenumgebung (siehe Installieren von Zertifikaten in einer • Arbeitsgruppenumgebung für die Kommunikation mit dem Management-Server oder dem Aufzeichnungsserver auf Seite 104)

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 72/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Milestone XProtect® VMS
15.3.2 So installieren Sie AD CS:

1. Wählen Sie in der Server-Manager-Anwendung Verwalten > Rollen und Funktionen hinzufügen aus.

ᡖ Server Manager		–
GO Server M	anager • Dashboard	
Tashboard	WELCOME TO SERVER MANAGER	Remove Roles and Features Add Servers
Local Server All Servers File and Storage Services	1 Configure this	Create Server Group S local server S server Manager Properties
	QUICK START	

- 2. Klicken Sie unter Bevor Sie beginnen auf Weiter.
- 3. Wählen Sie unter Installationstyp die Option Rollenbasierte oder featurebasierte Installation aus, und klicken Sie auf Weiter.
- 4. Wählen Sie in der Serverauswahl den lokalen Server als Ziel für die Installation aus, und klicken Sie auf Weiter
- 5. Wählen Sie unter Serverrollen die Rolle Active Directory-Zertifikatdienste aus. Überprüfen Sie die Liste der zu installierenden Funktionen, und klicken Sie auf Funktionen hinzufügen.

	Select one or more roles to install on the sel	lected server.
and the second	Roles	Description
New Telegion	Active Directory Certificate Services	Active Directory Certificate Servic
Fization in	Ad Ad Ad Ad Ad Ad Ad Ad Certificate Services? Di Fa The following tools are require have to be installed on the sar Ha Active Directory C [Tools] Certificate Re Re Vc W W	red to manage this feature, but do not me server. Tation Tools Certificate Services Tools Cation Authority Management Tools
		Cance

6. Klicken Sie auf **Weiter**.

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 73/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Milestone XProtect® VMS

- 7. Klicken Sie **unter** Features auf **Weiter**. Alle erforderlichen Funktionen werden für die Installation ausgewählt.
- 8. Lesen Sie in **AD CS** die Beschreibung der Active Directory-Zertifikatdienste, und klicken Sie auf **Weiter**.
- 9. Wählen Sie unter Rollendienste Folgendes aus:
 - Zertifizierungsstelle
 - Webdienst für die Zertifizierungsregistrierungsrichtlinie
 - Webdienst für die Zertifizierungsregistrierung
 - Webregistrierung der Zertifizierungsstelle
 - Registrierungsdienst für Netzwerkgeräte

Fügen Sie bei der Auswahl der einzelnen Rollendienste die erforderlichen Features hinzu, um die Installation der einzelnen Dienste zu unterstützen .

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

- 10. Klicken Sie auf **Weiter**.
- 11. Wählen Sie unter **Bestätigung** die Option **Zielserver bei Bedarf automatisch neu starten aus**, und klicken Sie auf **Installieren**.

- 12. Wenn die Installation abgeschlossen ist, klicken Sie auf die Schaltfläche Schließen.
- 13. Wählen Sie das Benachrichtigungsflag in der Server-Manager-Anwendung aus.



- 14. Eine Meldung, dass die Konfiguration nach der Bereitstellung gestartet werden soll, wird unter dem **Benachrichtigungsflag** aufgeführt.
- 15. Klicken Sie auf den Link, um mit der Konfiguration der installierten Dienste zu beginnen.



- 16. Der Konfigurationsassistent für Active Directory-Zertifikatdienste wird gestartet.
- 17. Wählen Sie unter **Anmeldeinformationen** das Benutzerkonto aus, das zum Ausführen der installierten Dienste erforderlich ist. Wie im Text angegeben, ist die Mitgliedschaft in den Gruppen "Lokaler Administrator" und "Unternehmensadministrator" erforderlich.
- 18. Geben Sie die erforderlichen Kontoinformationen ein und klicken Sie auf **Weiter**.

DESTIN ICES Iocal Administrators gr Enterprise Admins gro	IP-0A00 roup:	RVER 0450
iCES local Administrators gi Enterprise Admins gro	roup: up:	
local Administrators gi Enterprise Admins gro	roup: up:	
Enterprise Admins gro	up:	
Enterprise Admins gro	up:	
Change		
	Change	Change Configure Canc

- 19. Wählen Sie unter Rollendienste die folgenden Dienste aus:
 - Zertifizierungsstelle
 - Webregistrierung der Zertifizierungsstelle
- 20. Klicken Sie auf **Weiter**.

AD CS Conngulation					^
Role Services			DESTINAT	TION SER	VER 1450
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation	Select Role Services to conf Certification Authority Certification Authority Web Enrollme Online Responder Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service	figure ent evice			
	More about AD CS Server Roles				

21. Wählen Sie **unter** Setup-Typ die Option **Eigenständige Zertifizierungsstelle** aus und klicken Sie auf **Weiter**.

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

22. Wählen Sie unter **CA-Typ** die Option zum Installieren einer **Root-CA aus**, und klicken Sie auf **Weiter**.

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

23. n **Privater Schlüssel**, wählen Sie die Option zum Erstellen eines neuen privaten Schlüssels aus, und klicken Sie auf **Weiter**.

AD US Configuration	,
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	 Use existing private key Use this option to ensure continuity with previously issued certificates when reinstalling a CA. Select a certificate and use its associated private key Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key. Select an existing private key on this computer Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.
	More about Private Key

24. Wählen Sie unter **Kryptografie** die Option **RSA#Microsoft Software Key Storage Provider** für die Option Kryptografieanbieter mit einer **Schlüssellänge** von 2048 und einem Hashalgorithmus von SHA256 aus.

Klicken Sie auf **Weiter**.

Cryptography f	or CA		DESTINATIO	ON SERVER
Credentials Role Services Setup Type	Specify the cryptographic options Select a cryptographic provider:		Key length:	
CA Type Private Key	RSA#Microsoft Software Key Storage Provider	4: 64	2048	.*
Cryptography CA Name Validity Period Certificate Database Confirmation	SHA256 SHA384 SHA512 SHA1 MD5	accessed I	by the CA.	

25. Geben Sie unter **Name** der Zertifizierungsstelle den Namen für die Zertifizierungsstelle ein, und klicken Sie auf **Weiter**.

Standardmäßig lautet der Name "localhost-CA" - unter der Annahme, dass der Computername des lokalen Servers "localhost" lautet.

— 🗆 X
DESTINATION SERVER IP-0A000450
Specify the name of the CA Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.
IP-0A000450-CA
Distinguished name suffix:
CN=IP-0A000450-CA
More about CA Name

26. Wählen Sie unter **Gültigkeitszeitraum** die Standardgültigkeitsdauer von 5 Jahren aus und klicken Sie auf **Weiter**.

📥 AD CS Configuration					-		×
Validity Period					DESTINA	TION SEF	RVER 0450
Credentials Role Services Setup Type	Spec Select t	ify the validit	y period for the certificate ger	nerated for this cert	ification authority (CA):	
CA Type	5	Years	*				
Private Key	CA expi	iration Date: 4/27/2	2026 3:27:00 PM				
Cryptography	The vali	dity period config	ured for this CA certi	ficate should excee	d the validity period	for the	
CA Name	certifica	tes it will issue.			a the renary period		
Validity Period							
Certificate Database							
Confirmation							
	More a	bout Validity Period	d				
			. Purchas				1

27. Geben Sie unter Zertifikatdatenbank die Speicherorte der Datenbank und der Protokolldatenbank ein.

Die Standarddatenbankspeicherorte für den Zertifikatspeicher sind: C:\Winksystem32\Certlog

- 28. Klicken Sie auf Weiter.
- 29. Überprüfen Sie unter Bestätigung die ausgewählten Konfigurationsoptionen und klicken Sie auf Konfigurieren, um den Konfigurationsprozess zu starten.
- 30. Wenn die Konfiguration abgeschlossen ist, klicken Sie auf Schließen.
- 31. Wenn Sie aufgefordert werden, zusätzliche Rollendienste zu konfigurieren, klicken Sie auf Nein.
- 32. Starten Sie den lokalen Server neu, um sicherzustellen, dass er bereit ist, als Active Directory-Zertifikatserver zu dienen.

15.4 Installieren von Zertifikaten in einer Domäne für die Kommunikation mit dem Management-Server oder dem Aufzeichnungsserver

Wenn Client- und Serverendpunkte alle in einer Domänenumgebung ausgeführt werden, ist es nicht erforderlich, CA-Zertifikate an Client-Arbeitsstationen zu verteilen. Die Gruppenrichtlinie innerhalb der Domäne verarbeitet die automatische Verteilung aller Zertifikate der vertrauenswürdigen Zertifizierungsstelle an alle Benutzer und Computer in der Domäne.

Dies liegt daran, dass bei der Installation einer Unternehmensstammzertifizierungsstelle Gruppenrichtlinien verwendet werden, um das Zertifikat für alle Benutzer und Computer in der Domäne an den Zertifikatspeicher der vertrauenswürdigen Stammzertifizierungsstellen weiterzugeben.

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 83/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden VMSLeitfaden Milestone XProtect® VMS

Sie müssen ein Domänenadministrator oder ein Administrator mit Schreibzugriff auf Active Directory sein, um eine Unternehmensstammzertifizierungsstelle installieren zu können.

Microsoft stellt eine umfangreiche Dokumentation für Windows Server-Betriebssysteme bereit, die Vorlagen für Serverzertifikate, die Installation der Zertifizierungsstelle und die Zertifikatbereitstellung enthält, die in der Übersicht über die Bereitstellung von

15.4.1 Hinzufügen eines Zertifizierungsstellenzertifikats zum Server

Ì

Fügen Sie dem Server das Zertifizierungsstellenzertifikat hinzu, indem Sie wie folgt vorgehen.

1. Öffnen Sie auf dem Computer, auf dem der MOBOTIX HUB-Server gehostet wird, die Microsoft Management Console.

	T	6.11	
e	resource, and Windows	gram, folder, docur will open it for you	nent, or internet I.
0	mmd		~
Upen:	mind		

2. Wählen Sie in der Microsoft Management Console im Menü Datei die Option Snap-In

🕌 File	Action View Favorites Wind New Ctrl+N	w Help		- 8 x		
	Open Ctrl+O	Na	Name	Actions		
	Save Ctrl+		There are no items to show in this view.	Console Root		
E	Add/Remove Snap-in Ctrl+N			More Actions		
	Options					
	Exit					

hinzufügen/entfernen....

3. Wählen Sie das Zertifikat-Snap-In aus, klicken Sie aufZertifikat-Snap-In hinzufügen, und wählen Sie

allable shap-ins;		-	Selected snap-Ins:	
Snap-in	Vendor	^	Console Root	Edit Extensions
ActiveX Control	Microsoft Cor		Certificates (Local Computer)	Janet e
Authorization Manager	Microsoft Cor			vessule
Certificates	Microsoft Cor			
Component Services	Microsoft Cor			(Michaello)
Computer Managem	Microsoft Cor			
Device Manager	Microsoft Cor	T	d S	THEYE DEVO
Disk Management	Microsoft and	L		
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
n)		-		
scription:			and the second	

Computerkonto aus.

ertificates snap-in	>
This snap-in will always manage certificates for:	
O My user account	
O Service account	
Computer account	

- 4. Wählen Sie unter Computer auswählen die Option Lokaler Computer aus.
- 5. Wählen Sie Fertig stellen und dann OK aus.

select computer		>
Select the computer you want this snap-in to	o manage.	
This snap-in will always manage:		
Local computer: (the computer this co	onsole is running on)	
O Another computer:	Browne	

© MOBOTIX AG www.mobotix.com

© MUBOTIX AG www.mobotix.com Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 87/136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Galage CTTX Milestone XProtect® VMS

- Erweitern Sie das Objekt Zertifikate. Klicken Sie mit der rechten Maustaste auf den Ordner
 Persönlich und wählen Sie Alle Aufgaben > Erweiterte Vorgänge > Benutzerdefinierte Anforderung erstellen.
- 7. Klicken Sie im Zertifikatregistrierungs-Assistenten auf Weiter, und wählen Sie Ohne Registrierungsrichtlinie fortfahren aus.



- 8. Klicken Sie auf Weiter.
- 9. Wählen Sie die Vorlage CNG-Schlüssel (keine Vorlage) und das CMC-Anforderungsformat aus und



Certificate Enrollment

Select Certificate Enrollment Policy

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

Configured by you	Add New
Proceed without enrollment policy	
	<u>N</u> ext Cancel
Sins Sins	

klicken Sie auf Weiter.

© MOBOTIX AG www.mobotix.com Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 88/136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Gür Context VMSLeitfaden VMSLe

10. Erweitern Sie, um die **Details** der benutzerdefinierten Anforderung anzuzeigen, und klicken Sie auf - 0

X

Certificate Enrollment

Custom request

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

Template:	(No template) CNG key -
	Suppress default extensions
Request format:	○ <u>P</u> KCS #10
	<u> <u> <u> </u> <u> </u></u></u>
ption is specified in	i the certificate template.

Eigenschaften.

11. Füllen Sie auf der **Registerkarte Allgemein** die Felder **Anzeigename** und **Beschreibung** mit dem Domänennamen, dem Computernamen oder der Organisation aus.

eneral Subject Extensions Private Key Signature	
A friendly name and description will make it easier to identify and use a certific Friendly name:	cate.
TestLabDomain.com	e certificate
Description:	
TestLabDomain.com	Details A ficate:
	operties
	Cance

12. Geben Sie auf der **Registerkarte Betreff** die erforderlichen Parameter für den Antragstellernamen ein. Geben Sie unter **Antragstellername Typ** unter **Allgemeiner Name** den Hostnamen des Computers ein, auf dem das Zertifikat installiert werden soll. 13. Erweitern Sie auf der Registerkarte Erweiterungen das Menü Erweiterte Schlüsselverwendung (Anwendungsrichtlinien). Fügen Sie die Serverauthentifizierung aus der Liste der verfügbaren Optionen

General Subject	Extensions	Private Key	Signature	
The subject of a ci can enter informa can be used in a c Subject of certifica The user or comp	ertificate is tion about ertificate. ate uter that is	the user or c the types of receiving the	omputer to w subject name e certificate	hich the certificate is issued. You and alternative name values that
Subject name:	_	n i		CN-MIT-12A
Common name			Add >	CH-INF ILS
Value			Remove	
Alternative name:		1		
Directory name		-		
Value:			≤bbA	
		c	Remove	

hinzu.

			Certifica	te Propert	ies			
General	Subject	Extensions	Private Key	Signature				
The foll	owing an	e the certific	ate extension	s for this cer	tificate typ	e.		^
Key us	sage						¥	
Extend	ded Key U	sage (applic	ation policie	s)			^	
An app certific certific Availab	dication p ate can b ates issue ble option	oolicy (called e used. Sele ed by this ter is:	l enhanced k ct the applica nplate.	ey usage in l ition policy r	Vindows 20 equired for Selected	000) define valid sign	es how a atures of	
Code S Secure Time S Micros IP secu IP secu IP secu	Email Email Contrust Cont Trust Cont Time Unity end s Unity tunne Unity user	List Signi Stamping system el termina	< R	dd > emove	Server A	uthentico II	Don.	
Mak	the Exte	ended Key U	sage critical					~

- 14. Erweitern Sie auf der Registerkarte Privater Schlüssel das Menü Schlüsseloptionen.
- 15. Legen Sie die Schlüsselgröße auf 2048 fest, und wählen Sie die Option aus, um den privaten Schlüssel exportierbar zu machen. Klicken Sie auf **OK.**

.cremieure i	Properti	ies				>
General S	ubject	Extensions	Private Key	Signature		
Cryptog	raphic S	Service Prov	ider			۷
Key opti	ons					*
Set the ke	ey lengt	th and expo	t options for	the private key.		
Key size:	2048			~	1	
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		
Hash Alo	orithm	sha256			~	
Select Si	gnature	e Format				~
Select Si	gnature	e Format				•
Select Si	gnature	E Format				¥

- 16. Wenn alle Zertifikateigenschaften definiert wurden, klicken Sie **im Zertifikatregistrierungs**-Assistenten auf Weiter.
- 17. Wählen Sie einen Speicherort für die Zertifikatanforderung und ein Format aus. Navigieren Sie zu diesem Speicherort, und geben Sie einen Namen für die REQ-Datei an. Das Standardformat ist die Basis 64.
- 18. Klicken Sie auf **Fertig stellen**.

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:	
C:\Users\Administrator\Desktop\CSR6.1.21	Browse
File format:	
Deres Ed	
Base 64 Binary	
 Base 64 Binary 	
● Base 64 ○ Binary	
 Base 64 Binary 	

Es wird eine .req-Datei generiert, die Sie zum Anfordern eines signierten Zertifikats verwenden müssen.

15.4.2 Laden Sie die .req-Datei hoch, um im Gegenzug ein signiertes Zertifikat zu erhalten.

Sie müssen den gesamten Text der REQ-Datei, einschließlich der Anfangs- und Endzeilen, kopieren und den Text in die interne Zertifizierungsstelle der Active Directory-Zertifikatdienste im Netzwerk einfügen. Weitere Informationen finden Sie unter Installieren von Active Directory-Zertifikatdiensten auf Seite 74.

Sofern in Ihrer Domäne die Active Directory-Zertifikatdienste nicht erst kürzlich installiert wurden oder nur zu diesem Zweck installiert wurde, müssen Sie diese Anforderung nach einem separaten Verfahren senden, das von Ihrem Domänenverwaltungsteam konfiguriert wurde. Bitte bestätigen Sie diesen Vorgang mit ihnen, bevor Sie fortfahren.

1. Navigieren Sie zum Speicherort der REQ-Datei, und öffnen Sie sie im Editor.

Ì

The Edit Exempt View Male		
The Edit Format View Help		-
BEGIN NEW CERTIFICATE REQU		
111FZAYJKOZINVCNAQCCOIIFyICCBC	UCAQMXDZANBgIghkgBZQMEAgEFADCCBB4G	
CSGAQUEBWWC011EEASCBAWWggQ1MG		1
WIBAT FHMEUGCSSGAQQBgJCVFDE4MD	YCAUUMUENSOXNOZXIXVEVNUAWAUOXVUIRF	
JFURUIQXEFKDWIUAXNOCMF0D3IMD0	INQUSEREUWEGUTOIIDIAIDATCCA40WEGJI	
ABEANDCCAOOCAGERAN/JOORDUSOCANOCA	TXAEAMODCCASTMD612K05TUACMA6Epp640	1
BELADCCAOOCBELDAKAD020571021CL	Hypain JSFBE9 JWOYKP+CSN00XTOUCN009g	
//////////////////////////////////////	UR29AYwf8vl NP1Ba0dkfatl Nap6EAYzHdS	
czK1vU7mY576TBwf6L7MutXbNDD52	XzdhG3pggarNdzHvg0RTJvro4TJ0rM6EsJ	
IN2d057ms4Ut i21DekEde3BsENvcvk	0/PH7k8b8Bww050+va3tk7iDbvw0a1VXE9	
nal +7v4nFP1iKnTwM1JvPmsXvw7gx60	CrTw8ntgFCAwFAAaCCAS8wHAYKKwYBBAGC	
W0CAzEOFgwxMC4wLiE0MzkzLiIwR0	YJKwYBBAGCNxUUMTewNeIBBOwMO2x1c3R1	
jFURU10DBpDTFVTVEVSMVRFTVBcOW	RtaW5pc3RyYXRycgwHTU1DLkVYRTBgBgkq	
kiG9w0BC04xUzBRMBMGA1UdJ00MMA	oGCCsGAOUFBwMBMBsGCSsGA00BgjcVCg00	
1AwwCgY1KwYBBQUHAwEwHQYDVR00BB1	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG	
MAwwCgYIKwYBBQUHAwEwHQYDVR0OBB CisGAQQBgjcNAgIxWDBWAgEAHk4ATQE	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0	3
MAWWCgYIKWYBBQUHAWEWHQYDVR0OBB isGAQQBgjcNAgIxWDBWAgEAHk4ATQE NHcAYQByAGUAIABLAGUAeQAgAFMAdAE	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1	
MAWWCgYIKWYBBQUHAWEWHQYDVR00BB isGAQQBgjcNAgIxWDBWAgEAHk4ATQB WHCAYQByAGUAIABLAGUAeQAgAFMAdAB WHIDAQAWDQYJKoZIhvcNAQELBQADggB	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN	
MAwwCgYIKwYBBQUHAwEwHQYDVR00BB LisGAQQBgjcNAgIxWDBWAgEAHk4ATQ NHcAYQByAGUAIABLAGUAeQAgAFMAdAB NHIDAQAwDQYJKoZIhvcNAQELBQADgg NAPtDKNDGskV/dq6rqgpYEKiQfWZeSr	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW	
MAwwCgYIKwYBBQUHAwEwHQYDVR00BB CisGAQQBgjcNAgIxWDBWAgEAHk4ATQ AHcAYQByAGUAIABLAGUAeQAgAFMAdAB AHIDAQAwDQYJKoZIhvcNAQELBQADgg DAPtDKNDGskV/dq6rqgpYEKiQfWZeSr (jUze/+WIiZifGFnkMKYwrzKgx7qIr)	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo	
MAwwCgYIKwYBBQUHAwEwHQYDVR00BB LisGAQQBgjcNAgIxWDBWAgEAHk4ATQ AHcAYQByAGUAIABLAGUAeQAgAFMAdAB AHIDAQAwDQYJKoZIhvcNAQELBQADgg DAPtDKNDGskV/dq6rqgpYEKiQfWZeSr (jUze/+WIiZifGFnkMKYwrzKgx7qIr 13dWazix8dSVOQIRZ3Lr7yXg9iiF49	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo	
MAWWCgYIKWYBBQUHAWEWHQYDVR00BB LisGAQQBgjcNAgIxWDBWAgEAHk4ATQ AHcAYQByAGUAIABLAGUAeQAgAFMAdAB AHIDAQAWDQYJKoZIhvcNAQELBQADgg DAPtDKNDGskV/dq6rqgpYEKiQfWZeSr (jUze/+WIiZifGFnkMKYwrzKgx7qIr 13dWazix8dSVOQIRZ3Lr7yXg9iiF49 EX7yVZFyEAs/6uoApcKXc2KPgBP8aHe	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo	G D L N L J D
MwwCgYIKwYBBQUHAwEwHQYDVR00BB isGAQQBgjcNAgIxWDBWAgEAHk4ATQ HcAYQByAGUAIABLAGUAeQAgAFMAdA HIDAQAwDQYJKoZIhvcNAQELBQADgg APtDKNDGskV/dq6rqgpYEKiQfWZeSr (jUze/+WIiZifGFnkMKYwrzKgx7qIr BdWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo Cut Copy	5)
AwwCgYIKwYBBQUHAwEwHQYDVR00BB isGAQQBgjcNAgIxWDBWAgEAHk4ATQ AHCAYQByAGUAIABLAGUAeQAgAFMAdAA HIDAQAwDQYJKoZIhvcNAQELBQADgg OAPtDKNDGskV/dq6rqgpYEKiQfWZeSr (jUze/+WIiZifGFnkMKYwrzKgx7qIr OdWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHo P4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQOAF0BsTd6/Hpi6c18h5H	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo Cut Copy Paste	i J L J J J J J
AwwCgYIKwYBBQUHAwEwHQYDVR00BB isGAQQBgjcNAgIxWDBWAgEAHk4ATQ HcAYQByAGUAIABLAGUAeQAgAFMAdA HIDAQAwDQYJKoZIhvcNAQELBQADgg APtDKNDGskV/dq6rqgpYEKiQfWZeSr (jUze/+WIiZifGFnkMKYwrzKgx7qIr 13dWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aH p4XCYYiuyw/+iHqyNca2fvIIm8Hpb zCCAYcCAQ0AF0BsTd6/Hpi6c18h5H wYJKoZIhvcNAQkDMQoGCCsGAQUFBw	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyiv0XG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo Cut Copy Paste Delete	
AwwCgYIKwYBBQUHAwEwHQYDVR00BB isGAQQBgjcNAgIxWDBWAgEAHk4ATQ HCAYQByAGUAIABLAGUAeQAgAFMAdA HIDAQAwDQYJKoZIhvcNAQELBQADgg APtDKNDGskV/dq6rqgpYEKiQfWZeSr (jUze/+WIiZifGFnkMKYwrzKgx7qIr 13dWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aH p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQOAF0BsTd6/Hpi6c18h5H wYJKoZIhvcNAQkDMQoGCCsGAQUFBw 0Y6dr8BzietMf5QwmoRNzq8MRGSQiN	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo Cut Copy Paste Delete	
AwwCgYIKwYBBQUHAwEwHQYDVR00BB isGAQQBgjcNAgIxWDBWAgEAHk4ATQ HcAYQByAGUAIABLAGUAeQAgAFMAdA HIDAQAwDQYJKoZIhvcNAQELBQADgg APtDKNDGskV/dq6rqgpYEKiQfWZeSu JUze/+WIIZifGFnkMKYwrzKgx7qIr I3dWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe P4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQOAF0BsTd6/Hpi6c18h5H WYJKoZIhvcNAQkDMQoGCCsGAQUFBw Y6dr8BzietMf5QwmoRNzq8MRGSQiN q73I6NKKLzg7ROhm16Xj7tL4Id2iV	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyiv0XG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo Cut Copy Paste Delete Select All	
AwwCgYIKwYBBQUHAwEwHQYDVR00BB isGAQQBgjcNAgIxWDBWAgEAHk4ATQ HCAYQByAGUAIABLAGUAeQAgAFMAdA HIDAQAwDQYJKoZIhvcNAQELBQADgg APtDKNDGskV/dq6rqgpYEKiQfWZeSr (jUze/+WIiZifGFnkMKYwrzKgx7qIr 3dWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQ0AF0BsTd6/Hpi6c18h5H wYJKoZIhvcNAQkDMQoGCCsGAQUFBw)Y6dr8BzietMf5QwmoRNzq8MRGSQiN q73I6NKKLzg7R0hm16Xj7tL4Id2iV WR7EktvnBLYuBQVPGYb+gwd8EfBh9	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyiv0XG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo Cut Copy Paste Delete Select All Right to left Reading order	5 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
AwwCgYIKwYBBQUHAwEwHQYDVR00BB isGAQQBgjcNAgIxWDBWAgEAHk4ATQ HCAYQByAGUAIABLAGUAeQAgAFMAdA HIDAQAwDQYJKoZIhvcNAQELBQADgg OAPtDKNDGskV/dq6rqgpYEKiQfWZeSr (jUze/+WIiZifGFnkMKYwrzKgx7qIr OdWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aH P4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 zCCAYcCAQOAF0BsTd6/Hpi6c18h5H WYJKoZIhvcNAQkDMQoGCCsGAQUFBw OY6dr8BzietMf5QwmoRNzq8MRGSQiN Q73I6NKKLzg7ROhm16Xj7tL4Id2iV WR7EktvnBLYuBQVPGYb+gwd8EfBh90 +5Z7i0E2HZpsBrS1d1+u89F0Pi+W/	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo Cut Copy Paste Delete Select All Right to left Reading order	
AwwCgYIKwYBBQUHAwEwHQYDVR00BB isGAQQBgjcNAgIxWDBWAgEAHk4ATQ HCAYQByAGUAIABLAGUAeQAgAFMAdA HIDAQAwDQYJKoZIhvcNAQELBQADgg APtDKNDGskV/dq6rqgpYEKiQfWZeSr (jUze/+WIiZifGFnkMKYwrzKgx7qIr 13dWazix8dSVOQIRZ3Lr7yXg9iiF49- X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb zCCAYcCAQOAFOBsTd6/Hpi6c18h5H wYJKoZIhvcNAQkDMQoGCCsGAQUFBw Y6dr8BzietMf5QwmoRNzq8MRGSQiN q73I6NKKLzg7ROhm16Xj7tL4Id2iV WR7EktvnBLYuBQVPGYb+gwd8EfBh9 +5Z7i0E2HZpsBrS1d1+u89F0Pi+W/ Ii7k+ce+EDoHhXkbSD+fHYFbUqaTY	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyiv0XG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo Cut Copy Paste Delete Select All Right to left Reading order Show Unicode control characters	
AwwCgYIKwYBBQUHAwEwHQYDVR00BB isGAQQBgjcNAgIxWDBWAgEAHk4ATQ HCAYQByAGUAIABLAGUAeQAgAFMAdA HIDAQAwDQYJKoZIhvcNAQELBQADgg APtDKNDGskV/dq6rqgpYEKiQfWZeS jUze/+WIiZifGFnkMKYwrzKgx7qIr 3dWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe p4XCYYiuyw/+iHqyNca2fvIIm8Hpb zCCAYcCAQOAF0BsTd6/Hpi6c18h5H wYJKoZIhvcNAQkDMQoGCCsGAQUFBw Y6dr8BzietMf5QwmoRNzq8MRGSQiN q73I6NKKLzg7ROhm16Xj7tL4Id2iV WR7EktvnBLYuBQVPGYb+gwd8EfBh9 +SZ7i0E2HZpsBrS1d1+u89F0Pi+W/ Ii7k+ce+EDoHhXkbSD+fHYFbUqaTV PmPVkUJGJEUMwfo8rb4xb9taP6ycU 8XTFWM01CPMvkW2	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyiv0XG0T0U4MS9VnU50sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo Cut Copy Paste Delete Select All Right to left Reading order Show Unicode control characters Insert Unicode control character	
AWWCgYIKWYBBQUHAWEWHQYDVR00BB LisGAQQBgjcNAgIxWDBWAgEAHk4ATQ AHCAYQByAGUAIABLAGUAeQAgAFMAdA AHIDAQAWDQYJKoZIhvcNAQELBQADgg DAPtDKNDGskV/dq6rqgpYEKiQfWZeS (jUze/+WIiZifGFnkMKYwrzKgx7qIr 13dWazix8dSVOQIRZ3Lr7yXg9iiF49 X7yVZFyEAs/6uoApcKXc2KPgBP8aHe P4XCYYiuyw/+iHqyNca2fvIIm8Hpb 2CCAYcCAQOAFOBsTd6/Hpi6c18h5H WYJKoZIhvcNAQkDMQoGCCsGAQUFBw DY6dr8BzietMf5QwmoRNzq8MRGSQiN -q73I6NKKLzg7ROhm16Xj7tL4Id2iV WR7EktvnBLYuBQVPGYb+gwd8EfBh9 +5Z7i0E2HZpsBrS1d1+u89F0Pi+W/ NI7k+ce+EDoHhXkbSD+fHYFbUqaTY PmPVkUJGJEUMwfo8rb4xb9taP6ycU 8XTFWM0JCPMykW2 FND NEW CERTIFICATE REQUE	YEFOBsTd6/Hpi6c18h5HHq88hWc911MGYG BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0 BvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1 EBAFGoQLCtyiv0XG0T0U4MS9VnUS0sQUnN ndEOzxieJtES/1I5hmVUm51TIVydzE8iyW Undo Cut Copy Paste Delete Select All Right to left Reading order Show Unicode control characters Insert Unicode control character > Open IME	5 5 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7

- 2. Kopieren Sie den gesamten Inhalt der Datei. Dazu gehören auch die gestrichelten Linien, die den Anfang und das Ende der Zertifikatsanforderung markieren.
- 3. Öffnen Sie einen Webbrowser und geben Sie die Adresse der Domänenzertifizierungsstelle ein.

Microsoft Active Directory Certif × +	0	- 🗆 ×
← → C ▲ Not secure 10.0.4.103/certsrv/	\$	Lupdate
Microsoft Active Directory Certificate Services – IP-0A000467-CA		Hom

Welcome

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

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

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

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

- 4. Klicken Sie auf den Link Zertifikat anfordern.
- 5. Klicken Sie auf den Link für die Anforderung eines erweiterten Zertifikats.

0	Micr	osoft A	ctive [Directory Certit	×	4	ł									
4	÷	C	4	Not secure	10.0	0.4.1	103	10	er	ts	rv/	ce	rtro	lus	asj	2
Micr	osof	t Active	e Dire	ctory Certifica	te Sei	rvice	es	-	IF)-O	A	000	46	7-C	A	
Req	uest	t a Ce	ertifi	cate												
Sele	ect th	ie cer	tifica	te type:												
V	Veb I	Brows	ser C	ertificate												
F	-Mai	I Prot	ectio	on Certificat	e											

Or, submit an advanced certificate request.

6. Fügen Sie den Inhalt der .req-Datei in das Formular ein. Wenn es erforderlich ist, eine Zertifikatvorlage auszuwählen, wählen Sie

Webserver aus der Liste Zertifikatvorlage.

Microsoft Active	Directory Certificate S	ervices - CLUSTER2T	EMP-CA	Home
ubmit a Cer	tificate Request o	r Renewal Request	8	
o submit a sa enewal reque	aved request to the st generated by ar	e CA, paste a base-6 n external source (su	4-encoded CMC or PKCS #10 c ch as a Web server) in the Save	ertificate request or PKCS #7 of Request box.
ase-64-encodec ertificate reques CMC or KCS #10 or KCS #7):	IWR7EktvnBLYuBQ r+52710E2H2psBr: nI17k+ce+EDoHhX: 2PmPVkUJGJEUMwf: TSXTFWM0JCPMykW: END NEW CE	/PGYD+gwd8EfBh9K9Qq Sldl+u89F0Pi+W/a8/Y dbSD+fHYFbUqaTYUfgU S8rb4xb9taP6ycUZwie 2 XTIFICATE REQUEST	vd5fMu: V7BhAl 4u5Fg6: LrNWw31	
dditional Attrib	outes:			
Attributes	-	, O		

7. Klicken Sie auf **Senden**.

Auf der Website wird eine Meldung angezeigt, dass das Zertifikat in einigen Tagen ausgestellt wird.

Ihr Domänenverwaltungsteam wird das Zertifikat wahrscheinlich für Sie verteilen und installieren. Wenn Ihnen das Zertifikat jedoch zugestellt wird, können Sie es manuell installieren.

15.5 Manuelles Installieren des Zertifikats

Wenn Ihnen das Zertifikat zugestellt wird, können Sie es manuell installieren.

- 1. Suchen Sie die Zertifikatsdatei auf dem Computer, auf dem der Management-Server oder der Aufzeichnungsserver gehostet wird.
- 2. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie Zertifikat installieren aus.
- 3. Akzeptieren Sie die Sicherheitswarnung, wenn sie angezeigt wird.
- 4. Wählen Sie aus, um das Zertifikat für den aktuellen Benutzer zu installieren, und klicken Sie auf Weiter.

Wählen Sie einen Speicherort aus, navigieren Sie zum Speicher für persönliche Zertifikate, und klicken Sie auf Weiter.

X

Certificate Import Win	zard
------------------------	------

Welcome to the Certificate Import Wizard

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

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

Store Location		
Current User		
O Local Machine		

To continue, click Next.

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

Certificate Store	
Certificate stores are system areas where certificates are kept.	
the certificate. Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store:	e Select Certificate Store Select the certificate store you want to use.
Brow	Se Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates
	Show physical stores

- 5. Beenden Sie den Assistenten zum Installieren von Zertifikaten.
- 6. Wechseln Sie zum Zertifikat-Snap-In der Microsoft Management Console (MMC).
- 7. Navigieren Sie in der Konsole zum persönlichen Speicher, in dem das Zertifikat installiert ist. Klicken Sie mit der rechten Maustaste auf das Zertifikat und wählen Sie Alle Aufgaben > Private Schlüssel verwalten.

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

📸 File Action View Favorites Window	Help		-		
🗢 🔿 🙍 💼 🔏 🐴 🗙 🖬 🔒					
🔁 Console Root	Issued To	1	lssu	ed By	Expiration
 Certificates (Local Computer) Personal 	Cluster1	Open	CLU	ISTERZTEMP-CA	10/26/202
 Certificates Trusted Root Certification Authoritie 		All Tasks	> (Open	
 Enterprise Trust Intermediate Certification Authoritie Trusted Publishers 		Cut Copy	F	Request Certificate with Ne Renew Certificate with New	w Key v Key
Ontrusted Certificates		Delete		Manage Private Keys	
Certificates		Properties	1	Advanced Operations	>
Trusted People		Help	E	Export	

- 8. Stellen Sie sicher, dass das Konto, auf dem die MOBOTIX HUB Management Server-, Recording Server- oder Mobile Server-Software ausgeführt wird, in der Liste der Benutzer mit der Berechtigung zur Verwendung des Zertifikats enthalten ist.
- 9. Stellen Sie sicher, dass für den Benutzer sowohl die Berechtigung Vollzugriff als auch die Leseberechtigung aktiviert sind.

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 99/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden Milestone XProtect® VMS

Standardmäßig verwendet die MOBOTIX HUB-Software das NETWORK SERVICE-Konto. In einer Domänenumgebung werden Dienstkonten häufig zum Installieren und Ausführen von MOBOTIX HUB-Diensten verwendet . Sie müssen dies mit Ihrem Domänenverwaltungsteam besprechen und den Dienstkonten die richtigen Berechtigungen hinzufügen, wenn sie noch nicht ordnungsgemäß konfiguriert

15.5.1 Aktivieren der Serververschlüsselung für Management-Server und Aufzeichnungsserver

Nachdem das Zertifikat mit den richtigen Eigenschaften und Berechtigungen installiert wurde, gehen Sie wie folgt vor.

- 10. Öffnen Sie auf einem Computer, auf dem ein Management-Server oder Aufzeichnungsserver installiert ist, den Server-Konfigurator über:
 - Das Windows-Startmenü oder
 - Der Server-Manager, indem Sie mit der rechten Maustaste auf das Server-Manager-Symbol in der Taskleiste des Computers klicken
- 11. Aktivieren Sie im Server-Konfigurator unter Serverzertifikat die Option Verschlüsselung.
- 12. Klicken Sie auf Zertifikat auswählen, um eine Liste mit eindeutigen Antragstellernamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und auf dem lokalen Computer im Windows-Zertifikatspeicher installiert sind.
- 13. Wählen Sie ein Zertifikat aus, um die Kommunikation zwischen dem Aufzeichnungsserver, dem Verwaltungsserver, dem Failover-Server und dem Datensammlerserver zu verschlüsseln.
- 14. Wählen Sie **Details** aus, um Informationen zum Windows-Zertifikatspeicher für das ausgewählte Zertifikat anzuzeigen.

Dem Benutzer des Aufzeichnungsserver-Dienstes wurde Zugriff auf den privaten Schlüssel gewährt. Es ist erforderlich, dass dieses Zertifikat auf allen Clients vertrauenswürdig ist.

Server Configurator		-		>
Encryption	Encryption			
Registering servers	It is recommended to secure communication with encryptic	n. <u>Learn n</u>	more	
anguage selection	Server certificate Applies to: management server, recording server, failover server, data collector			
	Encryption: On	0		
	Sectors.	¥.	Details	
	Carolicate issued by MS-Organization-P29-Actean (2021), Explores 5/8/2021			
	Streaming media certificate Applies to clients and servers that retrieve data streams from the reco server	ording		
	Encryption: On			
	And the second sec	4	Details	
	Certification instanti by MS-Deganizations 8(19: Access (2002)), Explored S70/2023			
			Apply	

15. Klicken Sie auf Übernehmen.

Wenn Sie Zertifikate anwenden, wird der Aufzeichnungsserver gestoppt und neu gestartet. Das Beenden des Aufzeichnungsserver-Dienstes bedeutet, dass Sie keine Live-Videos aufzeichnen und anzeigen können, während Sie die Grundkonfiguration des Aufzeichnungsservers

16 Installieren von Zertifikaten in einer Arbeitsgruppenumgebung für die Kommunikation mit dem Management-Server oder dem Aufzeichnungsserver

Beim Betrieb in einer Workgroup-Umgebung wird davon ausgegangen, dass keine Infrastruktur für Zertifizierungsstellen vorhanden ist. Zum Verteilen von Zertifikaten ist es erforderlich, eine Zertifizierungsstelleninfrastruktur zu erstellen. Es ist auch erforderlich, die Zertifikatsschlüssel an Client-Workstations zu verteilen. Abgesehen von diesen Anforderungen ähnelt der Prozess des Anforderns und Installierens eines Zertifikats auf einem Server sowohl dem Domänenszenario als auch dem Szenario einer kommerziellen Zertifizierungsstelle.

16.1 Hinzufügen eines Zertifizierungsstellenzertifikats zum Server

Fügen Sie dem Server das Zertifizierungsstellenzertifikat hinzu, indem Sie wie folgt vorgehen.

16. Öffnen Sie auf dem Computer, auf dem der MOBOTIX HUB-Server gehostet wird, die Microsoft Management Console.

đ	Type the name of a progressource, and Windows	jram, folder, docu will open it for you	ment, or Internet J.
<u>O</u> pen:	mmd		~

17. Wählen Sie in der Microsoft Management Console im **Menü Datei** die Option **Snap-In** hinzufügen/entfernen....

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

- 18. Wählen Sie das Snap-In Zertifikate aus, und klicken Sie auf Hinzufügen.
- 19. Klicken Sie auf **OK.**

nap-in	Vendor	~		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor			Certificates (Local Computer)	
Authorization Manager	Microsoft Cor	10			Remove
Certificates	Microsoft Cor	=			
Component Services	Microsoft Cor	1			MoveLip
Computer Managem	Microsoft Cor				
Device Manager	Microsoft Cor		Add		Move Down
Disk Management	Microsoft and		HUU >		
Eolder	Microsoft Cor				
Group Policy Object	Microsoft Cor.				
Internet Informatio	Microsoft Cor				
Internet Informatio	Microsoft Cor				
IP Security Monitor	Microsoft Cor				
IP Security Policy M	Microsoft Cor	~			Advanced
emption:					
and the point		_			

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 103/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfacen für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 103/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfacen für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 103/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfacen für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 103/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfacen für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 103/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfacen für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 103/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfacen für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 103/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfacen für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 103/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfacen für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 103/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfacen für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 103/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfacen für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 103/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfacen für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 103/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfacen für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 103/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfacen für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 103/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfacen für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 103/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfacen für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 103/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfacen für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 103/ 136Leitfaden für Zertifikates_V2-04_DE.docx Milestone XProtect® VMS

20. Erweitern Sie das Objekt Zertifikate. Klicken Sie mit der rechten Maustaste auf den Ordner Persönlich und wählen Sie Alle Aufgaben > Erweiterte Vorgänge > Benutzerdefinierte Anforderung erstellen.



- 21. Klicken Sie im Zertifikatregistrierungs-Assistenten auf Weiter, und wählen Sie Ohne Registrierungsrichtlinie fortfahren aus.
- 22. Klicken Sie auf Weiter.
- 23. Wählen Sie die Vorlage CNG-Schlüssel (keine Vorlage) und das CMC-Anforderungsformat aus und

X

```
Certificate Enrollment
```

Select Certificate Enrollment Policy

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

Configured by you	Add New
Custom Request	
Proceed without enrollment policy	

klicken Sie auf Weiter.

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 104/136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitface für Orf BeOTIX Milestone XProtect® VMS

24. Erweitern Sie, um die Details der benutzerdefinierten Anforderung anzuzeigen, und klicken Sie auf

X

Certificate Enrollment

Custom request

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

Template:	(No template) CNG key
	Suppress default extensions
Request format:	○ <u>P</u> KCS #10
	● <u>C</u> MC
ption is specified in	the certificate template.
	Next Car

Eigenschaften.

sected for this template, or click Details to cu	ustomize the certifica
i) STATUS: Available	Details
e uses and validity period that apply to this t	ype of certificate: Properties
	lected for this template, or click Details to cu STATUS: Available e uses and validity period that apply to this t

25. Füllen Sie auf der **Registerkarte Allgemein** die Felder **Anzeigename** und **Beschreibung** mit dem Domänennamen, dem Computernamen oder der Organisation aus.

Ceneral	C. biret	-	Deixada Vari	Charles in a		
A friend	Subject Ily name	and descript	tion will make	signature e it easier to iden	tify and use a cer	tificate.
TestLa	Domain.	.com				
Descrip	tion:					
TestLa	Domain.	com				

- 26. Geben Sie auf der **Registerkarte Betreff** die erforderlichen Parameter für den Antragstellernamen ein.
- 27. Geben Sie unter Antragstellername **Typ** unter **Allgemeiner Name** den Hostnamen des Computers ein, auf dem das Zertifikat installiert werden soll.

General	Subject	Extensions	Private Key	Signature	
The sub can ent can be Subject The use	er inform used in a of certific or comp	certificate is ation about certificate. cate puter that is	the user or c the types of s receiving the	omputer to w subject name certificate	hich the certificate is issued. You and alternative name values that
Subject	name:		-i		CN-MIT-124
Type				 K H50 	Citetto I - 124
Comn	non name	e		400 -	
Value				Remove	
Alternat	tive name	5	1		
Туре:					
Direct	ory name				
Value:				≤ bbA	
			E	Remove	

28. Erweitern Sie auf der Registerkarte Erweiterungen das Menü Erweiterte Schlüsselverwendung (Anwendungsrichtlinien). Fügen Sie die Serverauthentifizierung aus der Liste der verfügbaren Optionen hinzu.
| | | - | 1 | | | _ | | |
|---|--|--|---|---------------------------------|--------------------------------|---|-----------------------------------|---|
| General | Subject | Extensions | Private Key | Signature | | | | |
| The foll | owing an | e the certific | ate extension | s for this cer | tificate t | ype. | | ^ |
| Key us | age | | | | | | v | |
| Extend | led Key U | sage (applic | ation policies | 5) | | | ~ | |
| An app
certific
certific
Availab | olication p
ate can b
ates issue
ole option | oolicy (called
e used. Selected by this ter
s: | i enhanced k
ct the applica
nplate. | ey usage in V
ition policy n | Vindows
equired f
Select | 2000) def
for valid si
red option | ines how a
ignatures of
is: | |
| Code S
Secure
Time S
Micros
IP secu
IP secu
IP secu | Email
Email
Contrust
Soft Trust
Soft Time
Unity end s
Unity tunn
Unity user | List Signii
Stamping
system
el termina | < R. | dd >
emove | c | authenti
III | cation 2 | |
| Mak | e the Exte | ended Key U | sage critical | | | | | ~ |

- 29. Erweitern Sie auf der Registerkarte Privater Schlüssel das Menü Schlüsseloptionen.
- 30. Legen Sie die Schlüsselgröße auf 2048 fest, und wählen Sie die Option aus, um den privaten Schlüssel exportierbar zu machen. Klicken Sie auf **OK**.

Certificate F	Propert	ies				×
General S	ubject	Extensions	Private Key	Signature		
Cryptog	raphic	Service Prov	ider			۷
Key opti	ons					*
Set the ke	ey lengt	th and expo	rt options for	the private key.		
Key size:	2048			~		
Make	private	key exporta	ble			
Allow	private	key to be an	chived			
Strong	private	e kev protec	tion			
		- 10-7 (P.1-1-1-0)	617-671			
Select H	ash Alo	orithm				*
Select Ha	ish Algo	orithm to be	used for this	request		
Hash Alg	orithm	sha256			~	
Select Si	gnature	e Format				*

- **31.** Wenn alle Zertifikateigenschaften definiert wurden, klicken Sie **in der Zertifikatregistrierung** auf **Weiter**
- 32. Zauberer.
- 33. Wählen Sie einen Speicherort für die Zertifikatanforderung und ein Format aus. Navigieren Sie zu diesem Speicherort, und geben Sie einen Namen für die REQ-Datei an. Das Standardformat ist die Basis 64.
- 34. Klicken Sie auf **Fertig stellen**.

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 to your hard disk or removable media. Enter the location and n click Finish.	process the request later, save the reque ame of your certificate request, and then
File Name:	Presses
CAUSERS (Administrator/Desktop/CSR0/1/2)	browse
File format:	
Base 04 Binary	
Binary	
● Base 04 ○ Binary	
Base 04 Binary	
Base 04 Binary	

Es wird eine .req-Datei generiert, die Sie zum Anfordern eines signierten Zertifikats verwenden müssen.

16.1.1 Laden Sie die .req-Datei hoch, um im Gegenzug ein signiertes Zertifikat zu erhalten.

Sie müssen den gesamten Text der REQ-Datei, einschließlich der Anfangs- und Endzeilen, kopieren und den Text in die interne Zertifizierungsstelle der Active Directory-Zertifikatdienste im Netzwerk einfügen. Weitere Informationen finden Sie unter Installieren von Active Directory-Zertifikatdiensten auf Seite 74.

Sofern in Ihrer Domäne die Active Directory-Zertifikatdienste nicht erst kürzlich installiert wurden oder nur zu diesem Zweck installiert wurde, müssen Sie diese Anforderung nach einem separaten Verfahren senden, das von Ihrem Domänenverwaltungsteam konfiguriert wurde. Bitte bestätigen Sie diesen Vorgang mit ihnen, bevor Sie fortfahren.

1. Navigieren Sie zum Speicherort der REQ-Datei, und öffnen Sie sie im Editor.

Ì

107Test1 - Notepad	- 🗆 X
File Edit Format View Help	
BEGIN NEW CERTIFICATE REQUES	A
MIIF2AYJKoZIhvcNAQcCoIIFyTCCBcUCA	QMxDzANBg1ghkgBZQMEAgEFADCCBB4G
CCsGAQUFBwwCoIIEEASCBAwwggQIMGYwZ	AIBAgYKKwYBBAGCNwoKATFTMFECAQAw
AwIBATFHMEUGCSsGAQQBgjcVFDE4MDYCA	QUMDENsdXN0ZXIxVEVNUAwaQ0xVU1RF
UjFURU1QXEFkbWluaXN0cmF0b3IMB01NQ	y5FWEUwggOYoIID1AIBATCCA40wggJ1
AgEAMBcxFTATBgNVBAMMDENsdXN0ZXIxV	EVNUDCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAKVp0982yi05tcnyp	aTujsFBe9jwOyRp+c5N00xf8OcN0Dyg
dVMVTSU9s9rTMWmUDzP+zLumOmC6gCWIo	5RgiT+dLjOvq+Z6AUWC1H+WVUsaVbJc
ZktV8ut805gi46dkQ4MD71btX6mnjjUB2	94Xwf8yUVP1Be0dkfqjUVnn6EAYzHdS
zczK1yUZmY576IBwf6LZMujXbNDD5ZXzd	hG3pggarNdzHvg0RIJvro4IJ0rM6EsJ
JN2d0SZms4Utj21DekFde3BsENvcvk0/P	HZk8b8Bww050+ya3tk7jDbvw0a1VXE9
bqL+Zy4pEP1jKnTwM1IyPmsXyw7gx6CrT	w8ntqECAwEAAaCCAS8wHAYKKwYBBAGC
Nw0CAzEOFgwxMC4wLjE0MzkzLjIwRQYJK	wYBBAGCNxUUMTgwNgIBBQwMQ2x1c3R1
cjFURU1QDBpDTFVTVEVSMVRFTVBcQWRtal	W5pc3KyYXKvcgwHTU1DLkVYKTBgBgkq
hk1G9W0BCQ4xUZBKMBMGA1UdJQQMMAoGC	LSGAQUFBWMBMBSGCSSGAQQBgJCVCgQ0
MAWWCgYIKWYBBQUHAWEWHQYDVROUBBYEH	
0AP+DKNDGskV/da6ragpYEKi0fW7eSpdE	DzvieltES/1T5bmV/lm51TTV/dzE8iv/l
Xillze/+WTi7ifGEnkMKYwrzKgx7aTr	SZALES CLS/IISHNYOMSITIYYUZLOIYU
m3dWazix8dSV00TR73Lr7vXg9iiF49-	Undo
EX7vVZEvEAs/6uoApcKXc2KPgBP8aHe	Cut
Tp4XCYYiuyw/+iHgyNca2fvIIm8Hpb(Conv
izCCAYcCAQOAFOBsTd6/Hpi6c18h5H	Copy
FwYJKoZIhvcNAQkDMQoGCCsGAQUFBw	Paste
OY6dr8BzietMf5QwmoRNzq8MRGSQiN1	Delete
+q73I6NKKLzg7ROhm16Xj7tL4Id2iVL	Select All
1WR7EktvnBLYuBQVPGYb+gwd8EfBh9l	< Comparison of the second sec
r+5Z7iOE2HZpsBrSldl+u89F0Pi+W/a	Right to left Reading order
nIi7k+ce+EDoHhXkbSD+fHYFbUqaTYL	Show Unicode control characters
2PmPVkUJGJEUMwfo8rb4xb9taP6ycUJ T8XTEWM0JCPMvkW2	Insert Unicode control character > B
END NEW CERTIFICATE REQUES	Open IME
5	Reconversion 😵 👌

- 2. Kopieren Sie den gesamten Inhalt der Datei. Dazu gehören auch die gestrichelten Linien, die den Anfang und das Ende der Zertifikatsanforderung markieren.
- 3. Öffnen Sie einen Webbrowser und geben Sie die Adresse der internen Zertifizierungsstelle ein, die sich unter [ip.ad.dr.ess/certsrv] befinden sollte. Dabei ist ip.ad.dr.ess die IP-Adresse oder der DNS-Name des AD CS-Hostservers des internen Netzwerks.

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 112/136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfacen für Zertifikate - Milestone XP Milestone XProtect® VMS

Microsoft Active Directory Certii × +	0		Ш	^
← → C ▲ Not secure 10.0.4.103/certsrv/	4	-	Updat	te :)
Microsoft Active Directory Certificate Services – 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 Certificate Services</u> <u>Documentation</u>.

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

- 4. Klicken Sie auf den Link Zertifikat anfordern.
- 5. Klicken Sie auf den Link für die Anforderung eines erweiterten Zertifikats.



Web Browser Certificate E-Mail Protection Certificate

Or, submit an advanced certificate request.

6. Wählen Sie aus, ob Sie eine Zertifikatanforderung mithilfe einer Base64-codierten CMC-Datei übermitteln möchten.

- C S Microsoft Active Directory *	- ロ × 命☆愛
Microsoft Active Directory Certificate Services – CLUSTER2TEMP-CA	Home
Advanced Certificate Request	
The 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
using a base-64-encoded PKCS #7 file.	<u> </u>

7. Fügen Sie den Inhalt der .req-Datei in das Formular ein. Wenn es erforderlich ist, eine Zertifikatvorlage auszuwählen, wählen Sie

Webserver aus der Liste Zertifikatvorlage.

Microsoft Active	Directory Certificate	Services – CLUSTER2TEMP-CA	Home
Submit a Cer	tificate Request	or Renewal Request	
To submit a sa renewal reque	aved request to th est generated by a	e CA, paste a base-64-encoded CMC or PKCS #10 an external source (such as a Web server) in the Sav	certificate request or PKCS #7 ved Request box.
Base-64-encodec certificate reques (CMC or PKCS #10 or PKCS #7):	1WR7EktvnBLYuB r+52710E2H2p3B t n117k+ce+EDcHhb 2FmPVkUJGJEUMw TSXTFMM0JCFMyki END NEW CI	DVPGYD+gwd3EfBh9K9Qgvd5fMu: rSldl+u89F0Pi+W/a8/YV7BhAl; XkbSD+fHYFDUgaTYUfgU4u5Pg6: fo8rb4xb9taP6ycU2wieLrNWw3] w2 ERTIFICATE REQUEST	
Additional Attrib	outes:		
Attributes		3	

8. Klicken Sie auf **Senden**.

Auf der Website wird eine Meldung angezeigt, dass das Zertifikat in einigen Tagen ausgestellt wird.

- Interne CA-Server können zum manuellen Ausstellen von Zertifikaten verwendet werden
- Notieren Sie sich das Datum und die Uhrzeit, zu der die Zertifikatsanforderung eingereicht wurde.

0	Micr	osoft A	ctive !	Directory Certif	×	+	0	-		×
÷	7	C	A	Not secure	10.0	0.4.103/certsrv/certfnsh.asp	☆	8	Updat	te :)
Mic	rosof	t Activ	e Dire	ctory Certificat	e Se	rvices - IP-0A000467-CA				Home

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 Manuelles Ausstellen von Zertifikaten

Sie können Zertifikate manuell von dem Computer ausstellen, auf dem die Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS) gehostet werden.

- 1. Öffnen Sie die Microsoft Management Console (MMC).
- 2. Navigieren Sie zum **Snap-In** Zertifizierungsstelle.
- 3. Erweitern Sie das **Objekt Zertifizierungsstelle**.
- Klicken Sie im Ordner "Ausstehende Anforderungen" mit der rechten Maustaste auf die entsprechende Anforderungs-ID, und wählen Sie in der Liste "Alle Aufgaben" die Option "Problem" aus.
- 5. Öffnen Sie einen Browser, und rufen Sie die IIS-Site der internen Zertifizierungsstelle auf, die sich unter [

Console Root	Request ID	Binary Request	Request Status Co	de Actions
V di IP-0A000467-CA	5	All Ta	sks 👌 V	iew Attributes/Extensions
Revoked Certificates Issued Certificates		Refres	ih E	port Binary Data
Pending Requests		Help	ls	sue

ip.ad.dr.ess/certsrv]befindet.

6. Klicken Sie auf den Link Status einer ausstehenden Zertifikatanforderung anzeigen.

0	Micr	osoft A	ctive !	Directory Certif	×	+		0	-		×
4	÷	C	A	Not secure	10.0	0.4.103/certsrv/		☆	8	Updat	re ()
Mici	rosof	Active	e Dire	ctory Certificat	e Se	rvices - IP-0A0004	167-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. Wenn das Zertifikat ausgestellt wurde, ist auf der resultierenden Seite ein Link verfügbar, der das Datum der Zertifikatsanforderung enthält.

0	Micro	osoft A	ctive [Directory Certit	×	+		0	-		×
4	7	C	A	Not secure	10.0	0.4.103/certsrv/certc	kpn.asp	☆	4	Update	
Mici	rosoft	Active	e Dire	ctory Certifica	te Ser	vices — IP-0A00046	7-CA			l	lome
Viev	w the	Stat	tus o	of a Pendin	g Ce	rtificate Reques	t				_
Sele S	ect the	e cer I-Rec	tifica luest	te request <u>:</u> Certificate	you v (<u>6/1/</u>	vant to view: 2021 1:36:18 PM])				

8. Wählen Sie **DER-codiert aus**, und laden Sie die Zertifikatkette herunter.

	uve Directory Certificate Services - GEDSTERZTEMIC-CA	Home
ertificate	Issued	
he certifica	ate you requested was issued to you.	
(DER encoded or Description Base 64 encoded	
	Download certificate chain	

Navigieren Sie zum Ordner Downloads, klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie **im**

Kontextmenü die Option Zertifikat installieren aus.

↓ ↓ ↓ ↓ Downl File Home Sh	oads are View			
← ↑ ↓ >	This PC > Download	ds		
+ Quick accord	Name		Date modified	Туре
Desktop Downloads	x certnew	Open Install Certificate Scan with Windows Defender	10/26/2021 2:22 PM	PKCS #7.Certificates
Pictures	*	Open with		

- 9. Akzeptieren Sie die Sicherheitswarnung, wenn sie angezeigt wird.
- 10. Wählen Sie aus, um das Zertifikat für den aktuellen Benutzer zu installieren, und klicken Sie auf Weiter.

Welcome to the Ce	rtificate Imp	ort Wizard
This wizard helps you copy cer lists from your disk to a certific	tificates, certificate ate store.	trust lists, and certificate revocati
A certificate, which is issued by and contains information used connections. A certificate store	/ a certification auth to protect data or t a is the system area	nority, is a confirmation of your ide to establish secure network where certificates are kept.
Store Location		
Current User Cocal Machine		
To continue, click Next.		

- Wählen Sie einen Geschäftsstandort aus. Wählen Sie Alle Zertifikate im folgenden Speicher speichern aus, und klicken Sie auf die Schaltfläche Durchsuchen, um das Fenster Zertifikatspeicher auswählen zu öffnen. Navigieren Sie zum Speicher für persönliche Zertifikate, und klicken Sie auf OK.
- 12. Klicken Sie auf **Weiter**.

X

Ce	rtificate Store	
	Certificate stores are system areas where certificates are kept.	
_		
	Windows can automatically select a certificate store, or you can specify a locatio the certificate.	n for
	O Automatically select the certificate store based on the type of certificate	Select Certificate Store
	Place all certificates in the following store	
	Certificate store:	Select the certificate store you want to use.
	Browse	
		Trusted Root Certification Authorities
		Enterprise Trust
		Intermediate Certification Authorities
		<u>s</u>
		Show physical stores
		OK Cancel
		OK Cancer

- 13. Beenden Sie den Zertifikatimport-Assistenten.
- 14. Wechseln Sie zum Zertifikat-Snap-In der Microsoft Management Console (MMC).

15. Navigieren Sie in der Konsole zum persönlichen Speicher, in dem das Zertifikat installiert ist. Klicken Sie mit der rechten Maustaste auf das Zertifikat und wählen Sie Alle Aufgaben > Private Schlüssel verwalten.



- 16. Fügen Sie das Konto, auf dem die MOBOTIX HUB Management Server-, Recording Server- oder Mobile Server-Software ausgeführt wird, der Liste der Benutzer hinzu, die zur Verwendung des Zertifikats berechtigt sind.
- 17. Stellen Sie sicher, dass für den Benutzer sowohl die Berechtigung Vollzugriff als auch die Leseberechtigung aktiviert sind.

Standardmäßig verwendet die MOBOTIX HUB-Software das NETWORK SERVICE-Konto.

and at most themes.		
CREATOR OWNER		
NETWORK SERVICE		
SYSTEM		11
Administrators (CLUS) ER11	EIMP VAdministrator	s)
	Add	Remove
ermissions for NETWORK	. 24	11011070
ERVICE	Allow	Deny
Full control		
Read		
Special permissions		
repacial permissions or advance	ed settings.	Advantat
I SUCLIDI UCITIISSIULIS UL DUVOLI.		advanced

© MOBOTIX AG www.mobotix.com

Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 120/136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitfaden für Zertifikate - Milestone XP Milestone XProtect® VMS

16.1.3 Aktivieren der Serververschlüsselung für Management-Server und Aufzeichnungsserver

Nachdem das Zertifikat mit den richtigen Eigenschaften und Berechtigungen installiert wurde, gehen Sie wie folgt vor.

- 1. Öffnen Sie auf einem Computer, auf dem ein Management-Server oder Aufzeichnungsserver installiert ist, den **Server-Konfigurator** über:
 - Das Windows-Startmenü oder
 - Der Server-Manager, indem Sie mit der rechten Maustaste auf das Server-Manager-Symbol in der Taskleiste des Computers klicken
- 2. Aktivieren Sie im Server-Konfigurator unter Serverzertifikat die Option Verschlüsselung.
- 3. Klicken Sie auf Zertifikat auswählen, um eine Liste mit eindeutigen Antragstellernamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und auf dem lokalen Computer im Windows-Zertifikatspeicher installiert sind.
- 4. Wählen Sie ein Zertifikat aus, um die Kommunikation zwischen dem Aufzeichnungsserver, dem Verwaltungsserver, dem Failover-Server und dem Datensammlerserver zu verschlüsseln.
- 5. Wählen Sie **Details** aus, um Informationen zum Windows-Zertifikatspeicher für das ausgewählte Zertifikat anzuzeigen.

Dem Benutzer des Aufzeichnungsserver-Dienstes wurde Zugriff auf den privaten Schlüssel gewährt. Es ist erforderlich, dass dieses Zertifikat auf allen Clients vertrauenswürdig ist.

Server Configurator		-		×
ncryption	Encryption			
egistering servers	It is recommended to secure communication with encryptio	n. <u>Learn m</u>	iore	
anguage selection	Server certificate Applies to: management server, recording server, failover server, data collector			
	Encryption: On			
	The second secon	4	Details	
	Carolicate issued by MS-Organization-P29-Actess (2021), Expires 3/8/2021			
	Streaming media certificate Applies to clients and servers that retrieve data streams from the reco server	rding		
	Encryption: On			
	framewood and the second secon	*	Details	
	Cartillouin Insued by MS-Deganization-929-Accent (2023), Explem 520/2023			

6. Klicken Sie auf Übernehmen.

Wenn Sie Zertifikate anwenden, wird der Aufzeichnungsserver gestoppt und neu gestartet.Das Beenden des Aufzeichnungsserver-Dienstes bedeutet, dass Sie keine Live-Videos aufzeichnen und anzeigen können, während Sie die Grundkonfiguration des Aufzeichnungsservers

16.2 Installieren von Zertifikaten für die Kommunikation mit dem Ereignisserver

Sie können die bidirektionale Verbindung zwischen dem Ereignisserver und den Komponenten, die mit dem Ereignisserver kommunizieren, einschließlich des LPR-Servers, verschlüsseln. Wenn Sie die Verschlüsselung auf dem Ereignisserver aktivieren, gilt sie für Verbindungen von allen Komponenten, die eine Verbindung mit dem Ereignisserver herstellen. Bevor Sie die Verschlüsselung aktivieren, müssen Sie Sicherheitszertifikate auf dem



Ì

Wenn die Event-Server-Kommunikation verschlüsselt ist, gilt dies für die gesamte Kommunikation mit diesem Event-Server. Das heißt, es wird jeweils nur ein Modus unterstützt, entweder http oder https, aber nicht gleichzeitig.

Ereignisserver und allen Verbindungskomponenten installieren.

Die Verschlüsselung gilt für jeden Dienst, der auf dem Ereignisserver gehostet wird, einschließlich Transact, Maps, GisMap und Intercommunication.

Bevor Sie die Verschlüsselung im Event Server aktivieren, müssen alle Clients (Desk Client

und Management Client) und das MOBOTIX HUB LPR-Plug-In mindestens auf Version 2022 R1 aktualisiert werden.

HTTPS wird nur unterstützt, wenn jede Komponente mindestens auf Version 2022 R1 aktualisiert wurde.

Die Erstellung der Zertifikate ist je nach Zertifikatsumgebung die gleiche wie in diesen Abschnitten beschrieben: Installieren von Zertifikaten von Drittanbietern oder kommerziellen Zertifizierungsstellen für die Kommunikation mit dem Management Server oder Recording Server auf Seite 57

Installieren von Zertifikaten in einer Domäne für die Kommunikation mit dem Management Server oder Recording Server auf Seite 86

Installieren von Zertifikaten in einer Arbeitsgruppenumgebung für die Kommunikation mit dem Management-Server oder dem Aufzeichnungsserver auf Seite 104

16.3 Aktivieren der MOBOTIX HUB Event Server-Verschlüsselung

Nachdem das Zertifikat installiert wurde, können Sie es für die gesamte Kommunikation mit dem Ereignisserver aktivieren.



Nachdem alle Clients mindestens auf Version 2022 R1 aktualisiert wurden, können Sie die Verschlüsselung auf dem Ereignisserver aktivieren.

Sie können die bidirektionale Verbindung zwischen dem Ereignisserver und den Komponenten, die mit dem Ereignisserver kommunizieren, einschließlich des LPR-Servers, verschlüsseln.

© MOBOTIX AG www.mobotix.com Mx_GL_MX_HUB_Certificates_V2-04_DE.docx • 04.03.2025 • Seite 122/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitface für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 122/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitface für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 122/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitface für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 122/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitface für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 122/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitface für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 122/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitface für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 122/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitface für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 122/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitface für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 122/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitface für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 122/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitface für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 122/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitface für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 122/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitface für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 122/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitface für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 122/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitface für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 122/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitface für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 122/ 136Leitfaden für Zertifikate - Milestone XProtect® VMSLeitface für Certificates_V2-04_DE.docx • 04.03.2025 • Seite 122/ 136Leitfaden für Zertifikates_V Wenn Sie die Verschlüsselung für eine Servergruppe konfigurieren, muss sie entweder mit einem Zertifikat aktiviert werden, das zum selben Zertifizierungsstellenzertifikat gehört, oder, wenn die Verschlüsselung deaktiviert ist, auf allen Computern in der Servergruppe deaktiviert

16.3.1 Voraussetzungen:

Auf dem Computer, auf dem der Ereignisserver gehostet wird, ist ein Serverauthentifizierungszertifikat vertrauenswürdig Aktivieren Sie zunächst die Verschlüsselung auf dem Ereignisserver. Schritte:

- 7. Öffnen Sie auf einem Computer, auf dem ein Ereignisserver installiert ist, den **Serverkonfigurator** über:
 - Das Windows-Startmenü oder
 - Den Ereignisserver, indem Sie mit der rechten Maustaste auf das Ereignisserversymbol in der Taskleiste des Computers klicken
- 8. Aktivieren Sie im Serverkonfigurator unter Ereignisserver und Add-Ons die Option Verschlüsselung.
- 9. Klicken Sie auf Zertifikat auswählen, um eine Liste mit eindeutigen Antragstellernamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und auf dem lokalen Computer im Windows-Zertifikatspeicher installiert sind.
- 10. Wählen Sie ein Zertifikat aus, um die Kommunikation zwischen dem Ereignisserver und den zugehörigen Add-Ons zu verschlüsseln.
- 11. Wählen Sie **Details** aus, um Informationen zum Windows-Zertifikatspeicher für das ausgewählte Zertifikat anzuzeigen.

Server Configurator	100 mm	~		×
Encryption	Encryption configuration successful			×
Registering servers Language selection	Encryption It is recommended to secure communication Streaming media certificate	with encryption. <u>Learn r</u>	more	
	Applies to clients and servers that retrieve data stream server Encryption: Off	ns from the recording		
	Select certificate	÷.		ा
	No pertificate selected			
	Event server and add-ons Applies to: event server, LPR server			
	Encryption: On	0		
		*	Details	5
	Certificate issued by I Exp	ires 1/6/2022	-	
			Apply	

12. Klicken Sie auf Übernehmen.

Um die Aktivierung der Verschlüsselung abzuschließen, besteht der nächste Schritt darin, die Verschlüsselungseinstellungen auf jedem zugehörigen Add-on-LPR-Server zu aktualisieren .

16.3.2 Importieren von Clientzertifikaten

In diesem Abschnitt wird beschrieben, wie Clientzertifikate auf eine Client-Workstation oder ein Client-Gerät importiert werden.

 Nachdem Sie ein CA-Zertifikat auf den Management-Server oder den Aufzeichnungsserver importiert haben, können Sie von jeder Workstation oder jedem Server im Netzwerk aus auf die folgende Adresse zugreifen:

http://localhost/certsrv/

Die Adresse des Servers, auf dem sich das Zertifikat (privater Schlüssel) befindet, wird jedoch an die Stelle von "localhost" gesetzt. Zum Beispiel:

• Microsoft Active Directory Cetter A	0	-	Ц	×
← → C ▲ Not secure 10.0.4.103/certsrv/		☆	-	ŧ
Microsoft Active Directory Certificate Services – IP-0A000467-CA			H	lome

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>

Dieser Webserver wird auf dem AD CS-Hostserver (Active Directory Certificate Services) gehostet, auf dem sich das Zertifizierungsstellenzertifikat befindet.

- 2. Klicken Sie auf Zertifizierungsstellenzertifikat, Zertifikatkette oder Zertifikatsperrliste herunterladen.
- 3. Wählen Sie im **Feld CA-Zertifikat** das CA-Zertifikat aus, das mit dem MOBOTIX HUB-System verwendet werden soll, und klicken Sie auf

1. Laden Sie die CA-Zertifikatskette herunter.

Microsoft Active Directory CertiF x + →	• - □ ×
← → C ▲ Not secure 10.0.4.103/certsrv/certcarc.asp	☆ ≛ :
Microsoft Active Directory Certificate Services - IP-0A000467-CA	Home
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, insta	II this CA certificate.
To download a CA certificate, certificate chain, or CRL, select t	he certificate and encoding method.
CA certificate:	
Current [IP-0A000467-CA] ~	
Encoding method:	
DER	
O Base 64	
Install CA certificate	
Download CA certificate	
Download CA certificate chain	
Download latest base CRL	

- 4. Wählen Sie **DER-codiert aus**, und laden Sie die Zertifikatkette herunter.
- 5. Navigieren Sie zum Ordner Downloads, klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie **im** Kontextmenü die Option Zertifikat installieren aus.

← · · · · · · · · · · · · · · · · · · ·	> Downloads		v 0	Search D	ownloads	p
Desktop ^ Nar	me	~	Date mo	dified	Туре	Size
🗄 Documents	certnew.p7b		5/11/202	1 1:31 PM	PKCS #7 Certif	ficates
Music Pictures Videos Local Disk (C:) Network 1 item 1 item selected 832 byte	25 25	Install Certificate Edit with Notepad++ Share Open with Give access to Restore previous versions Send to	>			
		Cut Copy Create shortcut Delete Rename				
	1	Properties				

- 6. Dadurch wird der Zertifikatimport-Assistent gestartet.
- 7. Klicken Sie auf Weiter.

- " Certificate	Import Wizard	
-----------------	---------------	--

This wizard helps you cop lists from your disk to a c	ertificate store.	te trust lists, and certi	ficate revocation
A certificate, which is issu and contains information connections. A certificate	ued by a certification au used to protect data o store is the system ar	uthority, is a confirmat r to establish secure n ea where certificates a	ion of your identit etwork are kept,
To constitute shale black			
TO CONTINUE, CICK NEXT.			

8. Wählen Sie einen Geschäftsstandort aus. Wählen Sie Alle Zertifikate im folgenden Speicher speichern aus, und klicken Sie auf die Schaltfläche Durchsuchen

, um das Fenster Zertifikatspeicher auswählen zu öffnen.

9. Navigieren Sie zum Zertifikatspeicher für Stammzertifizierungsstellen von Drittanbietern, und

Certificate Store Certificate stores are system areas where o			
Certificate stores are system areas where o	Certificate Store		
	eruficates are kept.		
Windows can automatically select a certification the certificate.	te store, or you can specify a location for		
O Automatically select the certificate sto	ore based on the type of certificate		
Place all certificates in the following st	tore		
Certificate store:			
	Browse		
-			

klicken Sie auf **OK**. Klicken Sie auf **Weiter**.

alast the serificate stars usu ment to use		
elect the certificate store you want to use.		· · · · · · · · · · · · · · · · · · ·
Intermediate Certification Authorities	^	tificates are kept,
	*	store, or you can specify a location for
Show physical stores	-	e based on the type of certificate
OK. Cancel	1	
		Browse

10. Beenden Sie den Zertifikatimport-Assistenten.

Jetzt hat die Workstation die Zertifikatskomponenten importiert, die für die sichere Kommunikation mit dem Management-Server oder dem Aufzeichnungsserver erforderlich sind.

Next

Cancel

16.4 Anzeigen des Verschlüsselungsstatus für Clients

So überprüfen Sie, ob Ihr Aufzeichnungsserver Verbindungen verschlüsselt:

- 1. Öffnen Sie den Management Client.
- 2. Wählen Sie im **Bereich Sitenavigation** die Option **Server > Aufzeichnungsserver aus**. Daraufhin wird eine Liste der Aufzeichnungsserver geöffnet.
- 3. Wählen Sie im **Bereich Übersicht** den entsprechenden Aufnahmeserver aus und wechseln Sie zur **Registerkarte Info**.

Wenn die Verschlüsselung für Clients und Server aktiviert ist, die Datenströme vom Aufzeichnungsserver abrufen, wird ein Vorhängeschloss-Symbol vor der Adresse des lokalen Webservers und der optionalen Webserveradresse angezeigt.

Recording server information	
Name:	
Recording server 1	
Description:	
Covers sector 1	1
	196
Host name:	_
(c	
Local web server address:	
https://	
Web server address:	
https://www.recordingserver1.dk:89/	
Time zone:	
(UTC+01:00) Brussels, Copenhagen, Madrid, Paris	

16.4.1 Anzeigen des Verschlüsselungsstatus auf einem Failover-Aufzeichnungsserver

Gehen Sie folgendermaßen vor, um zu überprüfen, ob Ihr Failover-Aufzeichnungsserver Verschlüsselung verwendet:

- 1. Wählen Sie im **Bereich Websitenavigation** die Option **Server > Failoverserver aus**. Daraufhin wird eine Liste der Failover-Aufzeichnungsserver geöffnet.
- 2. Wählen Sie im **Bereich Übersicht** den entsprechenden Aufnahmeserver aus und wechseln Sie zur **Registerkarte Info**.

Wenn die Verschlüsselung für Clients und Server aktiviert ist, die Datenströme vom Aufzeichnungsserver abrufen, wird ein Vorhängeschloss-Symbol vor der Adresse des lokalen Webservers und der optionalen Webserveradresse angezeigt.

perfies	
Failover server information	
Name	
Failover recording server 1	-
Description:	
Failover for Recording server 1	p.
Host name:	5
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	
Info 📰 Network 💠 Multicast	

Anlage A | Erstellen eines Skripts für ein CA-

Führen Sie dieses Skript einmal aus, um ein Zertifikat zu erstellen, das SSL-Zertifikate mehrerer Server signieren kann

Privates Zertifikat zum Signieren anderer Zertifikate (im Zertifikatsspeicher)

Fingerabdruck des privaten Zertifikats, das zum Signieren anderer Zertifikate verwendet wird

Set-Content -Path "\$PSScriptRoot\ca_thumbprint.txt" -Wert \$ca_Zertifikat. Fingerabdruck

Öffentliches CA-Zertifikat, dem vertraut werden soll (Stammzertifizierungsstellen von Drittanbietern)

export-certificate -cert "cert:\CurrentUser\My\\$(\$ca_certificate. Fingerabdruck)" -FilePath "\$PSScriptRoot\root-authority-public.cer"

Anlage B | Erstellen eines Skripts für das Server-SSL-

Führen Sie dieses Skript einmal für jeden Server aus, für den ein SSL-Zertifikat benötigt wird.
Das Zertifikat sollte auf dem einzelnen Computer ausgeführt werden, auf dem sich das CA-Zertifikat befindet. # Das erstellte Server-SSL-Zertifikat sollte dann auf den Server verschoben und in den dortigen Zertifikatsspeicher # importiert werden.
Erlauben Sie nach dem Importieren des Zertifikats den Zugriff auf den privaten Schlüssel des Zertifikats für # den/die Dienstbenutzer der Dienste, die das Zertifikat verwenden müssen.

#CA-Zertifikat aus dem Speicher laden (Fingerabdruck muss in ca_thumbprint.txt sein)
\$ca_thumbprint = Get-Content -Pfad "\$PSScriptRoot\ca_thumbprint.txt"
\$ca_zertifikat = (Get-ChildItem -Pfad cert:\CurrentUser\Mein\\$ca_Fingerabdruck)

Benutzer zur Eingabe von DNS-Namen auffordern, die in das Zertifikat aufgenommen werden sollen \$dnsNames = Read-Host 'DNS-Namen für Server-SSL-Zertifikat (durch Leerzeichen getrennt - 1. Eintrag ist auch Gegenstand des Zertifikats)' \$dnsNamesArray = @(\$dnsNames -Split '' | foreach { \$_. Trimmen() } | wobei { \$_.})

if (\$dnsNamesArray.Länge -Gl 0) { Write-Host -ForegroundColor Red 'Mindestens ein DNS-Name sollte angegeben werden' exit

\$subjectName = \$dnsNamesArray[0]

\$dnsEntries = (\$dnsNamesArray | foreach { "DNS=\$_" }) -Join '&'

Erlauben Sie dem Benutzer optional, eine Liste von IP-Adressen einzugeben, die in das Zertifikat eingefügt werden sollen \$ipAddresses = Read-Host 'IP-Adressen für Server-SSL-Zertifikat (gelöscht durch Leerzeichen)' \$ipAddressesArray = @(\$ipAddresses -Teilen ' ' | foreach { \$_. Trimmen() } | where { \$_.}) if (\$ipAddressesArray.Länge -gt 0) { \$ipEntries = (\$ipAddressesArray | foreach { "IPAddress=\$_" }) -Join '&' \$dnsEntries = "\$dnsEntries&\$ipEntries" }

Erstellen Sie eine Zeichenfolge für die endgültigen DNS-Einträge (z. B. "2.5.29.17={text}DNS=myhost&DNS=myhost.domain.com&IPAddress=10.0.0.103") \$dnsEntries = "2.5.29.17={Text}\$dnsEntries"

Der einzige erforderliche Zweck des Zertifikats ist die "Serverauthentifizierung" \$serverAuthentication = '2.5.29.37={kritisch}{Text}1.3.6.1.5.5.7.3.1'

Erstellen Sie nun das SSL-Zertifikat des Servers \$certificate = New-SelfSignedCertificate -CertStoreLocation cert:\CurrentUser\My -Subject \$subjectName -Signer \$ca_certificate ' -FriendlyName 'VMS SSL-Zertifikat' -TextExtension @(\$dnsEntries, \$serverAuthentication)

#Zertifikat auf Festplatte exportieren - mit Passwort schützen
\$password = Read-Host -AsSecureString "Passwort für das SSL-Zertifikat des Servers"
export-pfxCertificate -cert "cert:\CurrentUser\My\\$(\$certificate. Fingerabdruck)" -FilePath "\$PSScriptRoot\\$subjectName.pfx" -Kennwort-\$password

Löschen Sie das SSL-Zertifikat des Servers aus dem lokalen Zertifikatsspeicher \$certificate | Artikel entfernen

Anlage C | Erstellen eines Skripts für ein CA-

Führen Sie dieses Skript einmal für jeden Management-Server aus, für den ein Zertifikat benötigt wird.
Das Zertifikat sollte auf dem einzelnen Computer ausgeführt werden, auf dem sich das CA-Zertifikat befindet. # Das erstellte Zertifikat sollte dann auf die Management-Server verschoben werden und
in den dortigen Zertifikatsspeicher importiert.

CA-Zertifikat aus dem Speicher laden (Fingerabdruck muss in ca_thumbprint.txt sein)
\$ca_thumbprint = Get-Content -Pfad "\$PSScriptRoot\ca_thumbprint.txt"
\$ca_Zertifikat = (Get-ChildItem -Pfad cert:\CurrentUser\Mein\\$ca_Fingerabdruck)

Benutzer zur Eingabe von DNS-Namen auffordern, die in das Zertifikat aufgenommen werden sollen \$dnsNames = Read-Host 'DNS-Namen für Management-Server-Zertifikat (komma getrennt - 1. Eintrag ist auch Gegenstand des Zertifikats)' \$dnsNamesArray = @(\$dnsNames-Split',' | foreach { \$_. Trimmen() }| wobei { \$_.})

wenn (\$dnsNamesArray. Länge -eq 0) { Write-Host -ForegroundColor Red 'Mindestens ein DNS-Name sollte angegeben werden' exit

}

\$dnsEntries = (\$dnsNamesArray | foreach { "DNS=\$_" }) -Join '&'

Erlauben Sie dem Benutzer optional, eine Liste von IP-Adressen einzugeben, die in das Zertifikat eingefügt werden sollen \$ipAddresses = Read-Host 'IP-Adressen für das Management-Server-Zertifikat (durch Kommas getrennt)' \$ipAddressesArray = @(\$ipAddresses -Teilen ',' | foreach { \$_. Trimmen() } | wobei { \$__}) if (\$ipAddressesArray. Länge -gt 0) { \$ipEntries = (\$ipAddressesArray | foreach { "IPAddress=\$_" }) -Join '&' \$dnsEntries = "\$dnsEntries&\$ipEntries" } \$subjectName = \$ipAddressesArray[0]

Erstellen Sie eine Zeichenfolge für die endgültigen DNS-Einträge (z. B. "2.5.29.17={text}DNS=myhost&DNS=myhost.domain.com&IPAddress=10.0.0.103") \$dnsEntries = "2.5.29.17={Text}\$dnsEntries"

Der einzige erforderliche Zweck des Zertifikats ist die "Serverauthentifizierung" \$serverAuthentication = '2.5.29.37={kritisch}{Text}1.3.6.1.5.5.7.3.1'

Erstellen Sie nun das Zertifikat des Management-Servers

#Zertifikat auf Festplatte exportieren - mit Passwort schützen

\$password = Read-Host -AsSecureString "Kennwort für das Zertifikat des Management-Servers"
export-pfxCertificate -cert "cert:\CurrentUser\My\\$(\$certificate. Fingerabdruck)" -FilePath "\$PSScriptRoot\\$subjectName.pfx" -Password \$password

Löschen Sie das Zertifikat des Management-Servers aus dem lokalen Zertifikatsspeicher \$certificate | Artikel entfernen



EN_03/25-Ärmel

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

MOBOTIX ist eine Marke der MOBOTIX AG, die in der Europäischen Union, den USA und in anderen Ländern eingetragen ist. Änderungen ohne vorherige Ankündigung vorbehalten. MOBOTIX übernimmt keine Haftung für technische oder redaktionelle Fehler oder Auslassungen. Alle Rechte vorbehalten. © MOBOTIX AG 2025