

# MOBOTIX HUB – Guida ai certificati

V2.04

## Sommario

|        | 1  | COPYRIGHT, MARCHI E DISCLAIMER  |
|--------|--|---|
|        | 2  | INFORMAZIONI SU QUESTA GUIDA  |
|        | 3  | QUANDO È NECESSARIO INSTALLARE I CERTIFICATI?   |
|        | 4  | INTRODUZIONE AI CERTIFICATI   |
|        | 4.1  | CERTIFICATO DISTRIBUZIONE   |
|        | 5  | PANORAMICA DEGLI SCENARI E DELLE PROCEDURE UTILIZZATE CON CERTIFICATI   |
|        | 5.1<br>5.2<br>5.3<br>5.4<br>5.5<br>5.6<br>5.7<br>6<br>7<br>7.1<br>7.2<br>7.3 | MOBOTIX HUB MOBILE SERVER       9         SERVER DI GESTIONE E SERVER DI REGISTRAZIONE MOBOTIX HUB       9         CERTIFICATO CA DI TERZE PARTI O COMMERCIALE       10         DOMINIO.       10         GRUPPO DI LAVORO       10         SERVER DI EVENTI MOBOTIX HUB       10         CLIENTE.       10         QUALI CLIENT HANNO BISOGNO DI CERTIFICATI?       12         SERVER CONFIGURATOR (SPIEGAZIONE)       14         CERTIFICATO SERVER       15         SERVER DI EVENTI E COMPONENTI AGGIUNTIVI.       16         CERTIFICATO MULTIMEDIALE DI FLUSSO       16 |
|        | 8  | SCRIPT DI POWERSHELL  |
|        | 9  | CREAZIONE E DISTRIBUZIONE MANUALE DEI CERTIFICATI   |
|        | 9.1<br>9.2   | IMPORTANTE DA SAPERE:   |
|        | 10   | INSTALLARE I CERTIFICATI NEI CLIENT   |
| © MOBC | <b>11</b><br>DTIX A  | CREARE UN CERTIFICATO SSL   |
| Mx_GL_ | MX_H<br>XPro   | UB_Certificates_V2-04_IT.docx • 04.03.2025 • Pagina 2/ 129Guida ai certificati - VMS Milestone XProtect®Guida ai certi 🕅 - 😡 Mast 😡 📗 🗙 tect®   |

### MOBOTIX HUB – Guida ai certificati - Error! Use the Home tab to apply

| 12         | IMPORTA CERTIFICATO SSL  |
|------------|--|
| 12.1       | GESTISCI LE CHIAVI PRIVATE   |
| 13         | CREARE UN CERTIFICATO SSL PER IL SERVER DI GESTIONE DEL FAILOVER   |
| 14         | INSTALLARE CERTIFICATI PER LA COMUNICAZIONE CON IL MOBILE SERVER   |
| 14.1       | Aggiungere una CA certificato al server  |
| 14.2       | CARICA IL FILE .REQ PER RICEVERE IN CAMBIO UN CERTIFICATO FIRMATO  |
| 14.3       | ABILITARE LA CRITTOGRAFIA SUL SERVER MOBILE  |
| 15<br>SERV | INSTALLARE CERTIFICATI CA DI TERZE PARTI O COMMERCIALI PER LA COMUNICAZIONE CON IL<br>VER DI GESTIONE O IL SERVER DI REGISTRAZIONE   |
| 15.1       | Aggiungere un certificato CA al server   |
| 15.2       | CARICA IL FILE .REQ PER RICEVERE IN CAMBIO UN CERTIFICATO FIRMATO  |
| 15.3       | ABILITARE LA CRITTOGRAFIA DA E VERSO IL SERVER DI GESTIONE   |
| 15.3.      | 1 Prerequisiti:  |
| 15.3.      | 2 Per Installare Servizi certificati Active Directory:   |
| 15.4       | INSTALLARE I CERTIFICATI IN UN DOMINIO PER LA COMUNICAZIONE CON IL SERVER DI GESTIONE O IL SERVER DI                                 |
| REGIS      | TRAZIONE   |
| 15.4.      | AGGIUNGERE UN CERTIFICATO CA AL SERVER   |
| 15.4.      | 2 CARICA IL FILE .REQ PER RICEVERE IN CAMBIO UN CERTIFICATO FIRMATO  |
| 15.5       | INSTALLARE IL CERTIFICATO MANUALMENTE  |
| 15.5.      | ABILITARE LA CRITTOGRAFIA DEL SERVER PER I SERVER DI GESTIONE E I SERVER DI REGISTRAZIONE  |
| 16<br>CON  | INSTALLARE CERTIFICATI IN UN AMBIENTE DI GRUPPO DI LAVORO PER LA COMUNICAZIONE<br>IL SERVER DI GESTIONE O IL SERVER DI REGISTRAZIONE |
| 16.1       | Aggiungere un certificato CA al server   |
| 16.1.      | CARICA IL FILE .REQ PER RICEVERE IN CAMBIO UN CERTIFICATO FIRMATO  |
| 16.1.      | 2 Emettere i certificati manualmente   |
| 16.1.      | ABILITARE LA CRITTOGRAFIA DEL SERVER PER I SERVER DI GESTIONE E I SERVER DI REGISTRAZIONE  |
| 16.2       | INSTALLARE I CERTIFICATI PER LA COMUNICAZIONE CON L'EVENTO SERVER  |
| 16.3       | ABILITARE CRITTOGRAFIA DEL SERVER DI EVENTI MOBOTIX HUB116   |
| 16.3.      | 1 Prerequisiti:  |
| 16.3.      | 2 IMPORTARE I CERTIFICATI CLIENT   |
| 1.         | Scarica la catena di certificati CA  |
| 16.4       | VISUALIZZARE LO STATO DELLA CRITTOGRAFIA AI CLIENT122  |
| 16.4.      | 1 VISUALIZZARE LO STATO DELLA CRITTOGRAFIA IN UN SERVER DI REGISTRAZIONE DI FAILOVER   |

### 1 Copyright, marchi e disclaimer

Diritto d'autore © 2025 MOBOTIX AG

### Marchi

MOBOTIX HUB è un marchio registrato di MOBOTIX AG.

Microsoft e Windows sono marchi registrati di Microsoft Corporation. App Store è un marchio di servizio di Apple Inc. Android è un marchio di Google Inc.

Tutti gli altri marchi citati in questo documento sono marchi dei rispettivi proprietari.

### Disconoscimento

Il presente testo è destinato esclusivamente a scopi informativi generali e nella sua preparazione è stata prestata la dovuta cura.

Qualsiasi rischio derivante dall'uso di queste informazioni è a carico del destinatario e nulla di quanto contenuto nel presente documento deve essere interpretato come costituente alcun tipo di garanzia.

MOBOTIX AG si riserva il diritto di apportare modifiche senza preavviso.

Tutti i nomi di persone e organizzazioni usati negli esempi di questo testo sono fittizi. Qualsiasi somiglianza con un'organizzazione o una persona reale, viva o morta, è puramente casuale e non intenzionale.

Questo prodotto può utilizzare software di terze parti per i quali possono essere applicati termini e condizioni specifici. In questo caso, è possibile trovare ulteriori informazioni nel *file* 

*3rd\_party\_software\_terms\_and\_conditions.txt* si trova nella cartella di installazione del sistema MOBOTIX HUB.

### 2 Informazioni su questa guida

In questa guida viene fornita un'introduzione alla crittografia e ai certificati, insieme alle procedure dettagliate per l'installazione dei certificati in un ambiente Windows Workgroup.

MOBOTIX consiglia di creare un'infrastruttura a chiave pubblica (PKI) per la creazione e la distribuzione dei certificati. Un'infrastruttura a chiave pubblica è un insieme di ruoli, criteri, hardware, software e procedure necessari per creare, gestire, distribuire, utilizzare, archiviare e revocare i certificati digitali e gestire la crittografia a chiave pubblica. In un dominio Windows, è consigliabile stabilire un'infrastruttura PKI usando Servizi certificati Active Directory (AD CS).

Se non si è in grado di creare un'infrastruttura PKI, a causa della presenza di domini diversi senza attendibilità tra di essi o a causa del mancato utilizzo di domini, è possibile creare e distribuire manualmente i certificati.

ATTENZIONE: la creazione e la distribuzione manuale dei certificati non è consigliata come metodo sicuro per la distribuzione dei certificati. Se si sceglie la distribuzione manuale, si è responsabili di mantenere sempre al sicuro i certificati privati. Quando si mantengono sicuri i certificati privati, i computer client che considerano attendibili i certificati sono meno vulnerabili agli attacchi.

### 3 Quando è necessario installare i certificati?

Innanzitutto, decidi se il tuo sistema necessita di comunicazioni crittografate.

Non utilizzare certificati con crittografia del server di registrazione se si utilizzano una o più integrazioni che non supportano la comunicazione HTTPS. Si tratta, ad esempio, di integrazioni MIP SDK di terze parti che non supportano HTTPS.

A meno che l'installazione non venga eseguita in una rete fisicamente isolata, è consigliabile proteggere la comunicazione utilizzando i certificati.

In questo documento viene descritto quando utilizzare i certificati:

- Se il sistema MOBOTIX HUB VMS è configurato in un ambiente Windows Workgroup
- Prima di installare o eseguire l'aggiornamento a MOBOTIX HUB VMS 2019 R1 o versioni successive, se si desidera abilitare la crittografia durante l'installazione.
- Prima di abilitare la crittografia, se è stato installato MOBOTIX HUB VMS 2019 R1 o versioni successive senza crittografia
- Quando si rinnovano o si sostituiscono i certificati a causa della scadenza

### 4 Introduzione ai certificati

HTTPS (Hypertext Transfer Protocol Secure) è un'estensione dell'Hypertext Transfer Protocol (HTTP) per la comunicazione sicura su una rete di computer. In HTTPS, il protocollo di comunicazione viene crittografato utilizzando Transport Layer Security (TLS) o il suo predecessore, Secure Sockets Layer (SSL).

In MOBOTIX HUB VMS, la comunicazione sicura si ottiene utilizzando TLS/SSL con crittografia asimmetrica (RSA). TLS/SSL utilizza una coppia di chiavi, una privata e una pubblica, per autenticare, proteggere e gestire le connessioni sicure.

Un'autorità di certificazione (CA) è chiunque sia in grado di emettere certificati radice. Può trattarsi di un servizio Internet che emette certificati radice o di chiunque generi e distribuisca manualmente un certificato. Una CA può emettere certificati per i servizi web, ovvero per qualsiasi software che utilizza la comunicazione https. Questo certificato contiene due chiavi, una chiave privata e una chiave pubblica. La chiave pubblica viene installata sui client di un servizio Web (client del servizio) installando un certificato pubblico. La chiave privata viene utilizzata per firmare i certificati del server che devono essere installati nel server. Ogni volta che un client del servizio chiama il servizio Web, il servizio Web invia il certificato del server, inclusa la chiave pubblica, al client. Il client del servizio può convalidare il certificato del server utilizzando il certificato CA pubblico già installato. Il client e il server possono ora utilizzare i certificati del server pubblico e privato per scambiarsi una chiave segreta e stabilire così una connessione TLS/SSL sicura.

Per i certificati distribuiti manualmente, i certificati devono essere installati prima che il client possa eseguire tale verifica.

Per ulteriori informazioni su TLS, vedere Transport Layer Security.

In MOBOTIX HUB VMS, le seguenti posizioni sono quelle in cui è possibile abilitare la crittografia TLS/SSL:

• Nella comunicazione tra il server di gestione e i server di registrazione, i server di eventi e i server mobili

• Sul server di registrazione nella comunicazione con client, server e integrazioni che recuperano flussi di dati dal server di registrazione.

Nella comunicazione tra client e server mobile In questa guida vengono definiti client:

- MOBOTIX HUB Desk Client
- Client di gestione
- Server di gestione (per Monitor di sistema e per immagini e clip video AVI nelle notifiche e-mail)
- MOBOTIX HUB Mobile Server
- Server di eventi MOBOTIX HUB
- MOBOTIX HUB LPR
- Ponte di rete aperto MOBOTIX
- MOBOTIX HUB DLNA Server
- · Siti che recuperano flussi di dati dal server di registrazione tramite Milestone Interconnect
- Integrazioni MIP SDK di terze parti che supportano HTTPS

Per le soluzioni create con MIP SDK 2018 R3 o versioni precedenti che accedono ai server di registrazione:- Se le integrazioni vengono effettuate utilizzando le librerie MIP SDK, devono essere ricostruite con MIP SDK 2019 R1-Se le integrazioni comunicano direttamente con le API del server di registrazione senza utilizzare le librerie MIP SDK, gli integratori devono aggiungere autonomamente il supporto HTTPS- In caso di dubbio, Chiedi al tuo fornitore chi ha fornito l'integrazione

#### Distribuzione dei certificati 4.1

L'immagine illustra il concetto di base di come i certificati vengono firmati, considerati attendibili e distribuiti nelle macchine virtuali MOBOTIX HUB per proteggere la comunicazione con il server di gestione.



❶ Un certificato CA funge da terza parte attendibile, considerata attendibile sia dal soggetto/proprietario (server di gestione) che dalla parte che verifica il certificato (server di registrazione)

🥝 Il certificato CA deve essere considerato attendibile su tutti i server di registrazione. In questo modo i server di registrazione possono verificare la validità dei certificati emessi dalla CA

Il certificato CA viene utilizzato per stabilire una connessione sicura tra il server di gestione e i server di registrazione

🔮 Il certificato CA deve essere installato nel computer in cui è in esecuzione il server di gestione Requisiti per il certificato del server di gestione privato:

- Rilasciato al server di gestione in modo che il nome host del server di gestione sia incluso nel certificato, come soggetto (proprietario) o nell'elenco dei nomi DNS a cui viene rilasciato il certificato
- Attendibile nel server di gestione stesso, in quanto considera attendibile il certificato CA utilizzato per emettere il certificato del server di gestione
- Attendibile su tutti i server di registrazione connessi al server di gestione, in quanto considera attendibile il certificato CA utilizzato per emettere il certificato del server di gestione

I certificati hanno una data di scadenza. Non riceverai un avviso quando un certificato sta per scadere. Se un certificato scade, i client non considereranno più attendibile il server con il certificato scaduto e quindi non potranno comunicare con esso. Per rinnovare i certificati, segui i passaggi di questa guida come hai fatto quando hai creato i certificati.

#### © MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 8/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati - VMS Milestone XProtect® Guida ai certificati - VMS Milestone XProtect<sup>®</sup>

### 5 Panoramica degli scenari e delle procedure utilizzate con i certificati

Le procedure per configurare la comunicazione sicura in un ambiente MOBOTIX HUB VMS sono diverse, a seconda del tipo di server che richiede una comunicazione sicura.

Le procedure sono diverse anche in una rete WORKGROUP rispetto a una rete DOMAIN.

I tipi di applicazioni client MOBOTIX HUB VMS utilizzate nel sistema determinano anche alcune delle procedure necessarie per comunicazioni sicure.

L'utilizzo dei certificati per la comunicazione con il server può in genere essere ignorato in

un'installazione di un singolo server , ad eccezione del fatto che funge da protezione aggiuntiva durante la comunicazione con il server di gestione.

Questo elenco mostra i diversi scenari:

Ì

### 5.1 MOBOTIX HUB Mobile Server

In MOBOTIX HUB VMS, la crittografia è abilitata o disabilitata per ogni server mobile. È possibile abilitare o disabilitare la crittografia durante l'installazione del prodotto MOBOTIX HUB VMS o utilizzando il Server Configurator. Quando si abilita la crittografia su un server mobile, si utilizza la comunicazione crittografata con tutti i client, i servizi e le integrazioni che recuperano i flussi di dati.

Il server mobile si connette al client mobile MOBOTIX HUB e al client web MOBOTIX HUB. I browser, i sistemi operativi e i dispositivi mobili che ospitano questi client gestiscono un elenco di certificati radice CA attendibili. Solo l'autorità conosce la sua chiave privata, ma tutti conoscono la sua chiave pubblica, che è simile a qualsiasi certificato particolare.

Questi client, quindi, hanno già installato le chiavi del certificato e funzionano con la maggior parte dei certificati di terze parti disponibili per l'installazione sul server mobile stesso.

Poiché ogni CA di terze parti ha i propri requisiti per la richiesta di un certificato, è consigliabile esaminare i singoli requisiti direttamente con la CA.

In questo documento viene descritto come creare una richiesta di certificato sul server mobile e installare il certificato una volta emesso dalla CA.

Vedere:

Installare i certificati per la comunicazione con il Mobile Server a pagina 40

### <sup>52</sup> Server di gestione e server di registrazione MOBOTIX HUB

È possibile crittografare la connessione bidirezionale tra il server di gestione e il server di registrazione. Quando si abilita la crittografia sul server di gestione, questa si applica alle connessioni provenienti da tutti i server di registrazione che si connettono al server di gestione. Se si abilita la crittografia sul server di gestione, è necessario abilitare anche la crittografia su tutti i server di registrazione. Prima di abilitare la crittografia, è necessario installare i certificati di sicurezza nel server di gestione e in tutti i server di registrazione, inclusi i server di registrazione di failover.

### 5.3 Certificato CA di terze parti o commerciale

La procedura per la richiesta di certificati da parte di CA di terze parti per l'utilizzo con i server di gestione e i server di registrazione è identica a quella del server mobile. L'unica differenza è la configurazione con il Server Configurator.

Vedere:

Installare certificati CA di terze parti o commerciali per la comunicazione con il server di gestione o il server di registrazione a pagina 57

### 5.4 Dominio

Quando gli endpoint client e server operano tutti all'interno di un ambiente di dominio con la propria infrastruttura dell'autorità di certificazione, non è necessario distribuire i certificati CA alle workstation client. A condizione che si disponga di Criteri di gruppo all'interno del dominio, verrà gestita la distribuzione automatica di tutti i certificati CA attendibili a tutti gli utenti e i computer del dominio. Il processo per la richiesta di un certificato e l'installazione di un certificato server è identico a quello di un gruppo di lavoro.

Vedere:

Installare i certificati in un dominio per la comunicazione con il server di gestione o il server di registrazione a pagina 86

### 5.5 Gruppo di lavoro

Quando si opera in un ambiente di gruppo di lavoro, si presume che non sia presente un'infrastruttura dell'autorità di certificazione. Per distribuire i certificati, è necessario creare un'infrastruttura dell'autorità di certificazione. È inoltre necessario distribuire le chiavi del certificato alle workstation client. Ad eccezione di questi requisiti, il processo di richiesta e installazione di un certificato in un server è simile sia allo scenario di dominio che a quello di terze parti. Vedere:

Installare i certificati in un ambiente di gruppo di lavoro per la comunicazione con il server di gestione o il server di registrazione a pagina 104

### Server di eventi MOBOTIX HUB

È possibile crittografare la connessione bidirezionale tra il server di eventi e i componenti che comunicano con il server di eventi, incluso il server LPR. Quando si abilita la crittografia nel server eventi, questa si applica alle connessioni da tutti i componenti che si connettono al server eventi. Prima di abilitare la crittografia, è necessario installare i certificati di sicurezza nel server eventi e in tutti i componenti di connessione.

Vedere:

Installare i certificati per la comunicazione con il server eventi nella pagina 126

#### Cliente 5.7

Negli scenari di terze parti/commerciale e di dominio, i client non richiedono l'installazione di chiavi di certificato. È sufficiente installare le chiavi del certificato client in un ambiente di gruppo di lavoro.

Quando si abilita la crittografia su un server di registrazione, la comunicazione con tutti i client, i server e le integrazioni che recuperano i flussi di dati dal server di registrazione viene crittografata.

In questo documento questi sono indicati come "client" per il server di registrazione:

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 10/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati - VMS Milestone XProtect® Guida ai certificati - VMS Mileston XProtect<sup>®</sup>

- MOBOTIX HUB Desk Client
- Client di gestione
- Server di gestione (per Monitor di sistema e per immagini e clip video AVI nelle notifiche e-mail )
- MOBOTIX HUB Mobile Server
- Server di eventi MOBOTIX HUB
- MOBOTIX HUB LPR
- Ponte di rete MOBOTIX
- MOBOTIX HUB DLNA Server
- Siti che recuperano flussi di dati dal server di registrazione tramite MOBOTIX Interconnect
- Alcune integrazioni di MIP SDK di terze parti

Per le soluzioni create con MIP SDK 2018 R3 o versioni precedenti che accedono ai server di registrazione: se le integrazioni vengono effettuate utilizzando le librerie MIP SDK, devono essere ricompilate con MIP SDK 2019 R1; se le integrazioni comunicano direttamente con le API del server di registrazione senza utilizzare le librerie MIP SDK, gli integratori devono aggiungere autonomamente il supporto HTTPS.

Vedere:

Quali client hanno bisogno di certificati? a pagina 11 Importare i certificati client nella pagina 129

#### Quali client hanno bisogno di certificati? 6

Quali client richiedono l'installazione di certificati? Come ci pianifichiamo per questo? Cosa possiamo fare per prepararci?

I client basati su browser Web e i client distribuiti tramite un servizio o uno store pubblico di distribuzione di applicazioni di terze parti, ad esempio Google Play o Apple AppStore, non devono richiedere l'installazione di un certificato. MOBOTIX HUB Mobile non utilizzerà i certificati installati. MOBOTIX HUB Mobile può utilizzare solo certificati di terze parti affidabili.

Se i server MOBOTIX HUB (Server di gestione e Server di registrazione) sono installati su computer che fanno parte del Dominio e gli utenti che accedono al Desk Client sono tutti utenti del Dominio, il Dominio gestirà tutta la distribuzione della chiave pubblica e l'autenticazione necessarie per stabilire comunicazioni sicure.



No Public Key Distribution Needed

## **Public Key Distribution Needed**

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 12/129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati - VMS Milestone XProtect® XProtect<sup>®</sup>

Solo in uno scenario in cui Servizi certificati Active Directory viene utilizzato per creare certificati autofirmati e le risorse (utenti e computer) operano in un ambiente non di dominio, è necessario distribuire le chiavi pubbliche alle workstation client.

Vedere anche Installazione dei certificati sui client a pagina 19 e Importazione dei certificati client a pagina 129.

### 7 Server Configurator (spiegazione)

Utilizzare Server Configurator per selezionare i certificati sui server locali per la comunicazione crittografata e registrare i servizi server per renderli idonei a comunicare con i server.

I seguenti tipi di server in MOBOTIX HUB VMS necessitano di certificati per una comunicazione sicura:

- Server di gestione
- Server di registrazione
- Server di eventi
- Server mobili

Questi server funzionano con il Server Configurator per gestire le comunicazioni sicure. Utilizzare il configuratore server per impostare se i server MOBOTIX HUB utilizzano o meno comunicazioni crittografate sicure e per gestire i certificati utilizzati dai server MOBOTIX HUB.

Il configuratore del server è installato per impostazione predefinita su qualsiasi computer che ospita un server MOBOTIX HUB. Apri il Server Configurator da:

• Il menu Start di Windows

0

• Il server manager MOBOTIX HUB facendo clic con il pulsante destro del mouse sull'icona del server manager sulla barra delle applicazioni del computer e selezionando Server Configurator

### MOBOTIX HUB - Guida ai certificati - Server Configurator (spiegazione)

| Milestone Server Configurator |   | 7                  |         |
|-------------------------------|---|--------------------|---------|
| Encryption                    | Encryption  |                    |         |
| Registering servers           | It is recommended to secure communication with encryptic  | n, <u>Learn mo</u> | ore     |
| Language selection            | Server certificate<br>Applies to: management server, recording server, failover server, data<br>collector             |                    |         |
|                               | Encryption: On  |                    |         |
|                               | DocCert1  | ~                  | Details |
|                               | Ciertificate issued by mit-MJT-DC-CA, DC=mit, DC=tocal. Espires 4/27/2022   |                    |         |
|                               | Mobile streaming media certificate<br>Applies to mobile and web clients that retrieve data streams from the<br>server | mobile             |         |
|                               | Encryption: On  |                    |         |
|                               | DocCert1  | *                  | Details |
|                               | Certificate issued by mit-MUT-DC-CA, DC =mit, DC=local. Expires 4/27/2022   |                    |         |
|                               |   |                    |         |
|                               |   |                    | Apply   |
|                               |   |                    |         |

Utilizzare il Server Configurator per scegliere i certificati utilizzati dai server MOBOTIX HUB per proteggere le comunicazioni con le applicazioni client e per verificare che le impostazioni di crittografia siano configurate correttamente.

#### **Certificato server** 7.1

Selezionare il certificato da utilizzare per crittografare la connessione bidirezionale tra il server di gestione e i seguenti server:

- Server di registrazione
- Server degli eventi
- Server di registro
- Server LPR •
- Mobile Server •

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 15/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati - VMS Milestone XProtect® Guida ai certificati - VMS Mileston XProtect<sup>®</sup>

### <sup>72</sup> Server di eventi e componenti aggiuntivi

Selezionare il certificato da utilizzare per crittografare la connessione bidirezionale tra il server degli eventi e i componenti che comunicano con il server degli eventi, incluso il server LPR.

### 73 Certificato multimediale di flusso

Selezionare il certificato da utilizzare per crittografare la comunicazione tra i server di registrazione e tutti i client, i server e le integrazioni che recuperano i flussi di dati dai server di registrazione.

### 74 Certificato per lo streaming multimediale mobile

Selezionare il certificato da utilizzare per crittografare la comunicazione tra il server mobile e i client mobili e Web che recuperano i flussi di dati dal server mobile.

Nella sezione **Registrazione dei server** del Server Configurator, registrare i server in esecuzione sul computer con il server di gestione designato.

Per registrare i server, verificare l'indirizzo del server di gestione e selezionare **Registra**.

### 8 Script di PowerShell

È possibile utilizzare PowerShell e il modulo Milestone PSTools per installare, integrare, semplificare, monitorare e automatizzare la manutenzione continua e i processi di configurazione necessari di sistemi VMS MOBOTIX HUB di grandi dimensioni, complessi e tecnicamente avanzati.

Ciononostante, MOBOTIX raccomanda che gli amministratori, gli installatori e i tecnici sappiano come configurare manualmente l'ambiente MOBOTIX HUB VMS dei loro clienti. Con l'esperienza imparerai quando utilizzare gli script di PowerShell al posto delle configurazioni manuali. È possibile trovare gli script di PowerShell in questi percorsi:

- PowerShell Process/Video per server mobile e consente la crittografia
- Repository Github per informazioni, documentazione e script Milestone PSTools.

### 9 Creazione e distribuzione manuale dei certificati

### 9.1 Importante da sapere:

La creazione e la distribuzione manuale dei certificati non è consigliata come metodo sicuro per la distribuzione dei certificati. Se si sceglie la distribuzione manuale, l'utente è responsabile della sicurezza dei certificati privati in ogni momento. Quando si mantengono sicuri i certificati privati , i computer client che considerano attendibili i certificati sono meno vulnerabili agli attacchi.

In alcune situazioni, Windows Update può rimuovere periodicamente i certificati che non provengono da una "autorità di certificazione di terze parti attendibile".

Per assicurarsi che i certificati non vengano rimossi da Windows Update, è necessario abilitare l' opzione Disattiva aggiornamento automatico dei certificati radice. Prima di apportare questa modifica, è necessario assicurarsi che la modifica rispetti i criteri di sicurezza aziendali.

- 1. Abilita questa opzione aprendo l' **Editor Criteri di gruppo locali** sul computer (fai clic sulla barra di avvio di Windows e digita **gpedit.msc**).
- Nell'Editor Criteri di gruppo locali di Windows, accedere a Configurazione computer > Modelli amministrativi > Sistema > Gestione comunicazioni Internet > Impostazioni di comunicazione Internet.
- 3. Fare doppio clic su **Disattiva aggiornamento automatico del certificato radice** e selezionare **Abilitato**.
- 4. Fare clic su OK.

Si noti che questa impostazione potrebbe essere controllata da un criterio di dominio. In tal caso, deve essere disabilitato a quel livello.

Il certificato rimarrà ora sul computer anche se non proviene da una "autorità di certificazione di terze parti attendibile", perché Windows Update non contatterà il sito Web di Windows Update per vedere se Microsoft ha aggiunto la CA al suo elenco di autorità attendibili.

### 9.2 Creare un certificato CA

Su un computer con accesso limitato e non connesso al sistema MOBOTIX HUB, eseguire questo script una volta per creare un certificato CA.



Il computer usato per la creazione dei certificati deve eseguire Windows 10 o Windows Server OS 2016 o versioni successive.

Tenere presente che quando si creano certificati in questo modo, i certificati sono correlati al computer in cui sono installati. Se il nome del computer cambia, il VMS non sarà in grado di avviarsi fino a quando i certificati non verranno creati di nuovo e reinstallati nel computer.

### Questo script crea due certificati:

- Un certificato privato: esiste nell'archivio Certificati personali per l'utente corrente solo dopo l'esecuzione dello script . Si consiglia di creare un backup conservato su un supporto (USB) in un luogo sicuro e preferibilmente due backup conservati in posizioni fisicamente diverse. Ad eccezione dei backup, questo certificato non deve mai lasciare il computer in cui è stato creato il certificato
- Un certificato pubblico: da importare come certificato attendibile in tutti i computer client
- 1. Nell'Appendice A, alla fine di questa guida, è disponibile uno script per la creazione del certificato CA. Copia il contenuto.
- 2. Apri Blocco note e incolla il contenuto.

È molto importante che le righe si interrompano negli stessi punti dell'Appendice A. Puoi aggiungere le interruzioni di riga in Blocco note o, in alternativa, riaprire questo PDF con Google Chrome, copiare nuovamente il contenuto e incollarlo in Blocco note.

| 1  | CreateCACertificate.ps1 - Notepad   | ×   |
|--|---|---|
| File Edit Format View Help   |   |   |
| <pre># Run this script once, to creat<br/># Private certificate for signin<br/>Sca_certificate = New-SelfSigned<br/>KeyUsage CertSign, CRLSign, Dig<br/># Thumbprint of private certific<br/>Set-Content -Path "\$PSScriptRoot<br/># Public CA certificate to trust<br/>Export-Certificate -Cert "Cert:\</pre> | e a certificate that can sign multiple recording server certificates<br>g other certificates (in certificate store)<br>Certificate -CertStoreLocation cert:\CurrentUser\My -DnsName 'VMS Certificate Au<br>italSignature -FriendlyName 'VMS CA Certificate'<br>ate used for signing other certificates<br>cca_thumbprint.txt" -Value \$ca_certificate.Thumbprint<br>(Third-Party Root Certification Authorities)<br>CurrentUser\My\\$(\$ca_certificate.Thumbprint)" -FilePath "\$PSScriptRoot\root-auth | uthority' -KeyusageProperty All `<br>hority-public.cer" |
|  |   | >   |
|  |   | Ln & Col 130  |

 In Blocco note fare clic su File -> Salva con nome, assegnare al file il nome CreateCACertificate.ps1 e salvarlo localmente, in questo modo:

C:\Certificati\CreateCACertificate.ps1.

4. In Esplora file passare a C:\Certificates e selezionare il **file CreateCACertificate.ps1**.

5. Nel menu File selezionare Apri Windows PowerShell e quindi Apri Windows PowerShell come amministratore.

| 1 🔁 🖬 🕈 I                        |   |  | 1                             | Cert                      |      |      |
|----------------------------------|---|--|-------------------------------|---------------------------|------|------|
| File<br>Open <u>n</u> ew window  | * | Open Windows PowerShell                  | Open •                        | Select all                |      |      |
| Open command prompt              | + | Open Windows PowerShell as administrator | Properties<br>History<br>Open | Select                    |      |      |
| Open Windows Powe <u>r</u> Shell |   |  |                               |                           |      |      |
| Prolate bistory                  |   |  | Date modified                 | Туре                      | Size |      |
| Delete history                   |   |  | 04-02-2019 11:31              | File folder               |      |      |
|                                  |   |  | 04-02-2019 11:31              | File folder               |      |      |
| Teib                             |   |  | 04-02-2019 11:31              | File folder               |      |      |
| ¥                                |   |  | 04-02-2019 11:31              | File folder               |      |      |
| Close                            |   |  | 04-02-2019 11:31              | File folder               |      |      |
|                                  |   |  | 04-02-2019 11:31              | File folder               |      |      |
| Sec. 20                          |   | CreateCACertificate.ps1                  | 31-01-2019 15:01              | Windows PowerShell Script |      | 1 KE |
| 📕 This PC                        |   |  |                               |                           |      |      |

6. In PowerShell, al prompt, immettere .\CreateCACertificate.ps1 e premere INVIO.

| 🛃 Admir   | nistrator: Windows Pow | verShell    |                               |  | × |
|-----------|------------------------|-------------|-------------------------------|--|---|
| PS C:\Cer | tificates> .\Crea      | teCACertifi | tate.ps1                      |  | ^ |
| Direc     | tory: C:\Certific      | ates        |                               |  |   |
| Mode      | LastWr                 | iteTime     | Length Name                   |  |   |
| -a        | 31-01-2019             | 09:29       | 844 root-authority-public.cer |  |   |
| PS C:\Cer | tificates>             |             |                               |  |   |
|           | and the product of     |             |                               |  |   |

7. Verificare che il file root-authority-public.cer sia visualizzato nella cartella in cui è stato eseguito lo script.



### 10 Installare i certificati nei client

Dopo aver creato il certificato CA, è possibile considerare attendibile il certificato CA pubblico installandolo in tutti i computer che fungono da client per il servizio in base alle descrizioni descritte in Introduzione ai certificati a pagina 5.



Vedere Importazione dei certificati client a pagina 129 per una procedura alternativa all'installazione manuale dei certificati sui client.

 Copiare il file root-authority-public.cer dal computer in cui è stato creato il certificato CA (C:\Certificates\root-authority-public.cer) al computer in cui è installato il client MOBOTIX HUB.



Per informazioni sui servizi client e server e sulle integrazioni che richiedono il certificato, vedere Introduzione ai certificati a pagina 5.



9. Fare clic con il pulsante destro del mouse sul certificato e selezionare Installa certificato.

| Certificate Import Wizard  |   |
|--|---|
| Welcome to the Certificate Impor   | t Wizard  |
| This wizard helps you copy certificates, certificate tru<br>lists from your disk to a certificate store,   | ust lists, and certificate revocation   |
| A certificate, which is issued by a certification authori<br>and contains information used to protect data or to e<br>connections. A certificate store is the system area wi | ity, is a confirmation of your identity<br>stablish secure network<br>here certificates are kept. |
| Store Location   |   |
|  |   |
| To continue, click Next.   |   |
|  |   |
|  |   |
|  | Next Cancel   |

- 10. Nell'Importazione **guidata certificati**, selezionare per installare il certificato nell'archivio del **computer locale** e fare clic su **Avanti**.
- 11. Selezionare questa opzione per individuare manualmente l'archivio in cui verrà installato il certificato.

| Certificate Store   |   |                                       |                                      |
|---|---|---------------------------------------|--------------------------------------|
| Certificate stores are system areas   | where certifica                                       | tes are kept.                         |                                      |
| Windows can automatically select a<br>the certificate.<br>Automatically select the cert<br>Place all certificates in the fo | certificate store<br>ficate store bas<br>lowing store | e, or you can spe<br>ed on the type o | cify a location for<br>f certificate |
| Certificate store:  |   |                                       | Browse                               |
|   |   |                                       |                                      |
|   |   |                                       |                                      |
|   |   |                                       |                                      |
|   |   |                                       |                                      |

12. Fare clic su Sfoglia, selezionare Autorità di certificazione radice attendibili e fare clic su OK. Quindi fare clic su Avanti.



13. Nella finestra di dialogo Completamento dell'Importazione guidata certificati fare clic su Fine.



Se viene visualizzato un avviso di sicurezza che indica che si sta per installare un certificato radice, fare clic su **Sì** per continuare.

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 23/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati - VMS Milestone XProtect® XProtect<sup>®</sup>

| Completing                     | the Certificate Import Wi                             | zard             |
|--------------------------------|---|------------------|
| The certificate will b         | e imported after you dick Finish.                     |                  |
| You have specified             | he following settings:                                |                  |
| Certificate Store S<br>Content | elected by User Trusted Root Certifica<br>Certificate | tion Authorities |
|                                |   |                  |
|                                |   |                  |
|                                |   |                  |
|                                |   |                  |
|                                |   |                  |

14. Riceverai una finestra di dialogo di conferma dell'avvenuta importazione.



15. Per verificare che il certificato sia stato importato, avviare Microsoft Management Console.

| 🗐 Run |  | ×  |
|-------|--|----|
| D     | Type the name of a program, folder, document, or Intern<br>resource, and Windows will open it for you. | et |
| Open: | mmd  | ¥  |
|       | OK Cancel <u>B</u> rowse   |    |

In Microsoft Management Console, dal menu File selezionare Aggiungi/Rimuovi snap-in....

| Open                 | Ctrl+0 | ame                                      | Actions      |  |
|----------------------|--------|--|--------------|--|
| Save                 | Ctrl+S | There are a fame to the state fame       | Console Root |  |
| Save As              |        | There are no items to show in this view. | More Actions |  |
| Add/Remove Snap-in C | trl+M  | vi                                       |              |  |
| Options              |        |  |              |  |
| Recent File          |        |  |              |  |
| Exit                 |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |
|                      |        |  |              |  |

Selezionare lo snap-in Certificati e fare clic su Aggiungi.

| nap-in<br>ActiveX Control                  | Vendor<br>Microsoft Cor        | ^ | Console Root | Edit Extensions   |
|--|--------------------------------|---|--------------|-------------------|
| Authorization Manager                      | Microsoft Cor                  |   |              | gendys            |
| Component Services                         | Microsoft Cor                  |   |              | (More Ep)         |
| Device Manager<br>Disk Management          | Microsoft Cor<br>Microsoft and |   | Add >        | Wate Days         |
| Event Viewer<br>Folder                     | Microsoft Cor<br>Microsoft Cor |   |              |                   |
| Group Policy Object<br>Internet Informatio | Microsoft Cor<br>Microsoft Cor |   |              |                   |
| Internet Informatio                        | Microsoft Cor                  |   |              | -                 |
| SIP Security Monitor                       |                                | ~ |              | Ad <u>v</u> anced |

18. Selezionare l'opzione che lo snap-in deve gestire i certificati per l' **account computer**.

| Certificates snap-in                              | ×             |
|---|---------------|
| This snap-in will always manage certificates for: |               |
| <u>Service account</u> <u>Computer account</u>    |               |
|   |               |
|   |               |
|   |               |
|   |               |
| Bac   | Next > Cancel |

Selezionare Computer locale come computer che si desidera gestire con lo snap-in e fare clic su Fine.

| ect Computer  |                           |
|---|---------------------------|
| Select the computer you want this snap-in to manage.  |                           |
| This snap-in will always manage:      OLocal computer: the computer this console is running on) |                           |
| O Another computer:   | Byzante                   |
| Allow the selected computer to be changed when launching fr                                     | om the command line. This |
| ony applies il you save the console.  |                           |
| ony applies il you save the console.  |                           |
| ony applies il you save the console.  |                           |

20. Fare clic su **OK** dopo aver aggiunto lo snap-in.

| vailable <u>s</u> nap-ins:  |  |              | Selected snap-ins:                      |                   |
|---|--|--------------|---|-------------------|
| Snap-in<br>ActiveX Control<br>Authorization Manager<br>Certificates<br>Component Services<br>Computer Managem<br>Device Manager<br>Disk Management<br>Event Viewer<br>Folder<br>Group Policy Object | Vendor<br>Microsoft Cor<br>Microsoft Cor | A            | Console Root                            | Edit Extensions   |
| Internet Informatio   | Microsoft Cor<br>Microsoft Cor   | • the conten | of the certificate stores for yourself, | Ad <u>v</u> anced |

21. Verificare che il certificato sia elencato nella vista centrale delle autorità di certificazione radice attendibili

sottoalbero.

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 27/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati - VMS Milestone XProtect® Guida ai certificati - VMS Mileston XProtect<sup>®</sup>

| Eile <u>A</u> ction <u>V</u> iew Fav <u>o</u> rites <u>W</u> indow <u>H</u> e   | ip  |   |  |   | - 8 0 |
|---|---|---|--|---|-------|
|   |   |   |  |   |       |
| Console Root  | Issued To   | Issued By   | Exp ^  | Actions                                 |       |
| Console Root Personal Certificates (Local Computer) Personal Certificates (Local Certification Authorities Certificates Certificates Certificates Certificates Certificates Cultured Publishers Cultured People Client Authentication Issuers Preview Build Roots AD Token Issuer Set AAD Token Issuer Set Remote Desktop Certificate Enrollment Requests Remote Desktop Certificate Roots Trusted Roots Trusted Roots Certificate Set Certificates Certificate Reguests Certificate Roots Certificate Roots Certificate Roots Certificate Set Certificates Certificate Roots Certificate | Issued To<br>10.5,14.40<br>10.5,6,101<br>AddTrust External CA Root<br>Baltimore CyberTrust Root<br>Cass 3 Public Primary Certificat<br>Copyright (c) 1997 Microsoft C<br>DigiCert Assured ID Root CA<br>DigiCert Global Root CA<br>DigiCert High Assurance EV Ro<br>DST Root CA X3<br>Equifax Secure Certificate Auth<br>GobalSign<br>GlobalSign<br>GlobalSign<br>GlobalSign<br>GlobalSign<br>GlobalSign Root CA<br>Go Daddy Class 2 Certification<br>GTE CyberTrust Global Root<br>Hotspot 2.0 Trust Root CA - 03<br>Microsoft Authenticode(tm) Ro | Issued By<br>10.5.14.40<br>10.5.6.101<br>AddTrust External CA Root<br>Baltimore CyberTrust Root<br>CKMS<br>Class 3 Public Primary Certificatio<br>Copyright (c) 1997 Microsoft Corp.<br>DigiCert Global Root CA<br>DigiCert High Assurance EV Root<br>DST Root CA X3<br>Equifax Secure Certificate Authority<br>GeoTrust Global<br>GlobalSign<br>GlobalSign<br>GlobalSign Root CA<br>Go Daddy Class 2 Certification Au<br>GTE CyberTrust Global Root<br>Hotspot 2.0 Trust Root CA - 03<br>Microsoft Authenticode(tm) Root | Exp * 20:<br>20:<br>20:<br>20:<br>20:<br>20:<br>20:<br>20:<br>20:<br>20: | Actions<br>Certificates<br>More Actions | •     |
|   | Microsoft Root Certificate Auth     Starfield Class 2 Certification A     Starfield Services Root Certificat     Symantec Enterprise Mobile Ro  | Microsoft Root Certificate Authori<br>Microsoft Root Certificate Authori<br>Microsoft Root Certificate Authori<br>Microsoft Root Certificate Authori<br>MO LIABILITY ACCEPTED, (c)97 Ve<br>Starfield Class 2 Certification Auth<br>Starfield Services Root Certificate<br>Symantec Enterprise Mobile Root   | 202<br>202<br>202<br>202<br>202<br>202<br>202<br>202<br>202<br>202       |   |       |

22. Ripetere i passaggi nel computer successivo che viene eseguito come client per il servizio in cui viene abilitata la crittografia , fino a quando il certificato non è stato installato in tutti i computer pertinenti.

### **11** Creare un certificato SSL

Dopo aver installato il certificato CA su tutti i client, è possibile creare i certificati da installare su tutti i computer che eseguono server (server di registrazione, server di gestione, server mobili o server di failover).



Il computer usato per la creazione dei certificati deve eseguire Windows 10 o Windows Server 2016 o versioni successive.

Nel computer in cui è stato creato il certificato CA, dalla cartella in cui è stato inserito il certificato CA, eseguire lo script **Certificato server** per creare certificati SSL per tutti i server. Nell'Appendice B alla fine di questa guida, è disponibile uno script per la creazione di certificati server.

1. Apri Blocco note e incolla il contenuto.



È molto importante che le linee si interrompano negli stessi punti dell'Appendice B. Puoi aggiungere le interruzioni di riga in Blocco note o, in alternativa, riaprire questo PDF con Google Chrome, copiare nuovamente il contenuto e incollarlo in Blocco note.

In Blocco note fare clic su File -> Salva con nome, assegnare al file il nome
 CreateServerCertificate.ps1 e salvarlo localmente nella stessa cartella del certificato CA, in questo modo:

C:\Certificates\CreateServerCertificate.ps1.

- 3. In Esplora file passare a C:\Certificates e selezionare il file CreateServerCertificate.ps1.
- 4. Nel menu File selezionare Apri Windows PowerShell e quindi Apri Windows PowerShell come amministratore.

| Open <u>n</u> ew window  | * | Open Windows PowerShell                  | . Open ▼<br>→ Edit         | Select all               |       |     |
|--|---|--|----------------------------|--------------------------|-------|-----|
| Open command <u>p</u> rompt  |   | Open Windows PowerShell as administrator | Properties History<br>Open | Select                   |       |     |
| Open Windows Powe <u>r</u> Shell   | * |  |                            |                          |       |     |
| Diaman   |   |  | Date modified              | Туре                     | Size  |     |
| Delete history   | * |  | 04-02-2019 11              | 31 File folder           |       |     |
| and and a second se |   |  | 04-02-2019 11              | 31 File folder           |       |     |
| р цевр   |   |  | 04-02-2019 11              | :31 File folder          |       |     |
| a second   |   |  | 04-02-2019 11              | :31 File folder          |       |     |
| Llose  |   |  | 04-02-2019 11              | 53 File folder           |       |     |
|  |   |  | 04-02-2019 11              | :31 File folder          |       |     |
| Q  |   | CreateCACertificate.ps1                  | 31-01-2019 15              | :01 Windows PowerShell S | cript | 1K  |
| 🖳 This PC  |   | CreateServerCertificate.p                | s1 25-01-2019 15           | 31 Windows PowerShell S  | cript | 3 K |

- 5. In PowerShell al prompt immettere .\CreateServerCertificate.ps1 e premere INVIO.
- 6. Immettere il nome DNS per il server. Se il server ha più nomi, ad esempio per uso interno ed esterno, aggiungili qui, separati da uno spazio. Premere **Invio**.



Per trovare il nome DNS, aprire Esplora file nel computer che esegue il servizio Server di registrazione. Fare clic con il pulsante destro del mouse su **Questo PC** e selezionare **Proprietà**. Utilizzare il **nome completo del computer**.

×

Administrator: Windows PowerShell — PS C:\Certificates> .\CreateServerCertificate.ps1 DNS names for server SSL certificate (delimited by space - 1st entry is also subject of certificate): \_

7. Immettere l'indirizzo IP del server. Se il server ha più indirizzi IP, ad esempio per uso interno ed esterno, aggiungili qui, separati da uno spazio. Premere **Invio**.



Per trovare l'indirizzo IP, è possibile aprire il prompt dei comandi sul computer che esegue il servizio Server di registrazione. Immettere **ipconfig /all**. Se è stato installato il sistema MOBOTIX HUB, è possibile aprire il client di gestione, accedere al server e trovare l'indirizzo IP nella **scheda Info**.

8. Specificare una password per il certificato e premere **Invio** per completare la creazione.



Questa password viene utilizzata quando si importa il certificato nel server.

Nella cartella in cui è stato eseguito lo script viene visualizzato un file Subjectname.pfx.

9. Eseguire lo script fino a quando non si dispone di certificati per tutti i server.

### 12 Importa certificato SSL

Dopo aver creato i certificati SSL, installarli nei computer che eseguono il servizio server.



Tenere presente che ogni certificato viene creato per un server specifico.

- 10. Copiare il file Subjectname.pfx pertinente dal computer in cui è stato creato il certificato al computer del servizio server corrispondente.
- 11. Nel computer del servizio server avviare Gestisci **certificati computer**.
- 12. Fare clic su **Personale**, fare clic con il pulsante destro del mouse su **Certificati** e selezionare **Tutte le attività** > **importare**.



 Selezionare questa opzione per importare il certificato nell'archivio del computer locale e fare clic su Avanti.

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

14. Individuare il file del certificato e fare clic su Avanti.

| File to Import |                              |                          |                    |          |
|----------------|------------------------------|--------------------------|--------------------|----------|
| Specify the    | file you want to import.     |                          |                    |          |
| File name:     |                              |                          |                    |          |
| G:\Users\g     | is\Documents\Wy Received     | Files\VMS-REC-01.p       | Bro                | wse      |
| Note: More     | than one certificate can be  | e stored in a single fil | e in the following | formats: |
| Personal       | Information Exchange- PK     | CS #12 (.PFX,,P12)       |                    |          |
| Cryptogr       | aphic Message Syntax Sta     | ndard-PKCS #7 Cert       | ificates (.P7B)    |          |
| Microsofi      | Serialized Certificate Store | e (.SST)                 |                    |          |
|                |                              |                          |                    |          |
|                |                              |                          |                    |          |
|                |                              |                          |                    |          |

15. Immettere la password per la chiave privata specificata al momento della creazione del certificato del server, quindi fare clic su **Avanti**.

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

16. Inserire il file nell'archivio certificati: Personale, quindi fare clic su Avanti.

| ertificate Store              |                          |                     |                     |
|-------------------------------|--------------------------|---------------------|---------------------|
| Certificate stores are system | areas where certifica    | ites are kept.      |                     |
| Windows can automatically s   | elect a certificate stor | e, or you can speci | fy a location for   |
| the certificate.              |                          | et or for enrichen  | 17 5 10 10 10 10 10 |
| O Automatically select t      | e certificate store bas  | sed on the type of  | certificate         |
| Place all certificates in     | the following store      |                     |                     |
| Certificate store:            |                          |                     |                     |
| Personal                      |                          |                     | Browse              |
|                               |                          |                     |                     |
|                               |                          |                     |                     |
|                               |                          |                     |                     |
|                               |                          |                     |                     |
|                               |                          |                     |                     |

17. Verificare le informazioni e fare clic su **Fine** per importare il certificato.

| the certificate will be imported after you click  | Finish,                     |
|---|-----------------------------|
|   |                             |
| ou have specified the following settings:<br>Certificate Store Selected by User Persona |                             |
| Content PFX   |                             |
| File Name C; \User:   | \gis\Desktop\VMS-REC-01.ptx |
|   |                             |

Il certificato importato viene visualizzato nell'elenco.
| Certificates - Local Computer Personal Certificates Trusted Root Certification Authorities Intermediate Certification Authorities Intermediate Certification Authorities Intrusted Publishers Intrusted Publishers Intrusted Certificates Intrusted People Intrusted | Issued To<br>역:<br>*<br>역:<br>Iocalhost<br>VMS Certificate Authority<br>역: VMS-REC-01 | Issued By<br>Iocalhost<br>VMS Certificate Authority<br>VMS Certificate Authority |
|---|---|--|

 Per consentire a un servizio di utilizzare la chiave privata del certificato, fare clic con il pulsante destro del mouse sul certificato e selezionare Tutte le attività >

## 12.1 Gestisci le chiavi private.

| Open                             |
|----------------------------------|
| Request Certificate with New Key |
| Renew Certificate with New Key   |
| Manage Private Keys              |
| Advanced Operations              |
| Export                           |
|                                  |

1. Aggiungere l'autorizzazione di lettura per l'utente che esegue i servizi MOBOTIX HUB VMS che deve utilizzare il certificato del server.

| roup or user names:   |               |          |
|---|---------------|----------|
| SYSTEM  |               |          |
| Administrators (Administrato  | ors)          |          |
| NET WORK BERVICE  |               |          |
|   |               |          |
|   |               |          |
|   | A <u>d</u> d  | Remove   |
| ermissions for NETWORK<br>ERVICE  | Allow         | Deny     |
| Full control  |               |          |
| Read  | D             |          |
| Special permissions   |               |          |
| or special permissions or advan   | ced settings, | Advanced |
| a service provide a service ser |               | 11 PM    |

2. Passare al computer successivo fino a quando non sono stati installati tutti i certificati del server.

## 13 Creare un certificato SSL per il server di gestione del failover

Il failover del server di gestione MOBOTIX HUB è configurato su due computer. Per assicurarsi che i client considerino attendibile il server di gestione in esecuzione, installare il certificato SSL nel computer primario e in quello secondario.

Per creare e installare il certificato SSL per il cluster di failover, è necessario installare prima il certificato CA. Nel computer in cui è stato creato il certificato CA, dalla cartella in cui è stato inserito il certificato CA, eseguire lo script del certificato del server di gestione failover per creare un certificato SSL per il computer primario e secondario.



Il computer usato per la creazione dei certificati deve eseguire Windows 10 o Windows Server 2016 o versioni successive.

- 3. Nell'Appendice C di questa guida copiare lo script per la creazione dei certificati del server di gestione del failover.
- 4. Apri Blocco note e incolla lo script.



È molto importante che le righe si interrompano negli stessi punti come mostrato in Appendice C. Puoi aggiungere le interruzioni di riga in Blocco note o, in alternativa, riaprire questo PDF con Google Chrome, copiare nuovamente il contenuto e incollarlo in Blocco note.

5. In Blocco note selezionare File -> Salva con nome, assegnare al file il nome CreateFailoverCertificate.ps1 e salvarlo localmente nella stessa cartella del certificato CA:

#### Esempio: C:\Certificates\CreateFailoverCertificate.ps1.

- 6. In Esplora file passare a C:\Certificates e selezionare il file CreateFailoverCertificate.ps1.
- 7. Nel menu File selezionare Apri Windows PowerShell e quindi Apri Windows PowerShell come amministratore.

| File                            |   |  |                                 |                             |      |      |
|---------------------------------|---|--|---------------------------------|-----------------------------|------|------|
| Open <u>n</u> ew window         | • | Open Windows Powe <u>r</u> Shell         | Dopen •                         | Select all                  |      |      |
| Open command <u>p</u> rompt     | ÷ | Open Windows PowerShell as administrator | Properties<br>+ History<br>Open | Select                      |      |      |
| Open Windows Powe <u>r</u> Shel |   |  |                                 |                             |      |      |
|                                 |   | 4  | Date modified                   | Туре                        | Size |      |
|                                 |   |  | 04-02-2019 11:3                 | 1 File folder               |      |      |
| 0.000                           |   |  | 04-02-2019 11:3                 | 1 File folder               |      |      |
| С цер                           |   |  | 04-02-2019 11:3                 | 1 File folder               |      |      |
| 1                               |   |  | 04-02-2019 11:3                 | 1 File folder               |      |      |
| Llose                           |   |  | 04-02-2019 11:5                 | 3 File folder               |      |      |
|                                 |   |  | 04-02-2019 11:3                 | 1 File folder               |      |      |
| Sec. 2                          |   | ReateCACertificate.ps1                   | 31-01-2019 15:0                 | 1 Windows PowerShell Script |      | 1 KB |
| 🖳 This PC                       |   | CreateServerCertificate.p                | s1 25-01-2019 15:3              | 1 Windows PowerShell Script |      | 3 KB |

#### - Deskton

- 8. In PowerShell immettere .\CreateFailoverCertificate.ps1 al prompt e premere INVIO.
- 9. Specificare i nomi di dominio completi e i nomi host per il computer primario e secondario, separati da una virgola.

Esempio: pc1host,pc1host.domain,pc2host,pc2host.domain.

10. Premere Invio.

#### © MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 39/129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati XProtect<sup>®</sup>

## MOBOTIX HUB - Guida ai certificati - Creare un certificato SSL per il server di gestione

- 11. Specificare l'indirizzo IP virtuale del cluster di failover. Premere Invio.
- 12. Specificare una password per il certificato e premere **Invio** per completare la creazione.

Questa password viene utilizzata quando si importa il certificato nel server.

Il file [virtualIP].pfx viene visualizzato nella cartella in cui è stato eseguito lo script. Importare il certificato nello stesso modo in cui si importerà un certificato SSL, vedere Importazione di un certificato SSL a pagina 29. Importare il certificato nei computer primario e secondario.

## 14 Installare i certificati per la comunicazione con il server mobile

Per utilizzare un protocollo HTTPS per stabilire una connessione sicura tra il server mobile e i client e i servizi, è necessario applicare un certificato valido al server. Il certificato conferma che il titolare del certificato è autorizzato a stabilire connessioni sicure.

In MOBOTIX HUB VMS, la crittografia è abilitata o disabilitata per ogni server mobile. È possibile abilitare o disabilitare la crittografia durante l'installazione del prodotto MOBOTIX HUB VMS o utilizzando il Server Configurator. Quando si abilita la crittografia su un server mobile, si utilizza la comunicazione crittografata con tutti i client, i servizi e le integrazioni che recuperano i flussi di dati.



٢

Quando si configura la crittografia per un gruppo di server, è necessario abilitarla con un certificato appartenente allo stesso certificato CA oppure, se la crittografia è disabilitata, deve essere disabilitata in tutti i computer del gruppo di server.

I certificati emessi da CA (Certificate Authority) hanno una catena di certificati e alla radice di tale catena si trova il certificato radice CA. Quando un dispositivo o un browser vede questo certificato, confronta il suo certificato radice con quelli preinstallati sul sistema operativo (Android, iOS, Windows, ecc.). Se il certificato radice è elencato nell'elenco dei certificati preinstallati, il sistema operativo garantisce all'utente che la connessione al server sia sufficientemente sicura. Questi certificati vengono emessi per un nome di dominio e non

## 14.1 Aggiungere un certificato CA al server

Aggiungere il certificato CA al server mobile effettuando le seguenti operazioniNel computer che ospita il server mobile, aprire Microsoft Management Console.

I parametri specifici dipendono dalla CA. Fare riferimento alla documentazione della CA prima di procedere.

|               | Type the name of a progressource, and Windows | gram, folder, docun<br>will open it for you | nent, or Internet |
|---------------|---|---|-------------------|
| <u>O</u> pen: | mmd   |   | Y                 |

1. In Microsoft Management Console, dal menu File selezionare Aggiungi/Rimuovi snap-in....

# MOBOTIX HUB – Guida ai certificati - Installare i certificati per la comunicazione con il

| New Ctrl+N                | 1  | 1                       | _ |
|---------------------------|--|-------------------------|---|
| Save Ctrl+S               | Name                                     | Actions<br>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. Selezionare lo snap-in Certificati e fare clic su Aggiungi.
- 3. Fare clic su OK.

| ailable snap-ins:                            |                   |                 | Selected snap-ins:                     | -                       |
|--|-------------------|-----------------|--|-------------------------|
| inap-in                                      | Vendor            | ^               | Console Root                           | Edit Extensions         |
| ActiveX Control                              | Microsoft Cor     |                 | Certificates - Current Us              | Remove                  |
| Authorization Manager                        | Microsoft Cor     |                 |  |                         |
| Certificate Templates                        | Microsoft Cor     |                 |  | -                       |
| Certificates                                 | Microsoft Cor     |                 |  | Albert Lo               |
| Certification Authority                      | Microsoft Cor     |                 |  | Salaran Crawn           |
| Component Services                           | Microsoft Cor     | Add >           |  |                         |
| Computer Managem                             | Microsoft Cor     |                 |  |                         |
| Device Manager                               | Microsoft Cor     |                 |  |                         |
| Enterprise DVT                               | Microsoft and     |                 |  |                         |
| Event Viewer                                 | Microsoft Cor     |                 |  |                         |
| Folder                                       | Microsoft Cor     |                 |  |                         |
| Group Policy Object                          | Microsoft Cor     |                 |  | with contract of        |
| Second react orderers                        |                   | *               |  | Advanced                |
| escription:                                  |                   |                 |  |                         |
| The Certificates snap-in allo                | ows you to browse | the contents of | the certificate stores for yourself, a | service, or a computer. |
| escription:<br>The Certificates snap-in allo | ows you to browse | the contents of | the certificate stores for yourself, a | service, or a computer. |

© MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 42/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati WS Mes Quida ai certificati VMS Milestone XProtect®

4. Espandere l'oggetto Certificati. Fare clic con il pulsante destro del mouse sulla cartella Personale e selezionare Tutte le attività > Operazioni avanzate > Crea richiesta personalizzata.

| 10.0                              |  |
|-----------------------------------|--|
| Type<br>ificates                  |  |
|                                   |  |
| Find Certificates                 |  |
| Request New Certificate<br>Import |  |
| Advanced Operations >             | Create Custom Request  |
|                                   | Enroll On Behalf Of<br>Manage Enrollment Policies                            |
| i                                 | ficates Find Certificates Request New Certificate Import Advanced Operations |

- 5. Fare clic su Avanti nella procedura guidata Registrazione certificati e selezionare Procedi senza criteri di registrazione.
- 6. Fare clic su Avanti.

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 Corre   |
|                                   | INext Cance |

© MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 43/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati - VMS Milestone XProtect® XProtect<sup>®</sup>

7. Selezionare il modello di chiave CNG (Nessun modello) e il formato della richiesta CMC, quindi fare

| Certificate Enrollment                          |  |                                    |
|---|--|------------------------------------|
| Custom request                                  |  |                                    |
| Chose an option from                            | the list below and configure the certificate option                              | ns as 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<br>option is specified in | not available for certificates based on a custom ce<br>the certificate template. | ertificate request, even when this |
|   |  |                                    |
|   |  |                                    |
|   |  |                                    |
|   |  |                                    |
|   |  | <u>N</u> ext Can                   |
|   |  |                                    |

- 8. Espandere per visualizzare i dettagli della richiesta personalizzata e fare clic su Proprietà.
- 9. Nella scheda Generale, compila i campi Nome descrittivo e Descrizione con il nome di dominio registrato con la CA.



Il formato della richiesta dipende dalla CA. Se viene scelto il formato errato, la CA genererà un errore quando viene inviata la richiesta di firma del certificato (CSR). Verifica con la CA per assicurarti di scegliere correttamente.

© MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 44/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati - VMS Milestone XProtect® XProtect<sup>®</sup>

# MOBOTIX HUB – Guida ai certificati - Installare i certificati per la comunicazione con il

| ertificati | ePropen | 185          |                |                     |                 |              |
|------------|---------|--------------|----------------|---------------------|-----------------|--------------|
| General    | Subject | Extensions   | Private Key    | Signature           |                 |              |
| A friend   | ly name | and descript | tion will make | e it easier to ider | ntify and use a | certificate. |
| Friendly   | name:   |              |                |                     |                 |              |
| TestLab    | Domain  | .com         |                |                     |                 |              |
| Descript   | tion:   |              |                |                     |                 |              |
| TestLab    | Domain  | .com         |                |                     |                 |              |
|            |         |              |                |                     |                 |              |
|            |         |              |                |                     |                 |              |
|            |         |              |                |                     |                 |              |
|            |         |              |                |                     |                 |              |
|            |         |              |                |                     |                 |              |
|            |         |              |                |                     |                 |              |
|            |         |              |                |                     |                 |              |
|            |         |              |                |                     |                 |              |
|            |         |              |                |                     |                 |              |
|            |         |              |                |                     |                 |              |
|            |         |              |                |                     |                 |              |
|            |         |              |                |                     |                 |              |
|            |         |              |                |                     |                 |              |
|            |         |              |                |                     |                 |              |

10. Nella scheda **Oggetto** immettere i parametri richiesti dalla CA specifica.

Ad esempio, il nome del soggetto **Tipo** e **Valore** sono diversi per ogni CA. Un esempio sono le seguenti informazioni obbligatorie:

- Nome comune:
- Organizzazione:
- Unità organizzativa :
- Città/Località:
- Stato/Provincia:
- Paese/Regione:

| ertificat                    | e Propert                            | ties  |                               |                              |   | >                               |
|------------------------------|--------------------------------------|---|-------------------------------|------------------------------|---|---------------------------------|
| General                      | Subject                              | Extensions                                    | Private Key                   | Signature                    |   |                                 |
| The sub<br>can ent<br>can be | oject of a<br>er inform<br>used in a | certificate is<br>ation about<br>certificate. | the user or c<br>the types of | omputer to w<br>subject name | hich the certificate i<br>and alternative nam | s issued. You<br>ie values that |
| Subject                      | of certifi                           | cate  |                               |                              |   |                                 |
| The use                      | r or com                             | puter that is                                 | receiving the                 | certificate                  |   |                                 |
| Subject                      | name:                                |   | 0.11                          |                              |   |                                 |
| Туре:                        |                                      |   |                               |                              | CN=Test for Doc                               | 3                               |
| Count                        | ry                                   |   |                               | Add                          | OU=MJT Lab                                    |                                 |
| Value:                       |                                      |   | ×                             | Remove                       | L=Maple Grove<br>S=MN<br>C=USA                |                                 |
| Alternat                     | tive name                            | e;  | <u>-</u>                      |                              |   |                                 |
| Туре:                        |                                      |   |                               |                              | 1 m   |                                 |
| Direct                       | ory name                             | -   | -                             |                              |   |                                 |
| Value:                       |                                      |   |                               | Add >                        |   |                                 |
|                              |                                      |   | 10                            | Remove                       |   |                                 |
|                              |                                      |   |                               |                              |   |                                 |
|                              |                                      |   |                               |                              |   |                                 |
|                              |                                      |   | _                             |                              |   | _                               |
|                              |                                      |   |                               | OK                           | Cancel  | Apply                           |

 Alcune CA non richiedono estensioni. Tuttavia, se necessario, vai alla scheda Estensioni ed espandi il menu Utilizzo chiavi . Aggiungere le opzioni richieste dall'elenco Opzioni disponibili all' elenco Opzioni selezionate. 12. Nella scheda **Chiave privata** espandere il menu **Opzioni chiave**.

| Lertificate Properties                          |                      |  |    |
|---|----------------------|--|----|
| General Subject Extensions                      | Private Key Signa    | ature                                      |    |
| The following are the certific                  | ate extensions for t | this certificate type.                     | 1  |
| Key usage                                       |                      |  | ~  |
| The key usage extension des                     | scribes the purpose  | e of a certificate.                        |    |
| Available options:                              |                      | Selected options:                          |    |
| CRL signing<br>Data encipherment                |                      | Digital signature<br>Key certificate signi | ng |
| Decipher only                                   |                      | Key encipherment                           |    |
| Encipher only<br>Key agreement                  | Add >                |  |    |
| Non repudiation                                 | < Perman             |  |    |
| Make these key usages cr                        | itical               |  | _  |
|   |                      |  |    |
| Extended Key Usage (applic                      | ation policies)      |  | *  |
| Extended Key Usage (applic<br>Basic constraints | ation policies)      |  | *  |

13. Imposta la dimensione della chiave su 2048 e seleziona l'opzione per rendere esportabile la chiave privata.

La variabile della dimensione della chiave è determinata dalla CA, pertanto potrebbe essere necessaria una chiave di dimensione superiore. Potrebbero essere necessarie anche altre opzioni, come uno specifico algoritmo di hash (sha256). Regola tutte le opzioni richieste

Ì

# MOBOTIX HUB – Guida ai certificati - Installare i certificati per la comunicazione con il

| ertificate F | Properti | es           |                |                  |   | × |
|--------------|----------|--------------|----------------|------------------|---|---|
| General S    | Subject  | Extensions   | Private Key    | Signature        |   |   |
| Cryptog      | raphic S | Service Prov | ider           |                  |   | ۲ |
| Key opti     | ons      |              |                |                  |   | * |
| Set the ke   | ey lengt | h and expo   | rt options for | the private key. | 6 |   |
| Key size:    | 2048     |              |                |                  | * |   |
| Make         | private  | key exportal | ble            |                  | _ |   |
| Allow        | private  | key to be an | chived         |                  |   |   |
| Strong       | nrivate  | key protec   | tion           |                  |   |   |
|              |          | and house    |                |                  |   |   |
| Select H     | ash Alo  | orithm       |                |                  |   | * |
| Select Ha    | sh Algo  | prithm to be | used for this  | request          |   |   |
| Hash Alg     | orithm   | sha256       |                |                  | ~ |   |
|              |          |              |                |                  |   |   |
|              | gnature  | Format       |                |                  |   | * |
| Select Si    | -        |              |                |                  |   |   |
| Select Si    |          |              |                |                  |   |   |
| Select Si    |          |              |                |                  |   |   |
| Select Si    |          |              |                |                  |   |   |

- 14. A meno che la CA non richieda una firma, il passaggio successivo consiste nel fare clic su **OK.**
- 15. Una volta definite tutte le proprietà del certificato, fare clic su **Avanti** nella **procedura guidata** Registrazione certificati.

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

## 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.

| The following option | is describe the uses and validity period that apply to this ty | pe of certificate: |
|----------------------|--|--------------------|
| Key usage:           | Digital signature  |                    |
|                      | Key certificate signing  |                    |
| 1.6.4.6              | Key encipherment   |                    |
| Application polic    | ies:   |                    |
| Validity period (d   | lays):   |                    |
|                      |  | Properties         |
|                      |  | T to be the second |
|                      |  |                    |
|                      |  |                    |
|                      |  |                    |
|                      |  |                    |
|                      |  |                    |
|                      |  |                    |

16. Selezionare un percorso in cui salvare la richiesta di certificato e un formato. Individuare tale percorso e specificare un nome per il file .req. Il formato predefinito è base 64, tuttavia alcune CA richiedono il formato binario.

## MOBOTIX HUB – Guida ai certificati - Installare i certificati per la comunicazione con il

| 17. Fare clic su <b>Fine</b> .  |  |
|---|--|
|   | - 🗆 X  |
| Certificate Enrollment  |  |
| Where do you want to save the offline request?  |  |
| If you want to save a copy of your certificate request or want to process to your hard disk or removable media. Enter the location and name of yo click Finish. | the request later, save the request<br>our certificate request, and then |
| File Name:  |  |
| C:\Users\Administrator\Desktop\CSR6.1.21  | Browse   |
| File format:<br>Base 64<br>D Binary   |  |
|   |  |
|   | Finith Cancel  |

Viene generato un file .req, che è necessario utilizzare per richiedere un certificato firmato.

## 14.2 Carica il file .req per ricevere in cambio un certificato firmato

Ogni CA ha un processo diverso per il caricamento dei file .req al fine di ricevere in cambio un certificato firmato. Per informazioni sul recupero di un certificato firmato, fare riferimento alla documentazione della CA in uso.

Quando si lavora con il server mobile, si consiglia di utilizzare una CA di terze parti. Nella maggior parte delle situazioni di CA di terze parti, è necessario scaricare un file .ZIP ed estrarre il contenuto nel computer che ospita il server mobile.

Esistono diversi tipi di file che possono essere inclusi nel contenuto del file .ZIP estratto.

. CER o . I file CRT possono essere installati utilizzando un processo simile. Fare clic con il pulsante destro del mouse sul file e scegliere Installa certificato

dal menu di scelta rapida.

Nei passaggi seguenti viene utilizzato un file. CER da una CA interna.

La CA avrà bisogno del contenuto del file .req. Verrà richiesto di copiare l'intero testo del file .req, comprese le righe di inizio e fine, e di incollare il testo in un campo messo a disposizione presso un portale gestito dalla CA.

© MOBOTIX AG www.mobotix.com

Ì

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 50/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 50/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati XProtect<sup>®</sup>

1. Individuare il percorso del file .reg e aprirlo in Blocco note, quindi incollare il testo in un campo reso disponibile in un portale gestito dalla CA.

CSR6.1.21 - Notepad

X

File Edit Format View Help

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

MIIGBAYJKoZIhvcNAQcCoIIF9TCCBfECAQMxDzANBg1ghkgBZQMEAgEFADCCBEoG CCsGAQUFBwwcoIIEPASCBDgwggQ0MGQwYgIBAgYKKwYBBAGCNwoKATFRME8CAQAw AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QLTBBMDAwNDY3DB1JUC0wQTAw MDQ2N1xBZG1pbm1zdHJhdG9yDAdNTUMuRVhFMIIDxqCCA8ICAQEwgg07MIICowIB ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAgMAk10MRQwEgYDVQQHDAtNYXBsZSBH cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UECgwDTUpUMRYwFAYDVQQDDA1U ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7G1/ 5z1YrUGOo4dW1/b3o35rpcQQbyOUE0K1NWjaIy4YrRPM9HjhKReThbcSnxddj6eR Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ//Zi08bEPobLv8YnWieNDuw lkaJWWRx3mb1/Yz0f1bwZrKFT3nkrXY0FYmZ0R19W0J+Iin0BtziwiC8DHt+bxST nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9gC47RP9yMjyuuEtpdR9ERoR qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs18zBATRXkk/kRI+Po6cXNJp Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEAYI3DQIDMQ4WDDEwLjAuMTc3 NiMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/wQEAwICpDAdBgNVHQ4EFgQU vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCNxUUMTYwNAIBBQwLSVAtMEEw MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b3IMB01NQy5FWEUwZgYKKwYB BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFMAbwBmAHQAdwBh AHIAZQAgAEsAZQB5ACAAUwB0AG8AcgBhAGcAZQAgAFAAcgBvAHYAaQBkAGUAcgMB ADANBgkqhkiG9w0BAQsFAAOCAQEAqtKb5HCh2a1BD2QcKdFuhVQbNxg+G5wcVkZt 7bXdwVuzoAxd9BFd+uVy4D3TmvXtineT3GVWQbKJCcxRZeTKPBFnHG0SeaYupUrG cX4ySsKR1xGSuOhsfIVa/5NXiIYgYxMh1z3nt2CDw+RNqAp/1gLV2cLsui01y5ib 088po4/b9eiXV7A1DWFy7ecw/7Z20a07Sa00aRbwzGJ8He1IiVEjfyAt7KLoufAg LkeSaJtjokkJuGPdr+ykjfuCmIF4hSbcOxzVkPCQbiHOwSxDG1kqYHZ8Xru665Q6 0L7QgBXCc7tcecDieqbYmp50LJPpqEQDQiYjzg57j3eYIFNYYjAAMAAxggGLMIIB hwIBA4AUvruQxeU1yku5Cem3anpu1cbMEDAwDQYJYIZIAWUDBAIBBQCgSjAXBgkq hkiG9w0BC0MxCgYIKwYBB0UHDAIwLwYJKoZIhvcNAQkEMSIEICk1SKp5MUjMa+vr DU1UXU+V05r1F8bNdM0mDgYfmjCiMA0GCSqGSIb3DQEBAQUABIIBAEjqqe4GSGE4 oZQj0vbWrAP0Ab2u8epFm7ZIMZzsJSzR0z98m+R+1R2mCoqWC0SSafybJ701Jhly A3eqzDYxAu9p9drJft317sGAERE/i1D3BFvKZZQH0sz0JNRwDp3qByHHzVCULUEI JSOpYvI1s3S23ZYEed0Lp35Xy87378zLLGLpgGKTK4teav1IitUJwVCKikL47uyF uOY4XLagwI1WWALsPF1+5ZcVNZMvsgzsbuMEXvjBkFKyhMv49oisgFcLJ1AoMtWn 7Mbq8K6ckbKkVpuvmWThkVTp1W3hIS/i/J0X7c2unA25LxAC/P/LyWhPt/Vk/oqf 06jNaHC/zBQ=

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

Windows (CRLF Ln 1, Col 1 100%

2. Quando si riceve il certificato dalla CA, accedere alla cartella dei download (o alla posizione in cui si sceglie di archiviare la cartella nel computer), fare clic con il pulsante destro del mouse sul certificato e selezionare Installa certificato.

© MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 51/129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 51/129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati XProtect<sup>®</sup>

# MOBOTIX HUB – Guida ai certificati - Installare i certificati per la comunicazione con il

| ↓     ↓     ↓     ↓     Down       File     Home     S  | nloads<br>hare View |  |              |                      | - ×    |
|---|---------------------|--|--------------|----------------------|--------|
| < - · ↑ ↓   | This PC > Down      | lloads   | v Ö v        | earch Downloads      | Q      |
| E Desktop   | ^ Name              | ~  | Date modifie | ed Type              | Size   |
| <ul> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> </ul> | Certnew             | Open<br>Install Certificate<br>Edit with Notepad++<br>Share<br>Open with | E. 10021-12. | 23 PM Security Certi | ficate |
| Network   | ve                  | Give access to<br>Restore previous versio                                | >            |                      | >      |
| 1 item 1 item select  | ed 1.11 KB          | Send to  | >            |                      |        |

X

- 3. Accetta l'avviso di sicurezza, se visualizzato.
- 4. Selezionare questa opzione per installare il certificato per il computer locale e fare clic su Avanti.

| Welcome to the   | Certificate Import Wizard   |
|--|---|
| This wizard helps you copy<br>lists from your disk to a cer                                  | certificates, certificate trust lists, and certificate revocation tificate store.   |
| A certificate, which is issue<br>and contains information us<br>connections. A certificate s | d by a certification authority, is a confirmation of your identity<br>sed to protect data or to establish secure network<br>store is the system area where certificates are kept. |
| Store Location   |   |
| O Current User   |   |
| Local Machine  |   |
| To continue, click Next.   |   |
|  |   |
|  |   |

5. Scegliere un percorso di archiviazione, selezionare l'archivio certificati personali, quindi fare clic su Avanti.

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 52/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati - VMS Milestone XProtect® XProtect<sup>®</sup>

## MOBOTIX HUB - Guida ai certificati - Installare i certificati per la comunicazione con il

| 🗧 😸 Certificate Import Wizard   |                  |   |
|---|------------------|---|
| Certificate Store<br>Certificate stores are system areas where certificates are kept.   |                  | - 16  |
| Windows can automatcally select a certificate store, or you can     the certificate. <ul> <li>Automatically select the certificate store based on the typ</li> <li>Place all certificates in the following store</li> <li>Certificate store:</li> </ul> | e of certificate | Select Certificate Store ×<br>Select the certificate store you want to use. |
|   |                  | Show physical stores  |

6. Completare la procedura guidata Installa certificato.

## 14.3 Abilitare la crittografia sul server mobile

Una volta installato il certificato nel computer che ospita il server mobile, eseguire le operazioni seguenti.

- 1. Su un computer con un server mobile installato, aprire il **configuratore del server** da:
- Il menu Start di Windows
- Mobile Server Manager facendo clic con il pulsante destro del mouse sull'icona di Mobile Server Manager sulla barra delle applicazioni del computer
- 2. In Server Configurator, in Certificato multimediale per lo streaming mobile, attivare Encryption.
- 3. Fare clic su Seleziona certificato per aprire un elenco con nomi di soggetti univoci di certificati che dispongono di una chiave privata e che sono installati nel computer locale nell'archivio certificati di Windows.
- 4. Selezionare un certificato per crittografare la comunicazione del client MOBOTIX HUB Mobile e del client Web MOBOTIX HUB con il server mobile.

Selezionare **Dettagli** per visualizzare le informazioni dell'archivio certificati di Windows sul certificato selezionato. All'utente del servizio Mobile Server è stato concesso l'accesso alla chiave privata. È necessario che questo certificato sia considerato attendibile in tutti i client.

# MOBOTIX HUB – Guida ai certificati - Installare i certificati per la comunicazione con il

| Server Configurator |   |                    |         |
|---------------------|---|--------------------|---------|
| Encryption          | Encryption  |                    |         |
| legistering servers | It is recommended to secure communication with  | encryption. Learn  | more    |
| anguage selection   | Server certificate<br>Applies to: management server, recording server, failover s<br>collector              | server, data       |         |
|                     | Encryption: On  |                    |         |
|                     | Terrane .   | ~                  | Details |
|                     | Circulticate insteed by MS-Organization-P2P-Account[2021]. Expires 3/                                       | 8/2021             |         |
|                     | Mobile streaming media certificate<br>Applies to mobile and web clients that retrieve data stream<br>server | ns from the mobile |         |
|                     | Encryption: On  | 0                  |         |
|                     | Name  | ~                  | Details |
|                     | Certificane insued by Expires 5/3/212   | 1                  |         |
|                     |   |                    |         |
|                     |   |                    |         |

5. Fare clic su Applica.

Quando si applicano i certificati, il servizio Mobile Server viene riavviato.

Per ulteriori informazioni, è possibile visualizzare:

Video sul processo di Powershell.

Whitepaper sui certificati con il server mobile.

## 15 Installare certificati CA di terze parti o commerciali per la comunicazione con il server di gestione o il server di registrazione

I server di gestione e i server di registrazione non richiedono certificati CA di terze parti o commerciali attendibili per la crittografia, ma è possibile scegliere di utilizzare questi certificati se fa parte dei criteri di sicurezza e verranno automaticamente considerati attendibili dalle workstation e dai server client. Il processo è identico all'installazione del certificato di Mobile Server.

> Quando si configura la crittografia per un gruppo di server, è necessario abilitarla con un certificato appartenente allo stesso certificato CA oppure, se la crittografia è disabilitata, deve essere disabilitata in tutti i computer del gruppo di server.

I certificati emessi da CA (Certificate Authority) hanno una catena di certificati e alla radice di tale catena si trova il certificato radice CA. Quando un dispositivo o un browser vede questo certificato, confronta il suo certificato radice con quelli preinstallati sul sistema operativo (Android, iOS, Windows, ecc.). Se il certificato radice è elencato nell'elenco dei certificati preinstallati, il sistema operativo garantisce all'utente che la connessione al server sia sufficientemente sicura. Questi certificati vengono emessi per un nome di dominio e non

### 15.1 Aggiungere un certificato CA al server

1

Aggiungere il certificato CA al server effettuando le seguenti operazioni. Sul computer che ospita il server MOBOTIX HUB, aprire Microsoft Management Console.

I parametri specifici dipendono dalla CA. Fare riferimento alla documentazione della CA prima di procedere.

1. In Microsoft Management Console, dal menu File selezionare Aggiungi/Rimuovi snap-in....

| 📟 Run  |  | ×                            |
|--------|--|------------------------------|
| Ø      | Type the name of a program, folder, do<br>resource, and Windows will open it for | ocument, or Internet<br>you. |
| Onen:  | mmd  | ×                            |
| -phene |  |                              |

# MOBOTIX HUB – Guida ai certificati - Installare certificati CA di terze parti o

| 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. Selezionare lo snap-in Certificati e fare clic su Aggiungi.
- 3. Fare clic su **OK.**

|   | ~                   | Console Root                         | Edit Extensions        |
|---|---------------------|--------------------------------------|------------------------|
| Shap-In Vendor                                |                     | Certificates - Current Us            | er                     |
| Authorization Manager Microsoft Cor           |                     |                                      | Remove                 |
| Rertificate Templates Microsoft Cor           |                     |                                      |                        |
| Certificates Microsoft Cor                    |                     |                                      | Up etb.                |
| Certification Authority Microsoft Cor         |                     |                                      | Maria Court            |
| Component Services Microsoft Cor              | Add >               |                                      |                        |
| Device Manager Microsoft Cor                  |                     |                                      |                        |
| Disk Management Microsoft and                 |                     |                                      |                        |
| Enterprise PKI Microsoft Cor                  |                     |                                      |                        |
| Event Viewer Microsoft Cor                    |                     |                                      |                        |
| Group Policy Object Microsoft Cor             | ~                   |                                      | Advanced               |
| escription:                                   |                     |                                      |                        |
| The Certificates span-in allows you to browse | the contents of the | e certificate stores for vourself, a | service, or a computer |

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 56/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati Ws Descention of the second secon

4. Espandere l'oggetto Certificati. Fare clic con il pulsante destro del mouse sulla cartella Personale e selezionare Tutte le attività > Operazioni avanzate > Crea richiesta personalizzata.



- 5. Fare clic su Avanti nella procedura guidata Registrazione certificati e selezionare Procedi senza criteri di registrazione.
- 6. Fare clic su Avanti.

|   | ~    |
|---|------|
| _ | ~ ~  |
|   | <br> |

#### 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 |             |
|                                   |             |
|                                   |             |
|                                   |             |
|                                   |             |
|                                   |             |
|                                   |             |
|                                   |             |
|                                   |             |
|                                   | Next Cance  |
|                                   | ivext cance |

7. Selezionare il modello di chiave CNG (Nessun modello) e il formato di richiesta CMC, quindi fare clic su Avanti.

© MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 57/129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati - VMS Milestone XProtect® Guida ai certificati - VMS Milestone XProtect<sup>®</sup>

8. Espandere per visualizzare i **dettagli** della richiesta personalizzata e fare clic su **Proprietà**.

|                        | n the list below and configure the certificate options as req                             | uired.                |
|------------------------|---|-----------------------|
| Template:              | (No template) CNG key   |                       |
| 1                      | Suppress default extensions   |                       |
| Request format:        | O <u>P</u> KCS #10  |                       |
|                        | ● <u>C</u> MC.  |                       |
| option is specified in | not available for certificates based on a custom certificate<br>the certificate template. | request, even when th |
| option is specified in | not available for certificates based on a custom certificate<br>the certificate template. | request, even when th |

9. Nella scheda **Generale**, compila i campi **Nome descrittivo** e **Descrizione** con il nome di dominio registrato con la CA.

| Conoral  |          | -            |               | -                     |                      |        |
|----------|----------|--------------|---------------|-----------------------|----------------------|--------|
| General  | Subject  | Extensions   | Private Key   | Signature             |                      |        |
| A friend | dly name | and descript | ion will make | e it easier to identi | fy and use a certifi | icate. |
| Friendh  | / name:  |              |               |                       |                      |        |
| TestLa   | bDomain  | .com         |               |                       |                      |        |
| Descrip  | tion:    |              |               |                       |                      |        |
| TestLa   | bDomain  | .com         |               |                       |                      |        |
|          |          |              |               |                       |                      |        |
|          |          |              |               |                       |                      |        |
|          |          |              |               |                       |                      |        |
|          |          |              |               |                       |                      |        |
|          |          |              |               |                       |                      |        |
|          |          |              |               |                       |                      |        |
|          |          |              |               |                       |                      |        |
|          |          |              |               |                       |                      |        |
|          |          |              |               |                       |                      |        |
|          |          |              |               |                       |                      |        |
|          |          |              |               |                       |                      |        |
|          |          |              |               |                       |                      |        |
|          |          |              |               |                       |                      |        |
|          |          |              |               |                       |                      |        |
|          |          |              |               |                       |                      |        |

- 10. Nella scheda **Oggetto** immettere i parametri richiesti dalla CA specifica.
- 11. Ad esempio, il nome del soggetto **Tipo** e **Valore** sono diversi per ogni CA. Un esempio sono le seguenti informazioni obbligatorie:
- Nome comune:
- Organizzazione:
- Unità organizzativa :
- Città/Località:
- Stato/Provincia:
- Paese/Regione:

| ertificat                    | e Propert                            | ties  |                               |                              | >  |
|------------------------------|--------------------------------------|---|-------------------------------|------------------------------|--|
| General                      | Subject                              | Extensions                                    | Private Key                   | Signature                    |  |
| The sub<br>can ent<br>can be | oject of a<br>er inform<br>used in a | certificate is<br>ation about<br>certificate. | the user or c<br>the types of | omputer to w<br>subject name | which the certificate is issued. You<br>and alternative name values that                                       |
| Subject                      | of certifi                           | cate  |                               |                              |  |
| The use                      | er or com                            | puter that is                                 | receiving the                 | certificate                  |  |
| Subject                      | name:                                |   |                               |                              | The second s |
| Туре:                        |                                      |   |                               |                              | CN=Test for Docs   |
| Count                        | ny                                   | 4   |                               | Add:                         | OU=MJT Lab   |
| Value:                       |                                      |   | ×                             | Remove                       | L=Maple Grove<br>S=MN<br>C=USA   |
| Alterna                      | tive name                            | 2:  |                               |                              |  |
| Туре:                        |                                      |   |                               |                              | 1  |
| Direct                       | ory name                             | -   | -                             |                              |  |
| Value:                       |                                      |   |                               | Add >-                       |  |
|                              |                                      |   | ) <                           | Remiave                      |  |
|                              |                                      |   |                               |                              |  |
| _                            |                                      |   |                               |                              |  |
|                              |                                      |   |                               | OK                           | Cancel Apply   |

12. Alcune CA non richiedono estensioni. Tuttavia, se necessario, vai alla **scheda Estensioni** ed espandi il menu **Utilizzo chiavi**. Aggiungere le opzioni richieste dall'elenco Opzioni **disponibili** all' elenco **Opzioni selezionate**.

| ertificat        | te Propert        | ties           |               |                |                  |                                   |   | > |
|------------------|-------------------|----------------|---------------|----------------|------------------|-----------------------------------|---|---|
| General          | Subject           | Extensions     | Private Key   | Signature      |                  |                                   |   |   |
| The fol          | lowing ar         | e the certific | ate extension | ns for this ce | rtificate ty     | /pe.                              |   | ^ |
| Key us           | sage              |                |               |                |                  |                                   | * |   |
| The ke           | y usage e         | extension des  | cribes the pu | urpose of a d  | ertificate.      |                                   |   |   |
| Availat          | ble option        | ns:            |               |                | Select           | ed options:                       |   |   |
| CRL si<br>Data e | gning<br>ncipherm | ient           | <u> </u>      |                | Digita<br>Key ce | l signature<br>ertificate signing | 9 |   |
| Decipł           | ner only          |                | -             |                | Key er           | ncipherment                       |   |   |
| Enciph           | ner only          |                | A             | dd >           |                  |                                   |   |   |
| Key ag           | reement           | -              |               |                |                  |                                   |   |   |
|                  |                   |                |               |                |                  |                                   |   |   |
| ☑ Mak            | ke these k        | ey usages cr   | itical        |                |                  |                                   |   |   |
| Extend           | ded Key U         | lsage (applic  | ation policie | s)             |                  |                                   | ¥ | ĺ |
| Basic            | constrain         | ts             |               |                |                  |                                   | * |   |
|                  |                   |                |               |                |                  |                                   |   | V |
|                  |                   |                |               |                |                  |                                   |   |   |

13. Nella scheda **Chiave privata** espandere il menu **Opzioni chiave**.

Ì

14. Imposta la dimensione della chiave su 2048 e seleziona l'opzione per rendere esportabile la chiave privata.

La variabile della dimensione della chiave è determinata dalla CA, pertanto potrebbe essere necessaria una chiave di dimensione superiore. Potrebbero essere necessarie anche altre opzioni, come uno specifico algoritmo di hash (sha256). Regola tutte le opzioni richieste

| Certificate F | properti | ies          |                 |   |        | ×     |
|---------------|----------|--------------|-----------------|---|--------|-------|
| General S     | ubject   | Extensions   | Private Key     | Signature   |        |       |
| Cryptog       | raphic S | Service Prov | ider            |   |        | ۲     |
| Key optio     | ons      |              |                 |   |        | *     |
| Set the ke    | ey lengt | th and expo  | rt options for  | the private key.  |        |       |
| Key size:     | 2048     |              |                 |   |        |       |
| ☑ Make p      | orivate  | key exportal | ble             |   |        |       |
| Allow         | private  | key to be ar | chived          |   |        |       |
| Strong        | private  | key protec   | tion            |   |        |       |
|               |          |              |                 |   |        |       |
| Select Ha     | ash Alg  | orithm       |                 | and the second se |        | ^     |
| Select Ha     | sh Algo  | brithm to be | e used for this | request   |        |       |
| Hash Alg      | orithm   | sha256       |                 |   | ~      |       |
| Calact Si     |          | Format       |                 |   |        | i.    |
| SEIECE SI     | gnature  | romat        |                 |   |        |       |
|               |          |              |                 |   |        |       |
|               |          |              |                 |   | -      |       |
|               |          |              |                 | OK  | Cancel | Apply |

- 15. A meno che la CA non richieda una firma, il passaggio successivo consiste nel fare clic su **OK.**
- 16. Una volta definite tutte le proprietà del certificato, fare clic su **Avanti** nella **procedura guidata** Registrazione certificati.

| Click | k Next to use the options a | lready selected for this template, or click Details to cu | ustomize th  | e certifica |
|-------|-----------------------------|---|--------------|-------------|
| requ  | iest, and then click Next.  |   |              |             |
| R     | Custom request              | i) STATUS: Available                                      |              | Details     |
|       | The following options de    | scribe the uses and validity period that apply to this t  | ype of certi | ficate:     |
|       | Key usage:                  | Digital signature   |              |             |
|       |                             | Key certificate signing                                   |              |             |
|       | Application policies:       | Key encipherment  |              |             |
|       | Validity period (days)      |   |              |             |
|       |                             |   | P            | operties    |
|       |                             |   |              |             |

- 17. Selezionare un percorso in cui salvare la richiesta di certificato e un formato. Individuare tale percorso e specificare un nome per il file .req. Il formato predefinito è base 64, tuttavia alcune CA richiedono il formato binario.
- 18. Fare clic su Fine.

|   | - 🗆 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 p<br>to your hard disk or removable media. Enter the location and na<br>click Finish. | process the request later, save the request<br>me of your certificate request, and then |
| File Name:  |   |
| C:\Users\Administrator\Desktop\CSR6.1.21  | Browse  |
| File format:  |   |
| O Binary  |   |
|   |   |
|   |   |
|   |   |

Finish

Cancel

Viene generato un file .req, che è necessario utilizzare per richiedere un certificato firmato.

## 15.2 Carica il file .req per ricevere in cambio un certificato firmato



Nella maggior parte delle situazioni di CA di terze parti, è necessario scaricare un file .ZIP ed estrarre il contenuto sul computer che ospita il server MOBOTIX HUB.

Esistono diversi tipi di file che possono essere inclusi nel contenuto del file .ZIP estratto.

. CER o . I file CRT possono essere installati utilizzando un processo simile. Fare clic con il pulsante destro del mouse sul file e scegliere **Installa certificato** 

dal menu di scelta rapida.

5

Nei passaggi seguenti viene utilizzato un file . CER da una CA interna.

La CA avrà bisogno del contenuto del file .req. Verrà richiesto di copiare l'intero testo del file .req, comprese le righe di inizio e fine, e di incollare il testo in un campo messo a disposizione presso un portale gestito dalla CA.

1. Individuare il percorso del file .req e aprirlo in Blocco note, quindi incollare il testo in un campo reso disponibile in un portale gestito dalla CA.

CSR6.1.21 - Notepad

- 🗆 X

File Edit Format View Help ----BEGIN NEW CERTIFICATE REQUEST----MIIGBAYJKoZIhvcNAQcCoIIF9TCCBfECAQMxDzANBg1ghkgBZQMEAgEFADCCBEoG CCsGAQUFBwwcoIIEPASCBDgwggQ0MGQwYgIBAgYKKwYBBAGCNwoKATFRME8CAQAw AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QLTBBMDAwNDY3DB1JUC0wQTAw MDQ2N1xBZG1pbm1zdHJhdG9yDAdNTUMuRVhFMIIDxqCCA8ICA0Ewgg07MIICowIB ADBpM0wwCgYDV00GEwNVU0ExCzAJBgNVBAgMAk10MR0wEgYDV00HDAtNYXBsZSBH cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UECgwDTUpUMRYwFAYDVQQDDA1U ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7G1/ 5z1YrUG0o4dW1/b3o35rpcQQbyOUE0K1NWjaIy4YrRPM9HjhKReThbcSnxddj6eR Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ//Zi08bEPobLv8YnWieNDuw lkaJWWRx3mb1/Yz0f1bwZrKFT3nkrXY0FYmZ0R19W0J+Iin0BtziwiC8DHt+bxST nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9gC47RP9yMjyuuEtpdR9ERoR qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs18zBATRXkk/kRI+Po6cXNJp Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEAYI3DQIDMQ4WDDEwLjAuMTc3 NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/wQEAwICpDAdBgNVHQ4EFgQU vruQxeU1yku5Cem3anpu1cbMEDAwQwY3KwYBBAGCNxUUMTYwNAIBBQwLSVAtMEEw MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b3IMB01NQy5FWEUwZgYKKwYB BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwByAGYAdAAgAFMAbwBmAHQAdwBh AHIAZQAgAEsAZQB5ACAAUwB0AG8AcgBhAGcAZQAgAFAAcgBvAHYAaQBkAGUAcgMB ADANBgkqhkiG9w0BAQsFAAOCAQEAqtKb5HCh2a1BD2QcKdFuhVQbNxg+G5wcVkZt 7bXdwVuzoAxd9BFd+uVy4D3TmvXtineT3GVWQbKJCcxRZeTKPBFnHG0SeaYupUrG cX4ySsKR1xGSuOhsfIVa/5NXiIYgYxMh1z3nt2CDw+RNqAp/1gLV2cLsui01y5ib 088po4/b9eiXV7A1DWFy7ecw/7Z20a07Sa00aRbwzGJ8He1IiVEjfyAt7KLoufAg LkeSaJtjokkJuGPdr+ykjfuCmIF4hSbcOxzVkPCQbiHOwSxDG1kqYHZ8Xru665Q6 0L7QgBXCc7tcecDieqbYmp50LJPpqEQDQiYjzg57j3eYIFNYYjAAMAAxggGLMIIB hwIBA4AUvruQxeU1yku5Cem3anpu1cbMEDAwDQYJYIZIAWUDBAIBBQCgSjAXBgkg hkiG9w0BCQMxCgYIKwYBBQUHDAIwLwYJKoZIhvcNAQkEMSIEICk1SKp5MUjMa+vr DU1UXU+V05r1F8bNdM0mDgYfmjCiMA0GCSqGSIb3DQEBAQUABIIBAEjqqe4GSGE4 oZQj0vbWrAP0Ab2u8epFm7ZIMZzsJSzR0z98m+R+1R2mCoqWC0SSafybJ701Jh1y A3eqzDYxAu9p9drJft317sGAERE/i1D3BFvKZZQH0sz0JNRwDp3qByHHzVCULUEI JSOpYvI1s3S23ZYEedQLp35Xy87378zLLGLpgGKTK4teav1IitUJwVCKikL47uyF uOY4XLagwI1WWALsPF1+5ZcVNZMvsgzsbuMEXvjBkFKyhMv49oisgFcLJ1AoMtWn 7Mbg8K6ckbKkVpuvmWThkVTp1W3hIS/i/J0X7c2unA25LxAC/P/LyWhPt/Vk/ogf 06jNaHC/zBQ= -----END NEW CERTIFICATE REQUEST-----

81

Windows (CRLF Ln 1, Col 1 100%

2. Quando si riceve il certificato dalla CA, accedere alla cartella dei download (o alla posizione in cui si sceglie di archiviare la cartella nel computer), fare clic con il pulsante destro del mouse sul certificato e selezionare **Installa certificato**.

| ↓     ↓     ↓     ↓     Down       File     Home     S   | nloads<br>hare View |  |            |           | Ţ              | □ ×      |
|--|---------------------|--|------------|-----------|----------------|----------|
| < - ·↑↓,   | This PC > Down      | loads  | 5 V        | Search Do | wnloads        | <i>p</i> |
| E Desktop  | ^ Name              | ~  | Date modi  | fied      | Туре           | Size     |
| <ul> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>Local Disk (C:)</li> </ul> | Certnew             | Open<br>Install Certificate<br>Edit with Notepad++<br>Share<br>Open with | ן יראמ דיז | 2:23 PM   | Security Certi | ficate   |
| 🚽 Network  | v e                 | Give access to<br>Restore previous version                               | \$         |           |                | ,        |
| 1 item 1 item select   | ed 1.11 KB          | Send to  | >          |           |                |          |

3. Accetta l'avviso di sicurezza, se visualizzato.

Certificate Import Wizard

4. Selezionare questa opzione per installare il certificato per il computer locale e fare clic su Avanti.

| This wizard helps you copy certificates<br>ists from your disk to a certificate stor   | , certificate trust lists, and certificate revocation<br>e.   |
|--|---|
| A certificate, which is issued by a certi<br>and contains information used to prote<br>connections. A certificate store is the | fication authority, is a confirmation of your identity<br>act data or to establish secure network<br>system area where certificates are kept. |
| Store Location   |   |
| O Current User   |   |
| Local Machine  |   |
| To continue, click Next.   |   |
|  |   |
|  |   |
|  |   |

X

5. Scegliere un percorso di archiviazione, selezionare l'archivio certificati personali, quindi fare clic su Avanti.

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 66/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati XProtect<sup>®</sup>

| ÷ | 🔄 Certificate Import Wizard   |   |
|---|---|---|
|   | Certificate Store<br>Certificate stores are system areas where certificates are kept.<br>Windows can automatically select a certificate store, or you can specify a location for<br>the certificate |   |
|   | Automatically select the certificate store based on the type of certificate     Place all certificates in the following store     Certificate store:     Browse                                     | Select Certificate Store X<br>Select the certificate store you want to use. |

6. Completare la procedura guidata Installa certificato.

## 15.3 Abilitare la crittografia da e verso il server di gestione

È possibile crittografare la connessione bidirezionale tra il server di gestione e l'agente di raccolta dati affiliato quando si dispone di un server remoto del tipo seguente:

- Server di registrazione
- Server degli eventi
- Server di registro
- Server LPR
- Mobile Server

Se il sistema contiene più server di registrazione o server remoti, è necessario abilitare la crittografia su tutti di essi.

## 15.3.1 Prerequisiti:

1

Quando si configura la crittografia per un gruppo di server, è necessario abilitarla con un certificato appartenente allo stesso certificato CA oppure, se la crittografia è disabilitata, deve essere disabilitata in tutti i computer del gruppo di server.

Un certificato di autenticazione del server è considerato attendibile nel computer che ospita il server di gestione Innanzitutto, abilitare la crittografia nel server di gestione.

Passi:

- 7. Su un computer con un server di gestione installato, aprire Server **Configurator** da:
- Il menu Start di Windows

0

- Management Server Manager facendo clic con il pulsante destro del mouse sull'icona Management Server Manager sulla barra delle applicazioni del computer
- 1. Nel Server Configurator, in Certificato server, attivare Encryption.
- 2. Fare clic su Seleziona certificato per aprire un elenco con nomi di soggetti univoci di certificati che dispongono di una chiave privata e che sono installati nel computer locale nell'archivio certificati di Windows.
- 3. Selezionare un certificato per crittografare la comunicazione tra il server di registrazione, il server di gestione, il server di failover e il server dell'agente di raccolta dati.
- 4. Selezionare **Dettagli** per visualizzare le informazioni dell'archivio certificati di Windows sul certificato selezionato.

| Milestone Server Configurator |  | ~        |       |
|-------------------------------|--|----------|-------|
| ncryption                     | Encryption   |          |       |
| egistering servers            | It is recommended to secure communication with encryption.   | Learn mo | ore   |
| Language selection            | Server certificate<br>Applies to: management server, recording server, failover server, data<br>collector, api gateway, log server |          |       |
|                               | Encryption: Off (  |          |       |
|                               | Select certificate   | ~        |       |
|                               | No certificate selected  |          |       |
|                               | Streaming media certificate<br>Applies to clients and servers that retrieve data streams from the record<br>server                 | ling     |       |
|                               | Encryption: Off (  |          |       |
|                               | Select certificate   | ~        |       |
|                               | No certificate selected  |          |       |
|                               | Mobile streaming media certificate<br>Applies to mobile and web clients that retrieve data streams from the n<br>server            | nobile   |       |
|                               | Encryption: Off (  |          |       |
|                               | Select certificate   | ~        |       |
|                               | No certificate selected  |          |       |
|                               |  |          | Apply |

5. Fare clic su Applica.

Per completare l'abilitazione della crittografia, il passaggio successivo consiste nell'aggiornare le impostazioni di crittografia in ogni server di registrazione e in ogni server che dispone di un agente di raccolta dati (server eventi, server di registro, server LPR e server mobile). Installare Servizi certificati Active Directory

Servizi certificati Active Directory è un prodotto Microsoft che esegue funzionalità di infrastruttura a chiave pubblica (PKI). Funge da ruolo server che consente di costruire un'infrastruttura a chiave pubblica (PKI) e di fornire crittografia a chiave aperta, autenticazione computerizzata e funzionalità avanzate di contrassegno per l'associazione.

In questo documento, Servizi certificati Active Directory viene utilizzato durante l'installazione dei certificati:

- In un ambiente di dominio (vedere Installazione di certificati in un dominio per la comunicazione con il server di gestione o il server di registrazione a pagina 86)
- In un ambiente di gruppo di lavoro (vedere Installazione dei certificati in un ambiente di gruppo di lavoro per la comunicazione con il server di gestione o il server di registrazione a pagina 104)

## 15.3.2 Per installare Servizi certificati Active Directory:

1. Nell'applicazione Server Manager selezionare Gestisci > Aggiungi ruoli e funzionalità. © MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 69/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati - VMS Milestone XProtect® Guida ai certificati - VMS Mileston

|                               | A CONTRACTOR OF |                       |                      | -               | 2000   |      |  |
|-------------------------------|---|-----------------------|----------------------|-----------------|--|------|--|
| Server M                      | anager • Dashboard  |                       | • ©   ľ              | Manage<br>Add R | Tools View<br>oles and Features                  | Help |  |
| Dashboard                     | WELCOME TO SERVER MANAGER   | R                     |                      | Remo<br>Add S   | ve Roles and Feature<br>ervers                   | 5    |  |
| Local Server     All Servers  |   | oficiure this local s | ra this local conver |                 | Create Server Group<br>Server Manager Properties |      |  |
| ■ File and Storage Services ▷ | QUICK START   | inigure this local si | erver                |                 | initiager (Topenies                              |      |  |

- 2. In Prima di iniziare, fare clic su Avanti.
- 3. In Tipo di installazione, selezionare Installazione basata sui ruoli o sulle funzionalità, quindi fare clic su Avanti.
- 4. In Selezione server, selezionare il server locale come destinazione per l'installazione e fare clic su Avanti
- 5. In Ruoli server selezionare il ruolo Servizi certificati Active Directory. Esamina l'elenco delle funzionalità da installare e fai clic su Aggiungi funzionalità.



- 6. Fare clic su **Avanti**.
- 7. In Funzionalità, fare clic su Avanti. Tutte le funzioni richieste sono selezionate per l'installazione.
- In Servizi certificati Active Directory leggere la descrizione dei servizi certificati Active Directory e fare 8. clic su Avanti.

© MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 70/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati - VMS Milestone XProtect® Guida ai certificati ai XProtect<sup>®</sup>

- 9. In Servizi ruolo selezionare l'opzione seguente:
  - Autorità di certificazione
  - Servizio Web dei criteri di iscrizione alle certificazioni
  - Servizio Web Iscrizione Certificazioni
  - Registrazione Web dell'Autorità di certificazione
  - Servizio Registrazione dispositivi di rete

Quando si seleziona ognuno dei servizi ruolo, aggiungere le funzionalità necessarie per supportare l'installazione di ogni servizio.

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

- 10. Fare clic su **Avanti**.
- 11. In **Conferma**, selezionare **Riavvia automaticamente il server di destinazione, se necessario**, e fare clic su **Installa**.

- 12. Al termine dell'installazione, fare clic sul **pulsante Chiudi**.
- 13. Selezionare il flag di notifica nell'applicazione Server Manager.



- 14. Un messaggio per iniziare la configurazione post-distribuzione è elencato sotto il flag di notifica.
- 15. Clicca sul link per iniziare la configurazione dei servizi installati.

|    | • 🕲 I 🧗  |
|----|--|
| Å. | Post-deployment Configura  |
|    | Configuration required for Active Directory<br>Certificate Services at IP-0A000467 |
|    | Configure Active Directory Certificate Services on thus                            |
| 0  | Feature installation   |
|    | Configuration required. Installation succeeded on IP-0A000467.                     |
|    | Add Roles and Features   |
|    | Task Details   |

- 16. Viene avviata la configurazione guidata di Servizi certificati Active Directory.
- 17. In **Credenziali** selezionare l'account utente necessario per eseguire i servizi installati. Come indicato nel testo, è richiesta l'appartenenza ai gruppi amministratore locale e amministratore dell'organizzazione.
- 18. Immettere le informazioni sull'account richieste e fare clic su Avanti.
| AD CO COMINGUIAUON |  |              |                 |              |          |             |
|--------------------|--|--------------|-----------------|--------------|----------|-------------|
| Credentials        |  |              |                 | DESTINA      | TION SER | VER<br>)450 |
| Credentials        | Specify credentials to configure   | role serv    | vices           |              |          |             |
| Role Services      | T. 1. (10.4) - 2. (10.1)   |              |                 |              |          |             |
|                    | Standalone certification authority     Certification Authority Web Enrollment     Online Responder   | elong to the | e local Adminis | trators grou | p:       |             |
|                    | To install the following role services you must be   | elong to the | Enterprise Ad   | lmins group: |          |             |
|                    | <ul> <li>Enterprise certification authority</li> <li>Certificate Enrollment Policy Web Service</li> <li>Certificate Enrollment Web Service</li> <li>Network Device Enrollment Service</li> </ul> |              |                 |              |          |             |
|                    | Credentials: IP-0A000450\Administrator   |              | Change          |              |          |             |
|                    |  |              |                 |              |          |             |
|                    | More about AD CS Server Roles  |              |                 |              |          |             |
|                    |  |              |                 |              |          |             |

- 19. In **Servizi ruolo**, selezionare i seguenti servizi:
  - Autorità di certificazione
  - Registrazione Web dell'Autorità di certificazione
- 20. Fare clic su **Avanti**.

| Role Services   |   | DESTINAT | IP-0A000 | VER<br>450 |
|---|---|----------|----------|------------|
| Credentials   | Select Role Services to configure   |          |          |            |
| Role Services<br>Setup Type<br>CA Type<br>Private Key<br>Cryptography<br>CA Name<br>Validity Period<br>Certificate Database<br>Confirmation | <ul> <li>Certification Authority</li> <li>Certification Authority Web Enrollment</li> <li>Online Responder</li> <li>Network Device Enrollment Service</li> <li>Certificate Enrollment Web Service</li> <li>Certificate Enrollment Policy Web Service</li> </ul> |          |          |            |
|   | More about AD CS Server Roles   |          |          |            |

21. In Tipo di installazione, selezionare l' opzione CA autonoma e fare clic su Avanti.

| etup Type  | DESTINATION SERVE<br>IP-0A00045   |
|--|---|
| Credentials<br>Role Services<br>Setup Type                           | Specify the setup type of the CA<br>Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to<br>simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage |
| CA Type<br>Private Key<br>Cryptography<br>CA Name<br>Validity Period | certificates.  Enterprise CA Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.  Standalone CA   |
| Certificate Database<br>Confirmation                                 | 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. In **Tipo di CA** selezionare l'opzione per installare una **CA radice** e fare clic su **Avanti**.

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

23. n Chiave privata, selezionare l'opzione per creare una nuova chiave privata e fare clic su Avanti.

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

24. In **Crittografia** selezionare **RSA#Microsoft Software Key Storage Provider** per l'opzione del provider di crittografia con una **lunghezza della chiave** di 2048 e un algoritmo hash SHA256.

Fare clic su **Avanti**.

| Tryptography fo  | or CA  |            | DESTINATIO  | OA000450 |
|--|--|------------|-------------|----------|
| Credentials<br>Role Services<br>Setup Type<br>CA Type              | Specify the cryptographic options<br>Select a cryptographic provider:<br>RSA#Microsoft Software Key Storage Provider | ¥.         | Key length: |          |
| Private Key  | Select the hash algorithm for signing certificates issued by   | this CA:   |             |          |
| CA Name<br>Validity Period<br>Certificate Database<br>Confirmation | SHA256<br>SHA384<br>SHA512<br>SHA1<br>MD5  | accessed b | by the CA.  |          |
|  | More about Cryptography  |            |             |          |

25. In Nome CA, immettere il nome della CA e fare clic su Avanti.

Per impostazione predefinita, il nome è "localhost-CA", presupponendo che il nome del computer del server locale sia "localhost".

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

26. In Periodo di validità, selezionare il periodo di validità predefinito di 5 anni e fare clic su Avanti.

| 📥 AD CS Configuration                      |                  |                      |                          |                         | $\leftarrow$        |          | ×           |
|--|------------------|----------------------|--------------------------|-------------------------|---------------------|----------|-------------|
| Validity Period                            |                  |                      |                          |                         | DESTINA             | TION SEF | VER<br>0450 |
| Credentials<br>Role Services<br>Setup Type | Spec<br>Select t | ify the validit      | y period                 | erated for this certifi | cation authority (C | CA):     |             |
| СА Туре                                    | 5                | Years                | *                        |                         |                     |          |             |
| Private Key                                | CA exp           | iration Date: 4/27/2 | 2026 3:27:00 PM          |                         |                     |          |             |
| Cryptography                               | The val          | idity period configu | ured for this CA certifi | cate should exceed      | the validity period | for the  |             |
| CA Name                                    | certifica        | ates it will issue.  |                          |                         |                     |          |             |
| Validity Period                            |                  |                      |                          |                         |                     |          |             |
| Certificate Database                       | 1                |                      |                          |                         |                     |          |             |
| Confirmation                               |                  |                      |                          |                         |                     |          |             |
|  |                  |                      |                          |                         |                     |          |             |
|  |                  |                      |                          |                         |                     |          |             |
|  | More a           | bout Validity Period | 1                        |                         |                     |          |             |
|  |                  |                      | < Previous               | Next >                  | Configure           | Canc     | el          |

- 27. In Database certificati immettere i percorsi del database e del database di registro. I percorsi predefiniti del database per l'archivio certificati sono: C:\\\\\system32\Certlog
- 28. Fare clic su Avanti.
- 29. In Conferma, esaminare le opzioni di configurazione selezionate e fare clic su Configura per avviare il processo di configurazione.
- 30. Al termine della configurazione, fare clic su Chiudi.
- 31. Quando viene richiesto di configurare eventuali servizi ruolo aggiuntivi, fare clic su No.
- 32. Riavviare il server locale per assicurarsi che sia pronto per essere utilizzato come server di certificazione Active Directory.

## 15.4 Installare i certificati in un dominio per la comunicazione con il server di gestione o il server di registrazione

Quando gli endpoint client e server operano tutti all'interno di un ambiente di dominio, non è necessario distribuire i certificati CA alle workstation client. Criteri di gruppo all'interno del dominio gestisce la distribuzione automatica di tutti i certificati CA attendibili a tutti gli utenti e i computer del dominio. Ciò è dovuto al fatto che, quando si installa una CA radice dell'organizzazione, vengono utilizzati Criteri di gruppo per propagare il certificato all' archivio certificati Autorità di certificazione radice attendibili per tutti gli utenti e i computer del dominio.

Per installare una CA radice dell'organizzazione, è necessario essere un amministratore di dominio o un amministratore con accesso in scrittura ad Active Directory.

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 80/129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati XProtect<sup>®</sup>

Microsoft fornisce una documentazione completa per i sistemi operativi Windows Server, che include modelli per i certificati server, l'installazione della CA e la distribuzione dei certificati è disponibile in Panoramica della distribuzione dei certificati server di Microsoft.

#### 15.4.1 Aggiungere un certificato CA al server

Ì

Aggiungere il certificato CA al server effettuando le seguenti operazioni.

1. Sul computer che ospita il server MOBOTIX HUB, aprire Microsoft Management Console.

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

2. In Microsoft Management Console, dal menu File selezionare Aggiungi/Rimuovi snap-in....

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

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 81/129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati - VMS Milestone XProtect® XProtect<sup>®</sup>

3. Selezionare lo snap-in Certificati e fare clic sullosnap-in Aggiungi certificati, quindi selezionare Account

| allable shaphins,     |               |         | Selected snap-ins:       |                 |
|-----------------------|---------------|---------|--------------------------|-----------------|
| inap-in               | Vendor        | ^       | Console Root             | Edit Extensions |
| ActiveX Control       | Microsoft Cor |         | Certificates (Local Comp | uter)           |
| Authorization Manager | Microsoft Cor |         |                          | venove.         |
| Certificates          | Microsoft Cor |         |                          |                 |
| Component Services    | Microsoft Cor |         |                          | (d)sid!!!       |
| Computer Managem      | Microsoft Cor |         |                          |                 |
| Device Manager        | Microsoft Cor | a did a |                          | Mays Days       |
| Disk Management       | Microsoft and | Adds    | 2                        |                 |
| Event Viewer          | Microsoft Cor |         |                          |                 |
| Folder                | Microsoft Cor |         |                          |                 |
| Group Policy Object   | Microsoft Cor |         |                          |                 |
| Internet Informatio   | Microsoft Cor |         |                          |                 |
| IP Security Monitor   | Microsoft Cor |         |                          |                 |
| IP Security Policy M  | Microsoft Cor |         |                          | Advanced        |
| 5                     |               | × .     |                          |                 |
| sciptori.             |               |         |                          |                 |

computer.

| Certificates snap-in  | ×      |
|---|--------|
| This snap in will always manage certificates for:   |        |
| O My user account   |        |
| O Service account   |        |
| Computer account  |        |
|   |        |
|   |        |
|   |        |
|   |        |
|   |        |
|   |        |
|   |        |
|   |        |
|   |        |
|   |        |
| Contraction of the second s | Next a |

- 4. In Seleziona computer selezionare Computer locale.
- 5. Selezionare Fine, quindi OK.

| elect Computer                               |                       | > |
|--|-----------------------|---|
| Select the computer you want this snap-in to | o manage.             |   |
| This snap-in will always manage:             |                       |   |
| Local computer: (the computer this computer) | onsole is running on) |   |
| O Another computer:                          | Evolution             |   |
| and there a her ease we are reader.          |                       |   |
|  |                       |   |
|  |                       |   |

Model FLAG www.filopoux.com Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 83/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati - VMS Milestone XProtect® Guida ai certificati - VMS Milestone XP XProtect<sup>®</sup>

- 6. Espandere l'oggetto Certificati. Fare clic con il pulsante destro del mouse sulla **cartella Personale** e selezionare **Tutte le attività > Operazioni avanzate > Crea richiesta personalizzata**.
- 7. Fare clic su Avanti nella procedura guidata Registrazione certificati e selezionare Procedi senza criteri di registrazione.

Se i Criteri di gruppo contengono già un criterio di registrazione dei certificati, è consigliabile confermare il resto di questo processo con il team di amministrazione del dominio prima di procedere.

8. Fare clic su Avanti.

Ì

9. Selezionare il modello di chiave CNG (Nessun modello) e il formato di richiesta CMC, quindi fare clic

| ÷ | X |
|---|---|
|   |   |

#### Certificate Enrollment

#### Select Certificate Enrollment Policy

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

| Configured by you  | Add New     |
|--|-------------|
| Custom Request   |             |
| Proceed without enrollment policy  |             |
|  |             |
|  |             |
|  |             |
|  |             |
|  |             |
|  |             |
|  |             |
|  | Next Cancel |
| 🤉 🔤 Nellove Veskop<br>a 🔁 Certificate Enrollment Requests  |             |
| <ul> <li>Image: Signal Structure State State</li></ul> |             |
| Insted Root Certification Authorities     Instead Devices  |             |
| Web Hosting     Windows Live ID Token Issuer     Windows Care II of the Sequence   |             |
| 3 Windowsserverupdateservices  |             |
|  |             |
|  |             |
|  |             |

su **Avanti**.

© MOBOTIX AG www.mobotix.com Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 84/ 129Guida ai certificati - VMS Milestone XProtect®Guida ai certificati Guida ai certificati - VMS Milestone XProtect®Guida ai certificati - VMS Milestone XPro 10. Espandere per visualizzare i **dettagli** della richiesta personalizzata e fare clic su **Proprietà**. 

-

| Chose an option fron                            | n the list below and configure the certificate options as requ                              | iired.               |
|---|---|----------------------|
| Template:                                       | (No template) CNG key   |                      |
|   | <u>Suppress default extensions</u>  |                      |
| Request format:                                 | ○ <u>P</u> KCS #10  |                      |
|   | ● <u>CMC</u>  |                      |
| Note: Key archival is<br>option is specified in | not available for certificates based on a custom certificate r<br>the certificate template. | equest, even when th |
|   |   |                      |
|   |   | Next C               |

11. Nella scheda Generale compilare i campi Nome descrittivo e Descrizione con il nome di dominio, il nome del computer o l'organizzazione.

| ertificat | e Propent | 165          |               |                      |                    |          |
|-----------|-----------|--------------|---------------|----------------------|--------------------|----------|
| General   | Subject   | Extensions   | Private Key   | Signature            |                    |          |
| A friend  | lly name  | and descript | ion will make | e it easier to ident | ify and use a cert | ificate. |
| Friendly  | name:     |              |               |                      |                    |          |
| TestLa    | Domain,   | .com         |               |                      |                    |          |
| Descrip   | tion:     |              |               |                      |                    |          |
| TestLa    | Domain.   | .com         |               |                      |                    |          |
|           |           |              |               |                      |                    |          |
|           |           |              |               |                      |                    |          |
|           |           |              |               |                      |                    |          |
|           |           |              |               |                      |                    |          |
|           |           |              |               |                      |                    |          |
|           |           |              |               |                      |                    |          |
|           |           |              |               |                      |                    |          |
|           |           |              |               |                      |                    |          |
|           |           |              |               |                      |                    |          |
|           |           |              |               |                      |                    |          |
|           |           |              |               |                      |                    |          |
|           |           |              |               |                      |                    |          |
|           |           |              |               |                      |                    |          |
|           |           |              |               |                      |                    |          |

12. Nella scheda **Oggetto**, immettere i parametri necessari per il nome del soggetto.

In Tipo di nome soggetto, immettere in **Nome comune** il nome host del computer in cui verrà installato il certificato.

13. Nella scheda Estensioni espandere il menu Utilizzo chiavi esteso (criteri dell'applicazione). Aggiungere l'autenticazione server dall'elenco delle opzioni disponibili.

| The following are the cer   | tificate extensions for this                 | certificate type.                               | 6         |
|---|--|---|-----------|
| Key usage   |  |   | ~         |
|   |  |   |           |
| Extended Key Usage (ap  | oplication policies)                         |   | ~         |
| certificate can be used.<br>certificates issued by thi<br>Available options:  | Select the application polic<br>is template. | cy required for valid sign<br>Selected options: | atures of |
| Code Signing<br>Secure Email<br>Time Stamping<br>Microsoft Trust List Sign<br>Microsoft Time Stampin<br>IP security end system<br>IP security tunnel termin<br>IP security user | Add ><br>Add ><br>Add >                      | ]<br>]<br>с ш                                   | 2         |
| Make the Extended K   | ey Usage critical                            |   |           |

- 14. Nella scheda Chiave privata espandere il menu Opzioni chiave.
- 15. Imposta la dimensione della chiave su 2048 e seleziona l'opzione per rendere esportabile la chiave privata. Fare clic su **OK.**

| Certificate Pro | operti | es           |               |                  |        | ×     |
|-----------------|--------|--------------|---------------|------------------|--------|-------|
| General Sub     | oject  | Extensions   | Private Key   | Signature        |        |       |
| Cryptogra       | phic S | ervice Prov  | ider          |                  |        | ٣     |
| Key option      | ns     |              |               |                  |        | *     |
| Set the key     | lengt  | h and expor  | t options for | the private key. |        |       |
| Key size:       | 2048   |              |               | *                |        |       |
| Make pr         | ivate  | key exportal | ble           |                  |        |       |
| Allow pr        | ivate  | key to be ar | chived        |                  |        |       |
| □ Strong n      | rivate | key protect  | tion          |                  |        |       |
|                 | marc   | nel proces   |               |                  |        |       |
| Select Has      | h Ala  | orithm       |               |                  |        |       |
| Select Hash     | Algo   | rithm to be  | used for this | request          |        |       |
| Hash Algor      | rithm: | sha256       |               |                  | ~      |       |
|                 |        |              |               |                  |        |       |
| Select Sign     | nature | Format       |               |                  |        | v     |
|                 |        |              |               |                  |        |       |
|                 |        |              |               |                  |        |       |
|                 |        |              |               |                  |        |       |
|                 |        |              |               | OK               | Cancel | Apply |

- 16. Una volta definite tutte le proprietà del certificato, fare clic su **Avanti** nella **procedura guidata** Registrazione certificati.
- 17. Selezionare un percorso in cui salvare la richiesta di certificato e un formato. Individuare tale percorso e specificare un nome per il file .req. Il formato predefinito è base 64.
- 18. Fare clic su **Fine**.

| Castificate 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<br>to your hard disk or removable media. Enter the location and nar<br>click Finish. | process the request later, save the request of your certificate request, and ther |
| File Name:   | Rowse   |
| C. (Scister and the state of the skip (CSR) ALL  | E Drowsca.  |
| File format:   |   |
|  |   |
| O Binary   |   |
| () Binary  |   |
| () Binary  |   |
| O Binary   |   |
| O Binary   |   |

Viene generato un file .req, che è necessario utilizzare per richiedere un certificato firmato.

## 15.4.2 Carica il file .req per ricevere in cambio un certificato firmato

È necessario copiare l'intero testo del file .req, incluse le righe iniziale e finale, e incollare il testo nell' autorità di certificazione interna di Servizi certificati Active Directory nella rete. Vedere Installazione di Servizi certificati Active Directory a pagina 74.

A meno che il dominio non abbia installato Servizi certificati Active Directory solo di recente o non

sia stato installato solo per questo scopo, sarà necessario inviare questa richiesta

seguendo una procedura separata configurata dal team di amministrazione del dominio.

Si prega di confermare questo processo con loro prima di procedere.

1. Individua la posizione del file .req e aprilo in Blocco note.

Ì

|  |   | ^  |
|--|---|--|
| File Edit Format View Help   |   |  |
| BEGIN NEW CERTIFICATE REQU   | EST   |  |
| IIIF2AYJKoZIhvcNAQcCoIIFyTCCBcU  | CAQMxDzANBg1ghkgBZQMEAgEFADCCBB4  | G  |
| CsGAQUFBwwCoIIEEASCBAwwggQIMGY   | wZAIBAgYKKwYBBAGCNwoKATFTMFECAQA  | w  |
| wIBATFHMEUGCSsGAQQBgjcVFDE4MDY   | CAQUMDENsdXN0ZXIxVEVNUAwaQ0xVU1R  | F  |
| jFURU1QXEFkbWluaXN0cmF0b3IMB01   | NQy5FWEUwggOYoIID1AIBATCCA40wggJ  | 1  |
| gEAMBcxFTATBgNVBAMMDENsdXN0ZXI   | xVEVNUDCCASIwDQYJKoZIhvcNAQEBBQA  | D  |
| gEPADCCAQoCggEBAKVp0982yi05tcn   | ypaTujsFBe9jwOyRp+c5N00xf8OcN0Dy  | g  |
| IVMVTSU9s9rTMWmUDzP+zLumOmC6gCW  | Io5RgiT+dLjOvq+Z6AUWC1H+WVUsaVbJ  | c  |
| ZktV8ut805gi46dkQ4MD71btX6mnjjU  | B294Xwf8yUVP1Be0dkfqjUVnn6EAYzHd  | s  |
| zczK1yUZmY576IBwf6LZMujXbNDD5ZX  | zdhG3pggarNdzHvg0RIJvro4IJ0rM6Es  | 3  |
| IN2d0SZms4Utj21DekFde3BsENvcvk0  | /PHZk8b8Bww050+ya3tk7jDbvw0a1VXE  | 9  |
| pqL+Zy4pEP1jKnTwM1IyPmsXyw7gx6C  | rTw8ntqECAwEAAaCCAS8wHAYKKwYBBAG  | C  |
| W@CAzEOFgwxMC4wLjE0MzkzLjIwRQY   | JKwYBBAGCNxUUMTgwNgIBBQwMQ2x1c3R  | 1  |
| jFURU1QDBpDTFVTVEVSMVRFTVBcQWR   | taW5pc3RyYXRvcgwHTU1DLkVYRTBgBgk  | q  |
| 1kiG9w0BCQ4xUzBRMBMGA1UdJQQMMAo  | GCCsGAQUFBwMBMBsGCSsGAQQBgjcVCgQ  | 0  |
| 1AwwCgYIKwYBBQUHAwEwHQYDVR00BBY  | EFOBsTd6/Hpi6c18h5HHa88hWc911MGY  | G  |
| and the second   |   |  |
| isGAQQBgjcNAgIxWDBWAgEAHk4ATQB   | pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB  | 0  |
| isGAQQBgjcNAgIxWDBWAgEAHk4ATQB<br>AHcAYQByAGUAIABLAGUAeQAgAFMAdAB  | pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>vAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB  | 0<br>1   |
| CisGAQQBgjcNAgIxWDBWAgEAHk4ATQB<br>AHcAYQByAGUAIABLAGUAeQAgAFMAdAB<br>AHIDAQAwDQYJKoZIhvcNAQELBQADggEI   | pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>vAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn  | 0<br>1<br>N  |
| CisGAQQBgjcNAgIxWDBWAgEAHk4ATQB<br>AHcAYQByAGUAIABLAGUAeQAgAFMAdAB<br>AHIDAQAwDQYJKoZIhvcNAQELBQADggEI<br>DAPtDKNDGskV/dq6rqgpYEKiQfWZeSno   | pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgBu<br>vAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>dEOzxieJtES/1I5hmVUm51TIVydzE8iy   | 0<br>1<br>N<br>W   |
| CisGAQQBgjcNAgIxWDBWAgEAHk4ATQB<br>AHcAYQByAGUAIABLAGUAeQAgAFMAdAB<br>AHIDAQAwDQYJKoZIhvcNAQELBQADggE<br>DAPtDKNDGskV/dq6rqgpYEKiQfWZeSn<br>KjUze/+WIiZifGFnkMKYwrzKgx7qIr   | pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>vAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>dEOzxieJtES/1IShmVUm51TIVydzE8iy<br>Undo  |  |
| CisGAQQBgjcNAgIxWDBWAgEAHk4ATQB<br>AHcAYQByAGUAIABLAGUAeQAgAFMAdAB<br>AHIDAQAwDQYJKoZIhvcNAQELBQADggEl<br>DAPtDKNDGskV/dq6rqgpYEKiQfWZeSn<br>KjUze/+WIiZifGFnkMKYwrzKgx7qIr<br>m3dWazix8dSVOQIRZ3Lr7yXg9iiF49  | pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgBu<br>vAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>dEOzxieJtES/1I5hmVUm51TIVydzE8iyu<br>Undo  | 0<br>1<br>N<br>W<br>L                                    |
| LisGAQQBgjcNAgIxWDBWAgEAHk4ATQB<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdAB<br>AHIDAQAwDQYJKoZIhvcNAQELBQADggE<br>DAPtDKNDGskV/dq6rqgpYEKiQfWZeSn<br>(jUze/+WIiZifGFnkMKYwrzKgx7qIr)<br>adWazix8dSVOQIRZ3Lr7yXg9iiF49<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aHe  | pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0<br>vAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>dEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo<br>Cut  | 0 I N W L j D  |
| isGAQQBgjcNAgIxWDBWAgEAHk4ATQB<br>AHcAYQByAGUAIABLAGUAeQAgAFMAdAB<br>AHIDAQAwDQYJKoZIhvcNAQELBQADggE<br>OAPtDKNDGskV/dq6rqgpYEKiQfWZeSnc<br>(jUze/+WIiZifGFnkMKYwrzKgx7qIr<br>BdWazix8dSVOQIRZ3Lr7yXg9iiF49<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aHe<br>FP4XCYYiuyw/+iHqyNca2fvIIm8Hpb0  | pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>vAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>dEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo<br>Cut<br>Copy   | 0<br>1<br>N<br>W<br>L<br>j<br>d<br>B                     |
| LisGAQQBgjcNAgIxWDBWAgEAHk4ATQB<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdAB<br>AHIDAQAwDQYJKoZIhvcNAQELBQADggE<br>DAPtDKNDGskV/dq6rqgpYEKiQfWZeSno<br>(jUze/+WIiZifGFnkMKYwrzKgx7qIr<br>adWazix8dSVOQIRZ3Lr7yXg9iiF49<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aHe<br>[p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0<br>LzCCAYcCAQ0AF0BsTd6/Hpi6c18h5H   | pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0<br>vAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>dEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo<br>Cut<br>Copy<br>Paste   | 0<br>1<br>N<br>W<br>L<br>j<br>j<br>j<br>j<br>j<br>s<br>v |
| LisGAQQBgjcNAgIxWDBWAgEAHk4ATQB<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdAB<br>AHIDAQAwDQYJKoZIhvcNAQELBQADggE<br>DAPtDKNDGskV/dq6rqgpYEKiQfWZeSn<br>(jUze/+WIIZifGFnkMKYwrzKgx7qIr)<br>adWazix8dSVOQIRZ3Lr7yXg9iiF49<br>X7yVZFyEAs/6uoApcKXc2KPgBP8aHe<br>[p4XCYYiuyw/+iHqyNca2fvIIm8Hpb]<br>LzCCAYcCAQOAF0BsTd6/Hpi6c18h5H<br>WYJKoZIhvcNAQkDMQoGCCsGAQUFBw   | pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0<br>vAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>dEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo<br>Cut<br>Copy<br>Paste<br>Delete   | 0<br>1<br>N<br>W<br>L<br>j<br>d<br>3<br>V<br>L           |
| LisGAQQBgjcNAgIxWDBWAgEAHk4ATQB<br>AHcAYQByAGUAIABLAGUAeQAgAFMAdAB<br>AHIDAQAwDQYJKoZIhvcNAQELBQADggE<br>DAPtDKNDGskV/dq6rqgpYEKiQfWZeSno<br>(jUze/+WIiZifGFnkMKYwrzKgx7qIr)<br>n3dWazix8dSVOQIRZ3Lr7yXg9iiF49<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aHe<br>[p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0<br>izCCAYcCAQOAFOBsTd6/Hpi6c18h5H<br>FwYJKoZIhvcNAQkDMQoGCCsGAQUFBw<br>DY6dr8BzietMf5QwmoRNzq8MRGSQiN1  | pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>vAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>dEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo<br>Cut<br>Copy<br>Paste<br>Delete  | 01NWEj03VEV-   |
| isGAQQBgjcNAgIxWDBWAgEAHk4ATQB<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdAB<br>AHIDAQAwDQYJKoZIhvcNAQELBQADggE<br>OAPtDKNDGskV/dq6rqgpYEKiQfWZeSn<br>(jUze/+WIiZifGFnkMKYwrzKgx7qIr<br>13dWazix8dSVOQIRZ3Lr7yXg9iiF49-<br>X7yVZFyEAs/6uoApcKXc2KPgBP8aHe<br>P4XCYYiuyw/+iHqyNca2fvIIm8Hpb0<br>zCCAYcCAQOAFOBsTd6/Hpi6c18h5H<br>WYJKoZIhvcNAQkDMQoGCCsGAQUFBw<br>OY6dr8BzietMf5QwmoRNzq8MRGSQiN1<br>-q73I6NKKLzg7ROhm16Xj7tL4Id2iV  | pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>vAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnd<br>dEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo<br>Cut<br>Copy<br>Paste<br>Delete<br>Select All   | 01NWLj03vLv=   |
| isGAQQBgjcNAgIxWDBWAgEAHk4ATQB<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdAB<br>AHDAQAwDQYJKoZIhvcNAQELBQADggE<br>APtDKNDGskV/dq6rqgpYEKiQfWZeSn<br>(jUze/+WIIZifGFnkMKYwrzKgx7qIr<br>adWazix8dSVOQIRZ3Lr7yXg9iiF49<br>X7yVZFyEAs/6uoApcKXc2KPgBP8aHe<br>p4XCYYiuyw/+iHqyNca2fvIIm8Hpb<br>zCCAYcCAQOAFOBsTd6/Hpi6c18h5H<br>WYJKoZIhvcNAQkDMQoGCCsGAQUFBw<br>)Y6dr8BzietMf5QwmoRNzq8MRGSQiN<br>q73I6NKKLzg7ROhm16Xj7tL4Id2iV<br>WR7EktvnBLYuBQVPGYb+gwd8EfBh9  | pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>vAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnd<br>dEOzxieJtES/115hmVUm51TIVydzE8iyU<br>Undo<br>Cut<br>Copy<br>Paste<br>Delete<br>Select All<br>Right to left Reading order   | 01NWEj33vEv= <   |
| LisGAQQBgjcNAgIxWDBWAgEAHk4ATQB<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdAB<br>AHIDAQAwDQYJKoZIhvcNAQELBQADggE<br>DAPtDKNDGskV/dq6rqgpYEKiQfWZeSn<br>(jUze/+WIiZifGFnkMKYwrzKgx7qIr)<br>n3dWazix8dSVOQIRZ3Lr7yXg9iiF49-<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aHe<br>[p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0<br>izCCAYcCAQOAFOBsTd6/Hpi6c18h5H<br>FwYJKoZIhvcNAQkDMQoGCCsGAQUFBw<br>DY6dr8BzietMf5QwmoRNzq8MRGSQiN1<br>eq73I6NKKLzg7ROhm16Xj7tL4Id2iV<br>LWR7EktvnBLYuBQVPGYb+gwd8EfBh9<br>r+5Z7i0E2HZpsBrS1d1+u89F0Pi+W/a   | pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>vAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnd<br>dEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo<br>Cut<br>Copy<br>Paste<br>Delete<br>Select All<br>Right to left Reading order  | 01NWEjðsvEv=kJu  |
| LisGAQQBgjcNAgIxWDBWAgEAHk4ATQB<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdAB<br>AHDAQAwDQYJKoZIhvcNAQELBQADggE<br>DAPtDKNDGskV/dq6rqgpYEKiQfWZeSn<br>(jUze/+WIiZifGFnkMKYwrzKgx7qIr)<br>n3dWazix8dSVOQIRZ3Lr7yXg9iiF49-<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aHe<br>[p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0<br>LzCCAYcCAQOAFOBsTd6/Hpi6c18h5HF<br>wYJKoZIhvcNAQkDMQoGCCsGAQUFBw<br>DY6dr8BzietMf5QwmoRNzq8MRGSQiN1<br>-q73I6NKKLzg7ROhm16Xj7tL4Id2iV<br>LWR7EktvnBLYuBQVPGYb+gwd8EfBh9<br>+5Z7i0E2HZpsBrSld1+u89F0Pi+W/a<br>117k+ce+EDOHhXkbSD+fHYFbUqaTV  | pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>vAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnd<br>dEOzxieJtES/1I5hmVUm51TIVydzE8iyd<br>Undo<br>Cut<br>Copy<br>Paste<br>Delete<br>Select All<br>Right to left Reading order<br>Show Unicode control characters  | 0 1 N W L j J 3 V I V = K J J a                          |
| LisGAQQBgjcNAgIxWDBWAgEAHk4ATQB<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdAB<br>AHIDAQAwDQYJKoZIhvcNAQELBQADggE<br>DAPtDKNDGskV/dq6rqgpYEKiQfWZeSn<br>(jUze/+WIIZifGFnkMKYwrzKgx7qIr)<br>n3dWazix8dSVOQIRZ3Lr7yXg9iiF49<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aHe<br>[p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0<br>izCCAYcCAQOAFOBsTd6/Hpi6c18h5H<br>EwYJKoZIhvcNAQkDMQoGCCsGAQUFBw<br>DY6dr8BzietMf5QwmoRNzq8MRGSQiN<br>eq73I6NKKLzg7ROhm16Xj7tL4Id2iV<br>LWR7EktvnBLYuBQVPGYb+gwd8EfBh9<br>r+5Z7i0E2HZpsBrS1d1+u89F0Pi+W/a<br>nIi7k+ce+EDoHhXkbSD+fHYFbUqaTY<br>2PmPVkUJGJEUMwfo8rb4xb9taP6ycU   | pAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>vAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>BAFGoQLCtyivOXGOT0U4MS9VnUSOsQUnd<br>dEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo<br>Cut<br>Copy<br>Paste<br>Delete<br>Select All<br>Right to left Reading order<br>Show Unicode control characters<br>Insert Unicode control character →             | 01NWE josveve ve vjjs                                    |
| LisGAQQBgjcNAgIxWDBWAgEAHk4ATQB<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdAB<br>AHDAQAwDQYJKoZIhvcNAQELBQADggE<br>DAPtDKNDGskV/dq6rqgpYEKiQfWZeSn<br>(jUze/+WIiZifGFnkMKYwrzKgx7qIr)<br>adWazix8dSVOQIRZ3Lr7yXg9iiF49<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aHe<br>p4XCYYiuyw/+iHqyNca2fvIIm8Hpb0<br>LzCCAYcCAQOAFOBsTd6/Hpi6c18h5H<br>FwYJKoZIhvcNAQkDMQoGCCsGAQUFBw<br>DY6dr8BzietMf5QwmoRNzq8MRGSQiN1<br>eq73I6NKKLzg7ROhm16Xj7tL4Id2iV<br>LWR7EktvnBLYuBQVPGYb+gwd8EfBh9<br>r+SZ7i0E2HZpsBrS1d1+u89F0Pi+W/a<br>Li7k+ce+EDoHhXkbSD+fHYFbUqaTYU<br>PmPVkUJGJEUMwfo8rb4xb9taP6ycUI<br>8XTFWM0JCPMykW2<br>END_NEW_CERITCICATE_PEOUE | PAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>vAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>BAFGoQLCtyivOXG0T0U4MS9VnUS0sQUnd<br>dEOzxieJtES/1IShmVUm51TIVydzE8iy<br>Undo<br>Cut<br>Copy<br>Paste<br>Delete<br>Select All<br>Right to left Reading order<br>Show Unicode control characters<br>Insert Unicode control character ><br>Open IME | 01NWLj03VLV= <jj3< td=""></jj3<>                         |

- 2. Copia l'intero contenuto del file. Sono incluse le linee tratteggiate che segnano l'inizio e la fine della richiesta di certificato.
- 3. Apri un browser web e inserisci l'indirizzo della CA del dominio.

| S Microsoft Active Directory Certii × +                          | o - 🗆 ×      |
|--|--------------|
| ← → C ▲ Not secure   10.0.4,103/certsrv/                         | 🕁 🚨 Update 🕴 |
| Microsoft Active Directory Certificate Services - IP-0A000467-CA | Home         |

#### Welcome

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

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

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

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

- 4. Fai clic sul link Richiedi un certificato.
- 5. Fare clic sul collegamento di richiesta avanzata del certificato.

| 0           | Micr                    | osoft A                   | ctive D                     | irectory Certif          | ×      | +       |      |       |        |         |
|-------------|-------------------------|---------------------------|-----------------------------|--------------------------|--------|---------|------|-------|--------|---------|
| 4           | ÷                       | C                         | A                           | Not secure               | 10.0   | 0.4.103 | cer  | srv/o | certro | jus.asj |
| Micr        | osof                    | t Active                  | Direc                       | ctory Certifica          | te Ser | vices - | - IP | -0A0  | 0046   | 7-CA    |
|             |                         |                           |                             |                          |        |         |      |       |        |         |
| Req         | uest                    | t a Ce                    | ertific                     | cate                     |        |         |      |       |        |         |
| Req<br>Sele | uest<br>ect th          | t a Ce<br>le cer          | ertifica                    | c <b>ate</b><br>te type: |        | _       |      |       |        |         |
| Req<br>Sele | uest<br>ect th<br>Veb I | t a Ce<br>le cer<br>Brows | ertifica<br>tifica<br>ser C | te type:<br>ertificate   |        |         |      |       |        | _       |

Or, submit an advanced certificate request.

6. Incolla il contenuto del file .req nel modulo. Se è necessario selezionare un modello di certificato, selezionare

Server Web dall'elenco Modello di certificato.

| Microsoft Active  | Directory Certificate Serv  | vices - CLUSTER2TEMP-CA   | Home   |
|---|---|---|--|
| ubmit a Cer   | tificate Request or F   | Renewal Request   |  |
| o submit a sa<br>enewal reque   | ived request to the C<br>st generated by an e   | CA, paste a base-64-encoded CMC or PKCS #<br>external source (such as a Web server) in the s                                    | #10 certificate request or PKCS #7<br>Saved Request box. |
| ase-64-encodec<br>ertificate reques<br>CMC or<br>'KCS #10 or<br>'KCS #7): | 1WR7EktvnBLYuBQVPG<br>r+527iOE2HZpaBrSid<br>nIi7k+ce+EDoHhXkbS<br>2PmPVkUJGJEUMwfo8r<br>TSXTFWMOJCPMykW2<br>END NEW CERTI | SYD+gwd3EfBh9K9Qgvd5fMu:<br>11+u89F0P1+W/a8/YV7BhA1,<br>5D+fHYFbUqaTYDfgU4u5Pg6;<br>rb4xb9taP6ycUZwieLrNWw3]<br>IFICATE REQUEST |  |
| dditional Attrib  | utes:   |   |  |
|   |   | 3   |  |
| Attributes  | 1.5   | 2   |  |

7. Fai clic su Invia.

Il sito mostra un messaggio che indica che il certificato verrà emesso entro pochi giorni.

Il team di amministrazione del dominio probabilmente distribuirà e installerà il certificato per l'utente. Tuttavia, se il certificato viene consegnato all'utente, è possibile installarlo manualmente.

## 15.5 Installare il certificato manualmente

Se il certificato ti viene consegnato, puoi installarlo manualmente.

- 1. Individuare il file del certificato sul computer che ospita il server di gestione o il server di registrazione.
- 2. Fare clic con il pulsante destro del mouse sul certificato e selezionare Installa certificato.
- 3. Accetta l'avviso di sicurezza, se visualizzato.
- 4. Selezionare questa opzione per installare il certificato per l'utente corrente e fare clic su Avanti.

Scegliere un percorso di archiviazione, selezionare l'archivio certificati personali, quindi fare clic su Avanti.

×

| Certificate Import Wi | izard |
|-----------------------|-------|
|-----------------------|-------|

## 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.

| •               |  |  |
|-----------------|--|--|
| Ourrent User    |  |  |
| O Local Machine |  |  |

To continue, click Next.

|  | Next | Cancel |
|--|------|--------|
|--|------|--------|

| Certificate Store   |                                |  |
|---|--------------------------------|--|
| Certificate stores are system areas where certificates are kept.  |                                |  |
| Windows can automatically select a certificate store, or you can specify<br>the certificate.<br>Automatically select the certificate store based on the type of ce<br>Place all certificates in the following store | y a location for<br>ertificate | Select Certificate Store<br>Select the certificate store you want to use.  |
| Certificate store:  | Browse                         | Personal<br>Trusted Root Certification Authorities<br>Enterprise Trust<br>Intermediate Certification Authorities<br>Trusted Publishers<br>Untrusted Certificates |
|   |                                | Show physical stores   |

- 5. Completare la procedura guidata Installa certificato.
- 6. Passare allo snap-in Certificati di Microsoft Management Console (MMC).
- 7. Nella console passare all'archivio personale in cui è installato il certificato. Fare clic con il pulsante destro del mouse sul certificato e selezionare Tutte le attività > Gestisci chiavi private.

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

| 🗧 🔿 🙍 💼 🔏 🛍 🗶 🖻 🔒 🛛   |           |             |   |                 |
|---|-----------|-------------|---|-----------------|
| Console Root  | Issued To | ~           | Issued By   | Expiration      |
| <ul> <li>Gettificates (Local Computer)</li> <li>Personal</li> </ul>   | Cluster17 | Open        | CLUSTER2TEMP-CA   | 10/26/202       |
| <ul> <li>Trusted Root Certification Authoritie</li> </ul>   |           | All Tasks   | > Open  |                 |
| <ul> <li>Enterprise Trust</li> <li>Intermediate Certification Authoritie</li> <li>Trusted Publishers</li> </ul> |           | Cut<br>Copy | Request Certificate with N<br>Renew Certificate with Ne | ew Key<br>w Key |
| > 🛄 Untrusted Certificates  |           | Delete      | Manage Private Keys                                     |                 |
| <ul> <li>Ihird-Party Root Certification Author</li> <li>Certificates</li> </ul>                                 |           | Properties  | Advanced Operations                                     | >               |
| Trusted People  |           | Help        | Export  |                 |

- 8. Verificare che l'account che esegue il software MOBOTIX HUB Management Server, Recording Server o Mobile Server sia presente nell'elenco degli utenti autorizzati a utilizzare il certificato.
- 9. Assicurati che l'utente abbia abilitato sia il controllo completo che le autorizzazioni di lettura.

Per impostazione predefinita, il software MOBOTIX HUB utilizza l'account NETWORK SERVICE. In un ambiente di dominio , gli account di servizio vengono comunemente utilizzati per installare ed eseguire i servizi MOBOTIX HUB . Sarà necessario discuterne con il team di amministrazione del dominio e aggiungere le autorizzazioni appropriate agli account del servizio se non è già stato configurato correttamente. Conferma

# 15.5.1 Abilitare la crittografia del server per i server di gestione e i server di registrazione

Una volta installato il certificato con le proprietà e le autorizzazioni corrette, eseguire le operazioni seguenti.

- 10. Su un computer in cui è installato un server di gestione o un server di registrazione, aprire il configuratore server da:
  - Il menu Start di Windows
    - 0
  - Il gestore del server, facendo clic con il pulsante destro del mouse sull'icona del gestore del server sulla barra delle applicazioni del computer
- 11. Nel Server Configurator, in Certificato server, attivare Encryption.
- 12. Fare clic su Seleziona certificato per aprire un elenco con nomi di soggetti univoci di certificati che dispongono di una chiave privata e che sono installati nel computer locale nell'archivio certificati di Windows.
- 13. Selezionare un certificato per crittografare la comunicazione tra il server di registrazione, il server di gestione, il server di failover e il server di raccolta dati.
- 14. Selezionare **Dettagli** per visualizzare le informazioni dell'archivio certificati di Windows sul certificato selezionato.

All'utente del servizio Recording Server è stato concesso l'accesso alla chiave privata. È necessario che questo certificato sia attendibile su tutti i client.

| Server Configurator |  | -                |         | > |
|---------------------|--|------------------|---------|---|
| Encryption          | Encryption   |                  |         |   |
| Registering servers | It is recommended to secure communication with encryption  | . <u>Learn n</u> | nore    |   |
| anguage selection   | Server certificate<br>Applies to: management server, recording server, failover server, data<br>collector  |                  |         |   |
|                     | Encryption: On   | 0                |         |   |
|                     | Sectors.   | ý.               | Details |   |
|                     | Camblicate issued by MS-Grganization-P2P-Actess (2021), Espires 3/8/2021   |                  |         |   |
|                     | Streaming media certificate<br>Applies to clients and servers that retrieve data streams from the record<br>server   | ding             |         |   |
|                     | Encryption: On   | 0                |         |   |
|                     | And the second s | ÷                | Details |   |
|                     | Certificate instead by MS-Degarization-PDP-Access [2023], http://www.S20/2023-   |                  |         |   |
|                     |  |                  |         |   |
|                     |  |                  |         |   |
|                     |  |                  |         |   |
|                     |  |                  |         |   |
|                     |  |                  | Annalis |   |
|                     |  |                  | Арру    |   |

#### 15. Fare clic su Applica.

Quando si applicano i certificati, il server di registrazione viene arrestato e riavviato. L'arresto del servizio Server di registrazione significa che non è possibile registrare e visualizzare video in diretta durante la verifica o la modifica della configurazione di base del server di

## 16 Installare i certificati in un ambiente di gruppo di lavoro per la comunicazione con il server di gestione o il server di registrazione

Quando si opera in un ambiente di gruppo di lavoro, si presume che non sia presente un'infrastruttura dell'autorità di certificazione. Per distribuire i certificati, è necessario creare un'infrastruttura dell'autorità di certificazione. È inoltre necessario distribuire le chiavi del certificato alle workstation client. Ad eccezione di questi requisiti, il processo di richiesta e installazione di un certificato in un server è simile allo scenario di dominio e CA commerciale.

#### 16.1 Aggiungere un certificato CA al server

Aggiungere il certificato CA al server effettuando le seguenti operazioni.

16. Sul computer che ospita il server MOBOTIX HUB, aprire Microsoft Management Console.

| 😅 Run         |  | ×                         |
|---------------|--|---------------------------|
| Ð             | Type the name of a program, folder, docures or the second se | ument, or Internet<br>ou. |
| <u>O</u> pen: | mmd  | ×                         |
|               | OK Cancel  | <u>B</u> rowse            |

17. In Microsoft Management Console, dal menu File selezionare Aggiungi/Rimuovi snap-in....

| Console1 - [Console Root]  File Action View Favorites Window H  New Ctrl+N | Help                                     | - U X        |
|--|--|--------------|
| Open Ctrl+O  | Name                                     | Actions      |
| Save Ctrl+S  | There are no items to show in this view. | Console Root |
| Save As  |  | More Actions |
| Options Ctri+M   |  |              |
| Recent File  |  |              |
| Exit   |  |              |
|  |  |              |

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 97/129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati - VMS Milestone XProtect® Guida ai certificati - VMS Milestone XProtect<sup>®</sup>

- 18. Selezionare lo snap-in Certificati e fare clic su Aggiungi.
- 19. Fare clic su OK.

|                       |               | - |       |                               | 1                |
|-----------------------|---------------|---|-------|-------------------------------|------------------|
| ap-in                 | Vendor        | 1 |       | Console Root                  | Edit Extensions. |
| ActiveX Control       | Microsoft Cor |   |       | Certificates (Local Computer) | Domesti          |
| Authorization Manager | Microsoft Cor | 1 |       |                               | Nemove.          |
| Certificates          | Microsoft Cor | Ξ |       |                               |                  |
| Component Services    | Microsoft Cor |   |       |                               | Move Up          |
| Computer Managem      | Microsoft Cor |   |       |                               |                  |
| Device Manager        | Microsoft Cor | П | -     |                               | Moye Down        |
| Disk Management       | Microsoft and |   | A00 > |                               |                  |
| Event Viewer          | Microsoft Cor |   |       |                               |                  |
| Folder                | Microsoft Cor |   |       |                               |                  |
| Group Policy Object   | Microsoft Cor |   |       |                               |                  |
| Internet Informatio   | Microsoft Cor |   |       |                               |                  |
| Internet Informatio   | Microsoft Cor |   |       |                               |                  |
| IP Security Monitor   | Microsoft Cor |   |       |                               | Advanced         |
| IP Security Policy M  | Microsoft Cor | ~ |       |                               | Rovancean        |
| motion:               |               |   |       |                               |                  |
| np boin.              |               | _ |       |                               |                  |

20. Espandere l'oggetto Certificati. Fare clic con il pulsante destro del mouse sulla cartella Personale e selezionare Tutte le attività > Operazioni avanzate > Crea richiesta personalizzata.

| Console Root     | - Current User               | Object T | Type<br>ficates                   |   |
|------------------|------------------------------|----------|-----------------------------------|---|
| Tn               | Find Certificates            |          |                                   |   |
| En 📄 En          | All Tasks                    | >        | Find Certificates                 |   |
| Ac               | View<br>New Window from Here | ,        | Request New Certificate<br>Import |   |
| Th               | New Taskpad View             |          | Advanced Operations               | Create Custom Request                             |
| Tri<br>Cli<br>Ce | Refresh<br>Export List       |          |                                   | Enroll On Behalf Of<br>Manage Enrollment Policies |
| s 📄 Sn           | Help                         |          |                                   |   |

- 21. Fare clic su Avanti nella procedura guidata Registrazione certificati e selezionare Procedi senza criteri di registrazione.
- 22. Fare clic su Avanti.

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 98/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificati - VMS Milestone XProtect® Guida ai certificati ai XProtect<sup>®</sup>

23. Selezionare il modello di chiave CNG (Nessun modello) e il formato di richiesta CMC, quindi fare clic

Certificate Enrollment

Select Certificate Enrollment Policy

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

| Configured by you                 | Add New     |
|-----------------------------------|-------------|
| Custom Request                    |             |
| Proceed without enrollment policy |             |
|                                   |             |
|                                   |             |
|                                   |             |
|                                   |             |
|                                   |             |
|                                   |             |
|                                   |             |
|                                   |             |
|                                   |             |
|                                   | Next Cancel |

su **Avanti**.

## MOBOTIX HUB – Guida ai certificati - Installare i certificati in un ambiente di gruppo di

24. Espandere per visualizzare i **dettagli** della richiesta personalizzata e fare clic su **Proprietà**.

| Certificate Information  |  |                         |
|--|--|-------------------------|
| Click Next to use the options already<br>request, and then click Next. | selected for this template, or click Details to cu | ustomize the certificat |
| Custom request   | i) STATUS: Available                               | Details                 |
| The following options describe   | the uses and validity period that apply to this t  | ype of certificate:     |
| Key usage:<br>Application policies:                                    |  |                         |
| Validity period (days):  |  | -                       |
|  |  | Properties              |
|  |  | -                       |
|  |  |                         |
|  |  |                         |
|  |  |                         |

25. Nella scheda **Generale** compilare i campi **Nome descrittivo** e **Descrizione** con il nome di dominio, il nome del computer o l'organizzazione.

# MOBOTIX HUB – Guida ai certificati - Installare i certificati in un ambiente di gruppo di

| Ceneral outro                    | . Fidework     | Deixe te Verst | Carabia                             |                  |           |
|----------------------------------|----------------|----------------|-------------------------------------|------------------|-----------|
| A friendly name<br>Friendly name | e and descript | ion will make  | signature<br>e it easier to identif | y and use a cert | tificate. |
| TestLabDoma                      | in.com         |                |                                     |                  |           |
| Description:                     |                |                |                                     |                  |           |
| TestLabDoma                      | in.com         |                |                                     |                  |           |
|                                  |                |                |                                     |                  |           |
|                                  |                |                |                                     |                  |           |

- 26. Nella scheda **Oggetto**, immettere i parametri necessari per il nome del soggetto.
- 27. In Tipo di nome soggetto, immettere in **Nome comune** il nome host del computer in cui verrà installato il certificato.

| General  | Subject   | Extensions   | Private Key                                    | Signature                                   |   |
|--|---|--|--|---|---|
| The sub<br>can ent<br>can be<br>Subject<br>The use | er inform<br>used in a<br>of certific<br>or or comp | certificate is<br>ation about<br>certificate.<br>cate<br>puter that is | the user or c<br>the types of<br>receiving the | omputer to w<br>subject name<br>certificate | hich the certificate is issued. You<br>and alternative name values that |
| Subject  | name:   |  | - i  |   | CN-MIT-12A  |
| Type:  | _   |  | 1 1  |   | CINE NO I-IZA   |
| Comn   | non name  | E  |  | 400 *                                       |   |
| Value  |   |  |  | Remove                                      |   |
| Alternal   | tive name   | e -  | 1  |   | [   |
| Type:  | and and an  |  |  |   | ·   |
| Direct   | ory name  |  |  |   |   |
| Value:   |   |  |  | ≤bbA  |   |
|  |   |  | E.   | Remove                                      |   |
| Direct<br>Value:                                   | ory name  |  |  | Add ><br>Remove                             |   |

28. Nella scheda Estensioni espandere il menu Utilizzo chiavi esteso (criteri dell'applicazione). Aggiungere l'autenticazione server dall'elenco delle opzioni disponibili.

| General   | Subject  | Extensions  | Private Key                               | Signature                        |  |   |                  |   |
|---|--|---|---|----------------------------------|--|---|------------------|---|
| The foll  | owing an   | e the certific                                    | ate extension                             | s for this cer                   | tificate type                          |   |                  | ^ |
| Key us  | age  |   |   |                                  |  |   | Ŷ                |   |
| Extend  | led Key U  | sage (applic                                      | ation policies                            | s)                               |  |   | ~                |   |
| An app<br>certific<br>certific<br>Availab                                       | lication p<br>ate can b<br>ates issue<br>ble option  | oolicy (called<br>e used. Selec<br>ed by this ter | l enhanced k<br>ct the applica<br>nplate. | ey usage in V<br>ition policy re | Vindows 200<br>equired for<br>Selected | 00) defines<br>valid signat<br>options: | how a<br>ures of |   |
| Code S<br>Secure<br>Time S<br>Micros<br>Micros<br>IP secu<br>IP secu<br>IP secu | igning<br>Email<br>tamping<br>oft Trust<br>oft Time<br>urity end s<br>urity tunn<br>urity user | List Signii<br>Stamping<br>system<br>el termina   | A R                                       | dd ><br>emove                    |  |   |                  |   |
| Mak   | ii the Exte  | ended Key U                                       | sage critical                             |                                  | < III                                  |   | 2                |   |
|   |  |   |   |                                  |  |   |                  | ~ |

- 29. Nella scheda Chiave privata espandere il menu Opzioni chiave.
- 30. Imposta la dimensione della chiave su 2048 e seleziona l'opzione per rendere esportabile la chiave privata. Fare clic su **OK.**

## MOBOTIX HUB – Guida ai certificati - Installare i certificati in un ambiente di gruppo di

|  | Propert                                      | ies   |               |                  |   | > |
|--|--|---|---------------|------------------|---|---|
| General S                                      | Subject                                      | Extensions                                    | Private Key   | Signature        |   |   |
| Cryptog  | raphic                                       | Service Prov                                  | ider          |                  |   | ۷ |
| Key opti                                       | ions   |   |               |                  |   | * |
| Set the ke                                     | ey lengt                                     | th and expo                                   | t options for | the private key. |   |   |
| Key size:                                      | 2048   |   |               | ~                |   |   |
| Make   | private                                      | key exportal                                  | ble           |                  |   |   |
| Allow  | private                                      | key to be ar                                  | chived        |                  |   |   |
| <br>Strong                                     | , private                                    | e kev protec                                  | tion          |                  |   |   |
|  |  |   |               |                  |   |   |
|  |  |   |               |                  |   |   |
| Select H                                       | lash Alq                                     | orithm  |               |                  |   | * |
| Select H                                       | lash Alg                                     | jorithm<br>orithm to be                       | used for this | ; request        |   | * |
| Select H<br>Select Ha<br>Hash Alg              | lash Alg<br>ash Algo<br>Jorithm              | orithm<br>orithm to be<br>sha256              | used for this | ; request        | × | * |
| Select H<br>Select Ha<br>Hash Alg              | lash Alg<br>ash Algo<br>Jorithm              | orithm<br>orithm to be<br>sha256              | used for this | ; request        | ~ | * |
| Select H<br>Select Ha<br>Hash Alg<br>Select Si | lash Alg<br>ash Algo<br>jorithm<br>ignature  | gorithm<br>orithm to be<br>sha256<br>e Format | used for this | ; request        | ~ | * |
| Select H<br>Select Ha<br>Hash Alg<br>Select Si | lash Algo<br>ash Algo<br>porithm<br>ignature | gorithm<br>orithm to be<br>sha256<br>e Format | used for this | ; request        | ~ | * |
| Select H<br>Select Ha<br>Hash Alg<br>Select Si | lash Algo<br>ash Algo<br>gorithm<br>ignature | gorithm<br>orithm to be<br>sha256<br>e Format | used for this | ; request        | ~ | * |

- **31.** Quando tutte le proprietà del certificato sono state definite, fare clic su **Avanti** nella finestra di dialogo **Registrazione certificati**
- 32. mago.
- 33. Selezionare un percorso in cui salvare la richiesta di certificato e un formato. Individuare tale percorso e specificare un nome per il file .req. Il formato predefinito è base 64.
- 34. Fare clic su Fine.

| 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 po<br>to your hard disk or removable media. Enter the location and nam<br>click Finish. | rocess the request later, save the requ<br>ne of your certificate request, and the |
| File Name:  | parameter  |
| C:\Users\Administrator\Desktop\CSR6.1.21  | Browse   |
| File format:  |  |
| Binary  |  |
|   |  |
|   |  |
|   |  |
|   |  |

Viene generato un file .req, che è necessario utilizzare per richiedere un certificato firmato.

#### 16.1.1 Carica il file .req per ricevere in cambio un certificato firmato

È necessario copiare l'intero testo del file .req, incluse le righe iniziale e finale, e incollare il testo nell' autorità di certificazione interna di Servizi certificati Active Directory nella rete. Vedere Installazione di Servizi certificati Active Directory a pagina 74.

A meno che il dominio non abbia installato Servizi certificati Active Directory solo di recente o non

sia stato installato solo per questo scopo, sarà necessario inviare questa richiesta

seguendo una procedura separata configurata dal team di amministrazione del dominio.

Si prega di confermare questo processo con loro prima di procedere.

1. Individua la posizione del file .req e aprilo in Blocco note.

Ì

|   |  | ×  |
|---|--|--|
| File Edit Format View Help  |  |  |
| BEGIN NEW CERTIFICATE REQ   | QUEST  |  |
| MIIF2AYJKoZIhvcNAQcCoIIFyTCCBc  | UCAQMxDzANBg1ghkgBZQMEAgEFADCCBB4  | G  |
| CCsGAQUFBwwCoIIEEASCBAwwggQIMG  | GYWZAIBAgYKKWYBBAGCNWOKATFTMFECAQA   | w  |
| AwIBATFHMEUGC5sGAQQBgjcVFDE4MD  | )YCAQUMDENsdXN0ZXIxVEVNUAwaQ0xVU1R   | IF   |
| UjFURU1QXEFkbWluaXN0cmF0b3IMB0  | )1NQy5FWEUwggOYoIID1AIBATCCA40wggJ   | 1  |
| AgeAMBcxFTATBgNVBAMMDENsdXN0ZX  | (1xVEVNUDCCAS1wDQYJKoZ1hvcNAQEBBQA   | D  |
| ggEPADCCAQoCggEBAKVp0982y105tc  | Inypalujs-Be9jW0yRp+c5N00xf80cN0Dy   | g  |
| dVMV1SU9S9P1MWmUUZP+ZLumUmC6gC  | WIOSKgII+dLJOVQ+Z6AUWCIH+WVUSaVDJ  | C  |
| zczK1vUZmV576TBwf6L7MusVbNDD52  | VzdbG3pggapNdzHyg0RTJypo/TJ0pM6Ec  | 2  |
| 1N2d0S7ms4lHtj21DekEde3RsENvcvk   | c0/PH7k8b8Bww050+va3tk7iDbvw0a1VXF   | 9  |
| bal+Zv4pEP1iKnTwM1IvPmsXvw7gx6  | 5CrTw8ntgECAwEAAaCCAS8wHAYKKwYBBAG   | c  |
| Nw0CAzEOFgwxMC4wLjE0MzkzLjIwRC  | )YJKwYBBAGCNxUUMTgwNgIBBQwM02x1c3R   | 1  |
| cjFURU1QDBpDTFVTVEVSMVRFTVBcQW  | RtaW5pc3RyYXRvcgwHTU1DLkVYRTBgBgk  | q  |
| hkiG9w0BC04xUzBRMBMGA1UdJ00MMA  | -CCC-CAOUED HEND-CCC-CAOOD-4-VC-O  | n  |
|   | aooccsoaQurbwmbmbsocssoaQQbgJcvcgQ   | 0  |
| MAwwCgYIKwYBBQUHAwEwHQYDVRØOBB  | WEFOBsTd6/Hpi6c18h5HHq88hWc911MGY  | G  |
| MAwwCgYIKwYBBQUHAwEwHQYDVRØOBB<br>CisGAQQBgjcNAgIxWDBWAgEAHk4ATQ  | AGGCCSGAQUFBWMBMBSGCSSGAQQBgJcvCgQ<br>3YEFOBsTd6/Hpi6c18h5HHq88hWc911MGY<br>)BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB   | G<br>10  |
| MAwwCgYIKwYBBQUHAwEwHQYDVRØOBB<br>CisGAQQBgjcNAgIxWDBWAgEAHk4ATQ<br>AHcAYQByAGUAIABLAGUAeQAgAFMAdA  | AGGCCSGAQUFBWMBMBSGCSSGAQQBgJCVCgQ<br>3YEFOBsTd6/Hpi6c18h5HHq88hWc911MGY<br>2BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB   | G<br>10  |
| MAwwCgYIKwYBBQUHAwEwHQYDVRØOBB<br>CisGAQQBgjcNAgIxWDBWAgEAHk4ATQ<br>AHcAYQByAGUAIABLAGUAeQAgAFMAdA<br>AHIDAQAwDQYJKoZIhvcNAQELBQADgg  | AGGCCSGAQUFBWMBMBSGCSSGAQQBgJcvCgQ<br>3YEFOBsTd6/Hpi6c18h5HHq88hWc911MGY<br>2BpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>gEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn   | G<br>10<br>11<br>N                             |
| MAwwCgYIKwYBBQUHAwEwHQYDVRØOBB<br>CisGAQQBgjcNAgIxWDBWAgEAHk4ATQ<br>AHcAYQByAGUAIABLAGUAeQAgAFMAdA<br>AHIDAQAwDQYJKoZIhvcNAQELBQADgg<br>OAPtDKNDGskV/dq6rqgpYEKiQfWZeS  | AGGCCSGAQUFBWMBMBSGCSSGAQQBgJcvCgQ<br>BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGY<br>QBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>gEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>SndEOzxieJtES/1I5hmVUm51TIVydzE8iy   | G<br>IØ<br>IN<br>W                             |
| MAwwCgYIKwYBBQUHAwEwHQYDVRØOBB<br>CisGAQQBgjcNAgIxWDBWAgEAHk4ATQ<br>AHcAYQByAGUAIABLAGUAeQAgAFMAdA<br>AHIDAQAwDQYJKoZIhvcNAQELBQADgg<br>OAPtDKNDGskV/dq6rqgpYEKiQfWZeS<br>XjUze/+WIiZifGFnkMKYwrzKgx7qIr  | AGGCCSGAQUFBWMBMBSGCSSGAQQBgJcvCgQ<br>BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGY<br>QBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>gEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>SndEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo   | G<br>1<br>N<br>1                               |
| MAwwCgYIKwYBBQUHAwEwHQYDVR00BB<br>CisGAQQBgjcNAgIxWDBWAgEAHk4ATQ<br>AHcAYQByAGUAIABLAGUAeQAgAFMAdA<br>AHIDAQAwDQYJKoZIhvcNAQELBQADgg<br>OAPtDKNDGskV/dq6rqgpYEKiQfWZeS<br>XjUze/+WIiZifGFnkMKYwrzKgx7qIr<br>m3dWazix8dSVOQIRZ3Lr7yXg9iiF49<br>EX7vVZEvEAs/6uoApcKYc2KPgBP8ab  | AGGCCSGAQUFBWMBMBSGCSSGAQQBgJcvCgQ<br>BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGY<br>QBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>gEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>SndEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo   | G<br>G<br>N<br>W<br>T                          |
| MAwwCgYIKwYBBQUHAwEwHQYDVR00BB<br>CisGAQQBgjcNAgIxWDBWAgEAHk4ATQ<br>AHcAYQByAGUAIABLAGUAeQAgAFMAdA<br>AHIDAQAwDQYJKoZIhvcNAQELBQADgg<br>OAPtDKNDGskV/dq6rqgpYEKiQfWZeS<br>XjUze/+WIiZifGFnkMKYwrzKgx7qIr<br>m3dWazix8dSVOQIRZ3Lr7yXg9iiF49<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aH<br>Tp4XCYYiuvw/+iHqvNca2fyIIm8Hpb  | AGGCCSGAQUFBWMBMBSGCSSGAQQBgJCVCgQ<br>BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGY<br>QBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>gEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>SndEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo   | 9<br>6<br>1<br>1<br>1<br>1<br>1<br>1<br>3<br>3 |
| MAwwCgYIKwYBBQUHAwEwHQYDVR00BB<br>CisGAQQBgjcNAgIxWDBWAgEAHk4ATQ<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdA<br>AHIDAQAwDQYJKoZIhvcNAQELBQADgg<br>OAPtDKNDGskV/dq6rqgpYEKiQfWZeS<br>XjUze/+WIIZifGFnkMKYwrzKgx7qIr<br>m3dWazix8dSVOQIRZ3Lr7yXg9iiF49<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aH<br>Tp4XCYYiuyw/+iHqyNca2fvIIm8Hpb<br>izCCAYcCA00AF0BsTd6/Hpi6c18h5H  | AGGCCSGAQOFBWMBMBSGCSSGAQQBgJCVCgQ<br>BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGY<br>QBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>gEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>SndEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo<br>Cut<br>Copy  | G011NW<br>1333                                 |
| MAwwCgYIKwYBBQUHAwEwHQYDVR00BB<br>CisGAQQBgjcNAgIxWDBWAgEAHk4ATQ<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdA<br>AHIDAQAwDQYJKoZIhvcNAQELBQADgg<br>OAPtDKNDGskV/dq6rqgpYEKiQfWZeS<br>XjUze/+WIiZifGFnkMKYwrzKgx7qIr<br>m3dWazix8dSVOQIRZ3Lr7yXg9iiF49<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aH<br>Tp4XCYYiuyw/+iHqyNca2fvIIm8Hpb<br>izCCAYcCAQOAF0BsTd6/Hpi6c18h5H<br>FwYJKoZIhvcNA0kDMOoGCCsGAOUFBw  | AGGCCSGAQOFBWMBMBSGCSSGAQQBgJCVCgQ<br>BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGY<br>QBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>gEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>SndEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo<br>Cut<br>Copy<br>Paste   | G01NW L j 3 3 4 1                              |
| MAwwCgYIKwYBBQUHAwEwHQYDVR00BB<br>CisGAQQBgjcNAgIxWDBWAgEAHk4ATQ<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdA<br>AHIDAQAwDQYJKoZIhvcNAQELBQADgg<br>OAPtDKNDGskV/dq6rqgpYEKiQfWZeS<br>XjUze/+WIIZifGFnkMKYwrzKgx7qIr<br>m3dWazix8dSVOQIRZ3Lr7yXg9iiF49<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aH<br>Tp4XCYYiuyw/+iHqyNca2fvIIm8Hpb<br>izCCAYcCAQOAF0BsTd6/Hpi6c18h5H<br>FwYJKoZIhvcNAQkDMQoGCCsGAQUFBw<br>OY6dr8BzietMf5QwmoRNzq8MRGSQiN  | AGGCCSGAQOFBWMBMBSGCSSGAQQBgJCVCgQ<br>BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGY<br>QBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>gEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>5ndEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo<br>Cut<br>Copy<br>Paste<br>Delete   | G01NWLj33vIv                                   |
| MAwwCgYIKwYBBQUHAwEwHQYDVR00BB<br>CisGAQQBgjcNAgIxWDBWAgEAHk4ATQ<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdA<br>AHIDAQAwDQYJKoZIhvcNAQELBQADgg<br>OAPtDKNDGskV/dq6rqgpYEKiQfWZeS<br>XjUze/+WIIZifGFnkMKYwrzKgx7qIr<br>m3dWazix8dSVOQIRZ3Lr7yXg9iiF49<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aH<br>Tp4XCYYiuyw/+iHqyNca2fvIIm8Hpb<br>izCCAYcCAQOAFOBsTd6/Hpi6c18h5H<br>FwYJKoZIhvcNAQkDMQoGCCsGAQUFBw<br>OY6dr8BzietMf5QwmoRNzq8MRGSQiN<br>+q73I6NKKLzg7ROhm16Xj7 <u>tL4Id2iv</u>  | AGGCCSGAQOFBWMBMBSGCSSGAQQBgJCVCgQ<br>BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGY<br>QBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>gEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>SndEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo<br>Cut<br>Copy<br>Paste<br>Delete<br>Select All   | GOINWLJ23WIWE                                  |
| MAwwCgYIKwYBBQUHAwEwHQYDVR00BB<br>CisGAQQBgjcNAgIxWDBWAgEAHk4ATQ<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdA<br>AHIDAQAwDQYJKoZIhvcNAQELBQADgg<br>OAPtDKNDGskV/dq6rqgpYEKiQfWZeS<br>XjUze/+WIIZifGFnkMKYwrzKgx7qIr<br>m3dWazix8dSVOQIRZ3Lr7yXg9iiF49<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aH<br>Tp4XCYYiuyw/+iHqyNca2fvIIm8Hpb<br>izCCAYcCAQOAFOBsTd6/Hpi6c18h5H<br>FwYJKoZIhvcNAQkDMQoGCCsGAQUFBw<br>OY6dr8BzietMf5QwmoRNzq8MRGSQiN<br>+q73I6NKKLzg7ROhm16Xj7tL4Id2iv<br>1WR7EktvnBLYuBQVPGYb+gwd8EfBh9  | AGGCCSGAQQFBWMBMBSGCSSGAQQBgJCVCgQ<br>BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGY<br>QBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>gEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>SndEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo<br>Cut<br>Copy<br>Baste<br>Delete<br>Select All   | 0<br>G01NWLj33YIYE <                           |
| MAwwCgYIKwYBBQUHAwEwHQYDVR00BB<br>CisGAQQBgjcNAgIxWDBWAgEAHk4ATQ<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdA<br>AHIDAQAwDQYJKoZIhvcNAQELBQADgg<br>OAPtDKNDGskV/dq6rqgpYEKiQfWZeS<br>XjUze/+WIIZifGFnkMKYwrzKgx7qIr<br>m3dWazix8dSVOQIRZ3Lr7yXg9iiF49<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aH<br>Tp4XCYYiuyw/+iHqyNca2fvIIm8Hpb<br>izCCAYcCAQOAFOBsTd6/Hpi6c18h5H<br>FwYJKoZIhvcNAQkDMQoGCCsGAQUFBw<br>OY6dr8BzietMf5QwmoRNzq8MRGSQiN<br>+q73I6NKKLzg7ROhm16Xj7tL4Id2iV<br>1WR7EktvnBLYuBQVPGYb+gwd8EfBh9<br>r+5Z7i0E2HZpsBrSld1+u89F0Pi+W/  | AUGCCSGAQUFBWMBMBSGCSSGAQQBgJCVCgQ<br>BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGY<br>QBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>gEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>SndEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo<br>Cut<br>Copy<br>Paste<br>Delete<br>Select All<br>Right to left Reading order  | G01NWLj33wIw=кJ                                |
| MAwwCgYIKwYBBQUHAwEwHQYDVR0OBB<br>CisGAQQBgjcNAgIxWDBWAgEAHk4ATQ<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdA<br>AHIDAQAwDQYJKoZIhvcNAQELBQADgg<br>OAPtDKNDGskV/dq6rqgpYEKiQfWZeS<br>XjUze/+WIIZifGFnkMKYwrzKgx7qIr<br>m3dWazix8dSVOQIRZ3Lr7yXg9iiF49<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aH<br>Tp4XCYYiuyw/+iHqyNca2fvIIm8Hpb<br>izCCAYcCAQOAFOBsTd6/Hpi6c18h5H<br>FwYJKoZIhvcNAQkDMQoGCCsGAQUFBw<br>OY6dr8BzietMf5QwmoRNzq8MRGSQiN<br>+q73I6NKKLzg7ROhm16Xj7tL4Id2iv<br>IWR7EktvnBLYuBQVPGYb+gwd8EfBh9<br>r+5Z7i0E2HZpsBrSld1+u89F0Pi+W/<br>nIi7k+ce+EDOHhXkbSD+fHYFbUqaTY  | AVGCCSGAQUF BWMBMBSGCSSGAQQBgJCVCgQ<br>BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGY<br>QBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>gEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>SndEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo<br>Cut<br>Copy<br>Paste<br>Delete<br>Select All<br>Right to left Reading order<br>Show Unicode control characters  | 0G01NWにj23ペロッミ くしし                             |
| MAwwCgYIKwYBBQUHAwEwHQYDVR00BB<br>CisGAQQBgjcNAgIxWDBWAgEAHk4ATQ<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdA<br>AHIDAQAwDQYJKoZIhvcNAQELBQADgg<br>OAPtDKNDGskV/dq6rqgpYEKiQfWZeS<br>XjUze/+WIIZifGFnkMKYwrzKgx7qIr<br>m3dWazix8dSVOQIRZ3Lr7yXg9iiF49<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aH<br>Tp4XCYYiuyw/+iHqyNca2fvIIm8Hpb<br>izCCAYcCAQOAFOBsTd6/Hpi6c18h5H<br>FwYJKoZIhvcNAQkDMQoGCCsGAQUFBw<br>OY6dr8BzietMf5QwmoRNzq8MRGSQiN<br>+q73I6NKKLzg7ROhm16Xj7tL4Id2iv<br>IWR7EktvnBLYuBQVPGYb+gwd8EfBh9<br>r+5Z7i0E2HZpsBrSld1+u89F0Pi+W/<br>nIi7k+ce+EDoHhXkbSD+fHYFbUqaTY<br>2PmPVkUJGJEUMwfo8rb4xb9taP6ycU  | AVALUATE Select All<br>Right to left Reading order<br>Show Unicode control characters<br>Insert Unicode control character  | 0G01NWとj23ペロペーペリノ3                             |
| MAwwCgYIKwYBBQUHAwEwHQYDVR00BB<br>CisGAQQBgjcNAgIxWDBWAgEAHk4ATQ<br>AHCAYQByAGUAIABLAGUAeQAgAFMAdA<br>AHIDAQAwDQYJKoZIhvcNAQELBQADgg<br>OAPtDKNDGskV/dq6rqgpYEKiQfWZeS<br>XjUze/+WIIZifGFnkMKYwrzKgx7qIr<br>m3dWazix8dSVOQIRZ3Lr7yXg9iiF49<br>EX7yVZFyEAs/6uoApcKXc2KPgBP8aH<br>Tp4XCYYiuyw/+iHqyNca2fvIIm8Hpb<br>izCCAYcCAQOAFOBsTd6/Hpi6c18h5H<br>FwYJKoZIhvcNAQkDMQoGCCsGAQUFBw<br>OY6dr8BzietMf5QwmoRNzq8MRGSQiN<br>+q73I6NKKLzg7ROhm16Xj7tL4Id2iV<br>1WR7EktvnBLYuBQVPGYb+gwd8EfBh9<br>r+5Z7i0E2HZpsBrSld1+u89F0Pi+W/<br>nIi7k+ce+EDoHhXkbSD+fHYFbUqaTY<br>2PmPVkUJGJEUMwfo8rb4xb9taP6ycU<br>T8XTFWMOJCPMykW2<br>END NEW CERTIFICATE REQUE | AVGCCSGAQQFBWMBMBSGCSSGAQQBgJCVCgQ<br>BYEFOBsTd6/Hpi6c18h5HHq88hWc911MGY<br>QBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB<br>ABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB<br>gEBAFGoQLCtyivOXG0T0U4MS9VnUS0sQUn<br>ondEOzxieJtES/1I5hmVUm51TIVydzE8iy<br>Undo<br>Cut<br>Copy<br>Paste<br>Delete<br>Select All<br>Right to left Reading order<br>Show Unicode control characters<br>Insert Unicode control character ><br>Open IME | 9G01NWとj93WIW=ペリリ3                             |

- 2. Copia l'intero contenuto del file. Sono incluse le linee tratteggiate che segnano l'inizio e la fine della richiesta di certificato.
- 3. Apri un browser web e inserisci l'indirizzo della CA interna, che dovrebbe trovarsi in: [ip.ad.dr.ess/certsrv ].

Dove, ip.ad.dr.ess è l'indirizzo IP o il nome DNS del server host di Servizi certificati Active Directory della rete interna.

© MOBOTIX AG www.mobotix.com

MX\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 106/ 129Guida ai certificati - VMS Milestone XProtect®Guida ai certificati ai certificati - VMS Milestone XProtect®Guida ai certificati - VMS Mi Milestone XProtect®

## MOBOTIX HUB – Guida ai certificati - Installare i certificati in un ambiente di gruppo di

| S Microsoft Active Directory Certif × +                          | 0  |       | ^    |
|--|----|-------|------|
| ← → C ▲ Not secure   10.0.4.103/certsry/                         | \$ | Updat | e 1) |
| Microsoft Active Directory Certificate Services – IP-0A000467-CA |    | 1     | lome |

#### Welcome

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

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

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

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

- 4. Fai clic sul link Richiedi un certificato.
- 5. Fare clic sul collegamento di richiesta avanzata del certificato.



Web Browser Certificate E-Mail Protection Certificate

Or, submit an advanced certificate request.

6. Scegliere di inviare una richiesta di certificato utilizzando un file CMC con codifica Base 64.

## MOBOTIX HUB – Guida ai certificati - Installare i certificati in un ambiente di gruppo di

|   | X                             |
|---|-------------------------------|
| Microsoft Active Directory ×  | M 74 83                       |
| licrosoff Active Directory Certificate Services - CLUSTER2TEMP-CA                     | Home                          |
| dvanced Certificate Request   |                               |
| e policy of the CA determines the types of certificates you can request. Click one of | the following options to:     |
| Create and submit a request to this CA.   | and tester and graph and test |
| 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.   |                               |
|   |                               |
|   |                               |
|   |                               |
|   |                               |
|   |                               |

7. Incolla il contenuto del file .req nel modulo. Se è necessario selezionare un modello di certificato, selezionare

Server Web dall'elenco Modello di certificato.

| MIGTOSOTI FICUVE                 | Directory Certificate Services - CLUSTER2TEMP-CA   | Home                                    |
|----------------------------------|--|---|
| Submit a Cer                     | tificate Request or Renewal Request  |   |
| o submit a sa                    | aved request to the CA, paste a base-64-encoded CMC or   | PKCS #10 certificate request or PKCS #7 |
| enewal reque                     | ist generated by an external source (such as a web serve   | r) In the Saved Request box.            |
| aved Request:                    |  |   |
| ase-64-encodec                   | 1WR7EktvnBLYuBQVPGYb+gwd3EfBh9K90gvd5fMu:<br>1 r+527i0E2HZpsBrS1d1+u89F0Pi+W/a8/YV7BhAk;<br>t n1:7k+ce+FDoHbXkhS1+fHYFDUarYUFcD4u5Pa6/ |   |
| CMC or<br>KCS #10 or<br>KCS #7): | 2FmPVkUJGJEUMwfo8rb4xb9taP6ycUZwieLrNWw3)<br>TSXTFWMOJCPMykW2<br>END NEW CERTIFICATE REQUEST   |   |
|                                  | < >  |   |
| dditional Attrib                 | utes:  |   |
| Attributes                       |  |   |
|                                  | 5  |   |
|                                  |  |   |

8. Fai clic su Invia.

Il sito mostra un messaggio che indica che il certificato verrà emesso entro pochi giorni.

- I server CA interni possono essere utilizzati per emettere manualmente i certificati
- Prendere nota della data e dell'ora in cui è stata inviata la richiesta di certificato
| 0    | Micr  | osoft A | ctive ! | Directory Certi  | ×     | +                            | 0 | - |       | ×    |
|------|-------|---------|---------|------------------|-------|------------------------------|---|---|-------|------|
| 4    | 7     | C       | A       | Not secure       | 10.0  | 0.4.103/certsrv/certfnsh.asp | ☆ | 1 | Updat | e :) |
| Mica | rosof | t Activ | e Dire  | ctory Certificat | e Ser | rvices - IP-0A000467-CA      |   |   | 1     | 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 Emettere i certificati manualmente

È possibile emettere certificati manualmente dal computer che ospita Servizi certificati Active Directory.

- 1. Aprire Microsoft Management Console (MMC).
- 2. Passare allo **snap-in** Autorità di certificazione.
- 3. Espandere l' oggetto **Autorità di certificazione**.
- 4. Nella cartella **Richieste in sospeso** fare clic con il pulsante destro del mouse sull'ID richiesta corrispondente e, nell' **elenco Tutte le attività**, selezionare **Problema**.
- 5. Aprire un browser e accedere al sito interno di CA IIS all'indirizzo [ip.ad.dr.ess/certsrv].

Console1 - [Console Root\Certification Authority (Local)\IP-0A000467-CA\Pending Requests] 🔚 File Action View Favorites Window Help 🗢 🏟 🙍 📷 🙆 📾 🚺 🖬 Console Root Request ID **Binary Request** Actions **Request Status Code**  Certification Authority (Local) 5 - JIP-0A000467-CA View Attributes/Extensions... All Tasks Revoked Certificates Export Binary Data... Refresh Issued Certificates Issue Pending Requests Help Failed Requests Deny > 🔂 Certificates - Current User

6. Fare clic sul collegamento Visualizza lo stato di una richiesta di certificato in sospeso.

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

#### Welcome

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

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

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

#### Select a task:

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

7. Se il certificato è stato emesso, nella pagina risultante sarà disponibile un link contenente la data della richiesta del certificato.

| 0    | Microso | ft Active  | Directory Certit | ×     | +                            | 0 | - |       | ×           |
|------|---------|------------|------------------|-------|------------------------------|---|---|-------|-------------|
| ÷    | ⇒ (     | e 🔺        | Not secure       | 10.0  | 0.4.103/certsrv/certckpn.asp | ☆ | 4 | Updat | te :)       |
| Micr | osoft A | ctive Dire | ectory Certifica | te Se | rvices – IP-0A000467-CA      |   |   |       | <u>Home</u> |
| Viev | v the S | tatus      | of a Pendin      | g Ce  | ertificate Request           |   |   |       |             |
| Sele | ect the | certifica  | ate request      | you   | want to view:                |   |   |       |             |

8. Selezionare **Codifica DER** e scaricare la catena di certificati.

| Certificate | Issued  |  |
|-------------|---|--|
|             | <ul> <li>DER encoded or OBase 64 encoded</li> <li>Download certificate</li> <li>Download certificate chain</li> </ul> |  |
|             |   |  |
|             |   |  |

Passare alla cartella dei download, fare clic con il pulsante destro del mouse sul certificato e selezionare Installa certificato dal

menu di scelta rapida.

| ↓     ↓     ↓     Dowr       File     Home     SI | nloads<br>hare View |                            |                    |                      |
|---|---------------------|----------------------------|--------------------|----------------------|
| ← ↑ ↓ >   | This PC > Downlo    | bads                       |                    |                      |
| the Orviels account                               | Name                | ~                          | Date modified      | Туре                 |
| Desktop   | * certnew           | Onen                       | 10/26/2021 2:22 PM | PKCS #7 Certificates |
| 🕹 Downloads                                       | *                   | Install Certificate        |                    |                      |
| Documents   | *                   | Scan with Windows Defender |                    |                      |
| Pictures  | *                   | Open with                  |                    |                      |

- 9. Accetta l'avviso di sicurezza, se visualizzato.
- 10. Selezionare questa opzione per installare il certificato per l'utente corrente e fare clic su Avanti.

X

| Welcome to the C   | ertificate Import Wizard   |
|--|--|
| This wizard helps you copy o<br>lists from your disk to a cert                                 | ertificates, certificate trust lists, and certificate revocation ificate store.  |
| A certificate, which is issued<br>and contains information us<br>connections. A certificate st | by a certification authority, is a confirmation of your iden<br>ed to protect data or to establish secure network<br>ore is the system area where certificates are kept. |
| Store Location   |  |
| Current User     Local Machine   |  |
| To continue, click Next.   |  |
|  |  |
|  |  |

- Scegli una posizione del negozio. Selezionare Posiziona tutti i certificati nell'archivio seguente e fare clic sul pulsante Sfoglia per aprire la finestra Seleziona archivio certificati. Passare all' archivio certificati personali e fare clic su OK.
- 12. Fare clic su **Avanti**.

| Certificate Store  |  |
|--|--|
| Certificate stores are system areas where certificates are kept.   |  |
| Windows can automatically select a certificate store, or you can specify a location fi<br>the certificate.<br>Automatically select the certificate store based on the type of certificate<br>Place all certificates in the following store | or<br>Select Certificate Store<br>Select the certificate store you want to use.  |
| Browse   | Personal<br>Trusted Root Certification Authorities<br>Enterprise Trust<br>Intermediate Certification Authorities<br>Trusted Publishers |
|  | Show physical stores   |

- 13. Completare l'Importazione guidata certificati.
- 14. Passare allo snap-in Certificati di Microsoft Management Console (MMC).

15. Nella console passare all'archivio personale in cui è installato il certificato. Fare clic con il pulsante destro del mouse sul certificato e selezionare **Tutte le attività** > **Gestisci chiavi private**.



- 16. Aggiungere l'account che esegue il software MOBOTIX HUB Management Server, Recording Server o Mobile Server all'elenco degli utenti autorizzati a utilizzare il certificato.
- 17. Assicurati che l'utente abbia abilitato sia il controllo completo che le autorizzazioni di lettura.
- Per impostazione predefinita, il software MOBOTIX HUB utilizza l'account NETWORK SERVICE.

| 1                              |                   |          |
|--------------------------------|-------------------|----------|
| CREATOR OWNER                  |                   |          |
| NETWORK SERVICE                |                   |          |
| Administrators (CLUSTER1T      | EMP\Administrator | (2       |
|                                |                   |          |
|                                |                   |          |
|                                | A <u>d</u> d      | Remove   |
| missions for NETWORK<br>RVICE  | Allow             | Deny     |
| ull control                    |                   |          |
| Read                           |                   |          |
| pecial permissions             |                   |          |
|                                |                   |          |
|                                |                   |          |
|                                | ed settings       | Advanced |
| special permissions or advance | ood oottiingo,    | Auvanceu |

© MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 114/ 129Guida ai certificati - VMS Milestone XProtect®Guida ai certificati - VMS Milestone XProtect®Guida ai certificate Milestone XProtect®

# 16.1.3 Abilitare la crittografia del server per i server di gestione e i server di registrazione

Una volta installato il certificato con le proprietà e le autorizzazioni corrette, eseguire le operazioni seguenti.

- 1. Su un computer in cui è installato un server di gestione o un server di registrazione, aprire il configuratore server da:
  - Il menu Start di Windows
    - 0
  - Il gestore del server, facendo clic con il pulsante destro del mouse sull'icona del gestore del server sulla barra delle applicazioni del computer
- 2. Nel Server Configurator, in Certificato server, attivare Encryption.
- 3. Fare clic su Seleziona certificato per aprire un elenco con nomi di soggetti univoci di certificati che dispongono di una chiave privata e che sono installati nel computer locale nell'archivio certificati di Windows.
- 4. Selezionare un certificato per crittografare la comunicazione tra il server di registrazione, il server di gestione, il server di failover e il server di raccolta dati.
- 5. Selezionare **Dettagli** per visualizzare le informazioni dell'archivio certificati di Windows sul certificato selezionato.

All'utente del servizio Recording Server è stato concesso l'accesso alla chiave privata. È necessario che questo certificato sia attendibile su tutti i client.

| Server Configurator |  | -                 |         | × |
|---------------------|--|-------------------|---------|---|
| Encryption          | Encryption   |                   |         |   |
| legistering servers | It is recommended to secure communication with encryptio   | n. <u>Learn m</u> | ore     |   |
| anguage selection   | Server certificate<br>Applies to: management server, recording server, failover server, data<br>collector  |                   |         |   |
|                     | Encryption: On   | 0                 |         |   |
|                     | (hermony)  | 9                 | Details |   |
|                     | Camplicate issued by MS-Organization-929-Actess (2021), Expires 3/8/2021   |                   |         |   |
|                     | Streaming media certificate<br>Applies to clients and servers that retrieve data streams from the reco<br>server   | rding             |         |   |
|                     | Encryption: On   |                   |         |   |
|                     | Teaching and the second s | 4                 | Details |   |
|                     | Certificate Instead by MS-Degarization 9(9) Access (2021), Instead 5(0/2021  |                   |         |   |
|                     |  |                   |         |   |
|                     |  |                   |         |   |
|                     |  |                   |         |   |
|                     |  |                   |         |   |
|                     |  |                   | -       | 5 |
|                     |  |                   | Apply   |   |

6. Fare clic su **Applica**.

Quando si applicano i certificati, il server di registrazione viene arrestato e riavviato. L'arresto del servizio Server di registrazione significa che non è possibile registrare e visualizzare video in diretta durante la verifica o la modifica della configurazione di base del server di

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 115/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificate® Milestone XProtect®

#### 16.2 Installare i certificati per la comunicazione con il server di eventi

È possibile crittografare la connessione bidirezionale tra il server di eventi e i componenti che comunicano con il server di eventi, incluso il server LPR. Quando si abilita la crittografia nel server eventi, questa si applica alle connessioni da tutti i componenti che si connettono al server eventi. Prima di abilitare la crittografia, è necessario installare i certificati di sicurezza nel server eventi e in tutti i componenti di connessione.



Ì

Quando la comunicazione del server di eventi è crittografata, ciò si applica a tutte le comunicazioni con tale server di eventi. In altre parole, è supportata una sola modalità alla volta, http o https, ma non contemporaneamente.

La crittografia si applica a tutti i servizi ospitati nel server eventi, inclusi Transact, Maps, GisMap e Intercommunication.

Prima di abilitare la crittografia nel server degli eventi, tutti i client (Desk Client e

Management Client) e il plug-in MOBOTIX HUB LPR devono essere aggiornati almeno alla versione 2022 R1.

HTTPS è supportato solo se ogni componente viene aggiornato almeno alla versione 2022 R1.

La creazione dei certificati è la stessa descritta nelle sezioni seguenti, a seconda dell'ambiente dei certificati : Installare certificati CA di terze parti o commerciali per la comunicazione con il server di gestione o il server di registrazione a pagina 57

Installare i certificati in un dominio per la comunicazione con il server di gestione o il server di registrazione a pagina 86 Installare i certificati in un ambiente di gruppo di lavoro per la comunicazione con il server di gestione o il server di registrazione a pagina 104

## 16.3 Abilita la crittografia del server eventi MOBOTIX HUB

Dopo l'installazione, il certificato può essere abilitato per l'utilizzo con tutte le comunicazioni con il server eventi.



Dopo che tutti i client sono stati aggiornati almeno alla versione 2022 R1, è possibile abilitare la crittografia nel server eventi.

È possibile crittografare la connessione bidirezionale tra il server degli eventi e i componenti che comunicano con il server degli eventi, incluso il server LPR.



Quando si configura la crittografia per un gruppo di server, è necessario abilitarla con un certificato appartenente allo stesso certificato CA oppure, se la crittografia è disabilitata, deve essere disabilitata in tutti i computer del gruppo di server.

## 16.3.1 Prerequisiti:

Un certificato di autenticazione server è considerato attendibile nel computer che ospita il server eventi Innanzitutto, abilitare la crittografia nel server eventi.

Passi:

- 7. Su un computer in cui è installato un server di eventi , aprire il **configuratore del server** da:
  - Il menu Start di Windows

```
0
```

© MOBOTIX AG www.mobotix.com

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 116/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificati ai certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 116/ 129Guida ai certificati - VMS Milestone XProtect® Guida ai certificates Milestone XProtect®

- Il server di eventi facendo clic con il pulsante destro del mouse sull'icona del server di eventi sulla barra delle applicazioni del computer
- 8. In Server Configurator, in Server eventi e componenti aggiuntivi, attivare Crittografia.
- 9. Fare clic su Seleziona certificato per aprire un elenco con nomi di soggetti univoci di certificati che dispongono di una chiave privata e che sono installati nel computer locale nell'archivio certificati di Windows.
- 10. Selezionare un certificato per crittografare la comunicazione tra il server di eventi e i componenti aggiuntivi correlati.
- 11. Selezionare Dettagli per visualizzare le informazioni dell'archivio certificati di Windows sul certificato selezionato.

| Server Configurator | 12 m   | -  | ÷ [         | X      |
|---------------------|--|--|-------------|--------|
| Encryption          | Encryption configuration successful  |  |             | ×      |
| Registering servers | Encryption   |  |             |        |
| Language selection  | It is recommended to secure communication<br>Streaming media certificate<br>Applies to clients and servers that retrieve data stream<br>server | with encryption. <u>Learn</u><br>ms from the recording | <u>more</u> |        |
|                     | Encryption: Off  |  |             |        |
|                     | Select certificate   | ÷.   |             | ani.   |
|                     | No certificate selected  |  |             |        |
|                     | Event server and add-ons<br>Applies to: event server, LPR server   |  |             |        |
|                     | Encryption: On   |  |             | - 1    |
|                     |  | ×  | D           | etails |
|                     | Certificate issued by I . Exp  | ires 1/8/2022  | _           | _      |
|                     |  |  | Ap          | oply   |
|                     |  |  |             |        |

12. Fare clic su Applica.

Per completare l'abilitazione della crittografia, il passaggio successivo consiste nell'aggiornare le impostazioni di crittografia su ciascun componente aggiuntivo correlato sul server LPR.

## 16.3.2 Importare i certificati client

In questa sezione viene descritto come importare i certificati client in una workstation o in un dispositivo client.

1. Dopo aver importato un certificato CA nel server di gestione o nel server di registrazione, è possibile accedervi da qualsiasi workstation o server della rete recandosi al seguente indirizzo: http://localhost/certsrv/

Mx\_GL\_MX\_HUB\_Certificates\_V2-04\_IT.docx • 04.03.2025 • Pagina 117/ 129Guida ai certificati - VMS Milestone XProtect®Guida ai certificati - VMS Milestone XProtect®Guida ai certificate Milestone XProtect®

Tuttavia, l'indirizzo del server che detiene il certificato (chiave privata) prenderà il posto di "localhost". Per esempio:

| S Microsoft Active Directory Certit × +   |  | 0                           | -                                     |                            | ×        |
|---|--|-----------------------------|---------------------------------------|----------------------------|----------|
| ← → C ▲ Not secure   10.0.4.103/certsrv/  |  |                             | z                                     | 2 :                        | £ (      |
| Microsoft Active Directory Certificate Services - IP-0A000467-CA  |  |                             |                                       |                            | Home     |
| Welcome   |  |                             |                                       |                            | _        |
| Use this Web site to request a certificate for your Web browse<br>certificate, you can verify your identity to people you communi-<br>messages, and, depending upon the type of certificate you red<br>You can also use this Web site to download a certificate autho<br>certificate revocation list (CRL), or to view the status of a pend | r, e-mail client, or other p<br>cate with over the Web,<br>quest, perform other sect<br>prity (CA) certificate, certi<br>ding request. | orogra<br>sign a<br>urity f | am. By<br>and en<br>tasks.<br>e chain | / using<br>icrypt<br>i, or | a        |
| For more information about Active Directory Certificate Service<br>Documentation.   | es, see <u>Active Directory (</u>  | Certif                      | ficate S                              | Service                    | <u>s</u> |
| Select a task:  |  |                             |                                       |                            |          |
| Request a certificate   |  |                             |                                       |                            |          |
| view the status of a pending certificate request  |  |                             |                                       |                            |          |
| Download a CA certificate, certificate chain, or CRL  |  |                             |                                       |                            |          |

Questo server Web è ospitato nel server host di Servizi certificati Active Directory che contiene il certificato CA.

- 2. Fare clic su Scarica un certificato CA, una catena di certificati o un CRL.
- 3. Nel campo Certificato CA, selezionare il certificato CA da utilizzare con il sistema MOBOTIX HUB e fare clic su

## **1.** Scarica la catena di certificati CA.

| Microsoft Active Directory Certif × +  | • - • ×                         |
|--|---------------------------------|
| ← → C ▲ Not secure   10.0.4.103/certsrv/certcarc.asp   | ☆ ≛ :                           |
| Microsoft Active Directory Certificate Services - IP-0A000467-CA   | Home                            |
| Download a CA Certificate, Certificate Chain, or CRL   |                                 |
| To trust certificates issued from this certification authority, install this   | s CA certificate.               |
| To download a CA certificate, certificate chain, or CRL, select the ca   | ertificate and encoding method. |
| CA certificate:  |                                 |
|  |                                 |
| Current [IP-0A000467-CA] -   |                                 |
| Current [IP-0A000467-CA] =   |                                 |
| Current [IP-0A000467-CA]   |                                 |
| Current [IP-0A000467-CA] *   |                                 |
| Encoding method:   |                                 |
| Encoding method:<br>Base 64  |                                 |
| Encoding method:   |                                 |
| Encoding method:   |                                 |
| Encoding method:<br>DER<br>Base 64<br>Install CA certificate<br>Download CA certificate<br>Download CA certificate chain |                                 |

- 4. Selezionare **Codifica DER** e scaricare la catena di certificati.
- 5. Passare alla cartella dei download, fare clic con il pulsante destro del mouse sul certificato e selezionare Installa certificato dal menu di scelta rapida.

| ↓         ↓         ↓         Downloads           File         Home         Share         View | v                        |          |   | ÷             | - ×     |
|--|--------------------------|----------|---|---------------|---------|
| ← 🐳 🛧 🛧 > This PC >  | Downloads                | ~ 0      | Search D  | ownloads      | Q       |
| Desktop ^ Name   | *                        | Date mor | dified  | Туре          | Size    |
| 🗄 Documents 🔤 🕞  | ertnew,p7b               | 5/11/202 | 1 1:31 PM   | PKCS #7 Certi | ficates |
|  | Open                     |          |   |               |         |
| 💧 Music  | Install Certificate      |          |   |               |         |
| Pictures   | Edit with Notepad++      |          |   |               |         |
| Videos   | 🖻 Share                  |          |   |               |         |
| Local Disk (C:)  | Open with                |          |   |               |         |
| - Marcal   | Give access to           | >        |   |               |         |
|  | Restore previous version | ns       |   |               | )       |
| 1 item 1 item selected 832 bytes   | Send to                  | >        | and the second se |               |         |
|  | Cut                      |          |   |               |         |
|  | Сору                     |          |   |               |         |
|  | Create shortcut          |          |   |               |         |
|  | Delete                   |          |   |               |         |
|  | Rename                   |          |   |               |         |
|  | Properties               |          |   |               |         |

- 6. Viene avviata l'Importazione guidata certificati.
- 7. Fare clic su Avanti.

| F) | - " Certificate Import Wizard   |
|----|---|
|    | Welcome to the Certificate Import Wizard  |
|    | This wizard helps you copy certificates, certificate trust lists, and certificate revocation<br>lists from your disk to a certificate store.  |
|    | A certificate, which is issued by a certification authority, is a confirmation of your identity<br>and contains information used to protect data or to establish secure network<br>connections. A certificate store is the system area where certificates are kept. |
|    |   |
|    | To continue, dick Next.   |
|    |   |
|    |   |
|    | Next Can  |

8. Scegli una posizione del negozio. Selezionare Posiziona tutti i certificati nell'archivio seguente e fare clic sul pulsante Sfoglia

per aprire la finestra Seleziona archivio certificati.

9. Passare all' archivio certificati delle autorità di certificazione radice di terze parti e fare clic su OK.

| Certificate Store<br>Certificate stores are system areas where certificates are kept. |  |                            |                           |
|---|--|----------------------------|---------------------------|
| Windov<br>the cer   | s can automatically select a co<br>ficate. | ertificate store, or you o | an specify a location for |
| 0   | utomatically select the certific           | ate store based on the     | type of certificate       |
| () F  | ace all certificates in the follo          | wing store                 |                           |
| 1.9   | ertificate store:                          |                            |                           |
|   |  |                            | Browse                    |
|   |  |                            |                           |
|   |  |                            |                           |
|   |  |                            |                           |
|   |  |                            |                           |
|   |  |                            |                           |

Fare clic su **Avanti**.

| elect Certificate Store  | ×  |
|--|--|
| elect the certificate store you want to use.   |  |
|  | <ul> <li>tificates are kept.</li> </ul>  |
| Ontrusted Certificates     Third-Party Root Certification Authorities     Tausted Reself | store, or you can specify a location for |
| Client & thentication Issuers  | e based on the type of certificate       |
| Show physical stores   | re                                       |
| OK Cancel  | Browse                                   |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  | Alua                                     |

10. Completare l'Importazione guidata certificati.

A questo punto, la workstation ha importato i componenti del certificato necessari per stabilire comunicazioni sicure con il server di gestione o il server di registrazione.

## 16.4 Visualizzare lo stato della crittografia ai client

Per verificare se il server di registrazione crittografa le connessioni:

- 1. Aprire il client di gestione.
- 2. Nel riquadro **Spostamento sito** selezionare **Server > Server di registrazione**. Viene visualizzato un elenco di server di registrazione.

3. Nel riquadro **Panoramica**, selezionare il server di registrazione pertinente e passare alla **scheda Info**. Se la crittografia è abilitata per i client e i server che recuperano i flussi di dati dal server di registrazione, viene visualizzata un'icona a forma di lucchetto davanti all'indirizzo del server Web locale e all'indirizzo del server Web opzionale.

| Recording server information                    |      |
|---|------|
| Name:   |      |
| Recording server 1                              |      |
| Description:                                    |      |
| Covers sector 1                                 | 14   |
|   | 1996 |
| Host name:                                      |      |
|   |      |
| 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 Visualizzare lo stato della crittografia in un server di registrazione di failover

- Per verificare se il server di registrazione di failover utilizza la crittografia, effettuare le seguenti operazioni:
  - 1. Nel riquadro **Spostamento sito** selezionare **Server > Server di failover**. Verrà visualizzato un elenco di server di registrazione di failover.

2. Nel riquadro **Panoramica**, selezionare il server di registrazione pertinente e passare alla **scheda Info**. Se la crittografia è abilitata per i client e i server che recuperano i flussi di dati dal server di registrazione, viene visualizzata un'icona a forma di lucchetto davanti all'indirizzo del server Web locale e all'indirizzo del server Web opzionale.

## Guida ai certificati | MOBOTIX HUB®

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

Appendice A | Crea script certificato CA

#### # Eseguire questo script una volta, per creare un certificato in grado di firmare più certificati SSL del server

#### # Certificato privato per la firma di altri certificati (nell'archivio certificati)

#### # Identificazione personale del certificato privato utilizzato per firmare altri certificati

Set-Content -Path "\$PSScriptRoot\ca\_thumbprint.txt" -Value \$ca\_certificate. Identificazione personale

#### # Certificato CA pubblico da considerare attendibile (autorità di certificazione radice di terze parti)

Export-Certificate -Cert "Cert:\CurrentUser\My\\$(\$ca\_certificate. Identificazione personale)" -FilePath "\$PSScriptRoot\root-authority-public.cer"

Appendice B | Crea script certificato SSL server

```
# Esegui questo script una volta per ogni server per il quale è necessario un certificato SSL.
# Il certificato deve essere eseguito sul singolo computer in cui si trova il certificato CA. # Il certificato SSL del server creato deve quindi essere spostato sul server e importato nell'archivio certificati #.
# Dopo aver importato il certificato, consentire l'accesso alla chiave privata del certificato per # gli utenti del servizio dei servizi che devono utilizzare il certificato.
```

# Carica il certificato CA dall'archivio (l'identificazione personale deve essere in ca\_thumbprint.txt)
\$ca\_thumbprint = Ottieni-Contenuto -Percorso "\$PSScriptRoot\ca\_thumbprint.txt"
\$ca\_certificate = (Get-ChildItem -Path cert:\CurrentUser\My\\$ca\_thumbprint)

# Richiedi all'utente i nomi DNS da includere nel certificato
\$dnsNames = Read-Host 'Nomi DNS per il certificato SSL del server (delimitato da spazio - anche la 1a voce è soggetta al certificato)'
\$dnsNamesArray = @(\$dnsNames -Split '' | foreach { \$\_. Trim() } | dove { \$\_}})

if (\$dnsNamesArray.Lunghezza -eq 0) { Write-Host -ForegroundColor Red 'Almeno un nome dns deve essere specificato' exit

\$subjectName = \$dnsNamesArray[0]

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

# Opzionalmente consentire all'utente di digitare un elenco di indirizzi IP da inserire nel certificato \$ipAddresses = Read-Host 'Indirizzi IP per il certificato SSL del server (delimitato dallo spazio)' \$ipAddressesArray = @(\$ipAddresses -Split ' | foreach { \$\_. Trim() }| dove { \$\_.}) if (\$ipAddressesArray.Lunghezza -gt 0) { \$ipEntries = (\$ipAddressesArray | foreach { "IPAddress=\$\_" }) -Join '&'

\$dnsEntries = "\$dnsEntries&\$ipEntries"

}

# Crea la stringa delle voci dns finali (ad esempio "2.5.29.17={text}DNS=myhost&DNS=myhost.domain.com&IPAddress=10.0.0.103")
\$dnsEntries = "2.5.29.17={testo}\$dnsEntries"

# L'unico scopo richiesto del servizio è "Autenticazione del server"
\$serverAuthentication = '2.5.29.37={critico}{testo}1.3.6.1.5.5.7.3.1'

# Ora - crea il certificato SSL del server \$certificate = New-SelfSignedCertificate -CertStoreLocation Cert:\CurrentUser\My -Subject \$subjectName -Signer \$ca\_certificate ' -FriendlyName 'Certificato SSL VMS' -TextExtension @(\$dnsEntries, \$serverAuthentication)

# Esporta certificato su disco - proteggi con una password

\$password = Read-Host -AsSecureString "Password del certificato SSL del server"
Export-PfxCertificate -Cert "Cert:\CurrentUser\My\\$(\$certificate. Identificazione personale)" -FilePath "\$PSScriptRoot\\$subjectName.pfx" -Password \$password

# Elimina il certificato SSL del server dall'archivio certificati locale \$certificate | Rimuovi-Elemento

Appendice C | Crea script certificato CA

# Eseguire questo script una volta per ogni server di gestione per il quale è necessario un certificato.
# Il certificato deve essere eseguito sul singolo computer in cui si trova il certificato CA. # Il certificato creato deve quindi essere spostato sui server di gestione e
# importato nell'archivio certificati lì.

# Carica il certificato CA dall'archivio (l'identificazione personale deve essere in ca\_thumbprint.txt)
\$ca\_thumbprint = Ottieni-Contenuto -Percorso "\$PSScriptRoot\ca\_thumbprint.txt"
\$ca\_certificate = (Get-ChildItem -Percorso certificato:\CurrentUser\My\\$ca\_thumbprint)

# Richiedi all'utente i nomi DNS da includere nel certificato

\$dnsNames = Read-Host 'Nomi DNS per il certificato del server di gestione (delimitato da virgole - anche la 1a voce è soggetta al certificato)'
\$dnsNamesArray = @(\$dnsNames -Dividi ',' | foreach {\$\_. Trim()}| dove {\$\_}})

se (\$dnsNamesArray. Lunghezza -eq 0) { Write-Host -ForegroundColor Red 'Almeno un nome dns deve essere specificato' exit

}

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

```
# Opzionalmente consentire all'utente di digitare un elenco di indirizzi IP da inserire nel certificato
```

\$ipAddresses = Read-Host 'Indirizzi IP per il certificato del server di gestione (delimitato da virgole)'
\$ipAddressesArray = @(\$ipAddresses -Dividi ',' | foreach { \$\_. Trim() } | dove { \$\_.}) if (\$ipAddressesArray. Lunghezza -gt 0) {
 \$ipEntries = (\$ipAddressesArray | foreach { "IPAddress=\$\_" }) -Join '&'
 \$dnsEntries = "\$dnsEntries&\$ipEntries"
}
\$subjectName = \$ipAddressesArray[0]

# Crea la stringa delle voci dns finali (ad esempio "2.5.29.17={text}DNS=myhost&DNS=myhost.domain.com&IPAddress=10.0.0.103")
\$dnsEntries = "2.5.29.17={testo}\$dnsEntries"

# L'unico scopo richiesto del servizio è "Autenticazione del server" \$serverAuthentication = '2.5.29.37={critico}{testo}1.3.6.1.5.5.7.3.1'

#### # Esporta certificato su disco - proteggi con una password

\$password = Read-Host -AsSecureString "Password del certificato del server di gestione"
Export-PfxCertificate -Cert "Cert:\CurrentUser\My\\$(\$certificate. Identificazione personale)" -FilePath "\$PSScriptRoot\\$subjectName.pfx" -Password \$password

# Eliminare il certificato del server di gestione dall'archivio certificati locale \$certificate | Rimuovi-Elemento



EN\_03/25

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

MOBOTIX è un marchio di MOBOTIX AG registrato nell'Unione Europea, negli Stati Uniti e in altri paesi. Con riserva di modifiche senza preavviso. MOBOTIX non si assume alcuna responsabilità per errori tecnici o editoriali o omissioni contenute nel presente documento. Tutti i diritti riservati. © MOBOTIX AG 2025