



MOBOTIX HUB – Guida ai certificati

V2.03

Contenuto

Copyright, marchi e disclaimer	3
Informazioni su questa guida	4
Introduzione ai certificati	5
Panoramica degli scenari e delle procedure utilizzate con i certificati	8
Quali client hanno bisogno di certificati?	11
Server Configurator (spiegazione)	13
Script di PowerShell	16
Creazione e distribuzione manuale dei certificati	17
Creare un certificato CA	17
Installare i certificati nei client	19
Creare un certificato SSL	27
Importa certificato SSL	29
Creare un certificato SSL per il server di gestione del failover	38
Installare i certificati per la comunicazione con il server mobile	40
Installare certificati CA di terze parti o commerciali per la comunicazione con il server di gestione o Server di registrazione	57
Installare Servizi certificati Active Directory	74
Installare i certificati in un dominio per la comunicazione con il server di gestione o il server di registrazione	86
Installare i certificati in un ambiente di gruppo di lavoro per la comunicazione con il server di gestione o Server di registrazione	104
Installare i certificati per la comunicazione con il server di eventi	126
Importare i certificati client	129
Visualizzare lo stato della crittografia ai client	135
Visualizzare lo stato della crittografia in un server di registrazione di failover	136
Appendice A Creare script di certificato CA	137
Appendice B Creazione dello script del certificato SSL del server	138
Appendice C Creazione di uno script di certificato del server di gestione failover	139

Copyright, marchi e disclaimer

Diritto d'autore © 2023 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.

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.

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

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

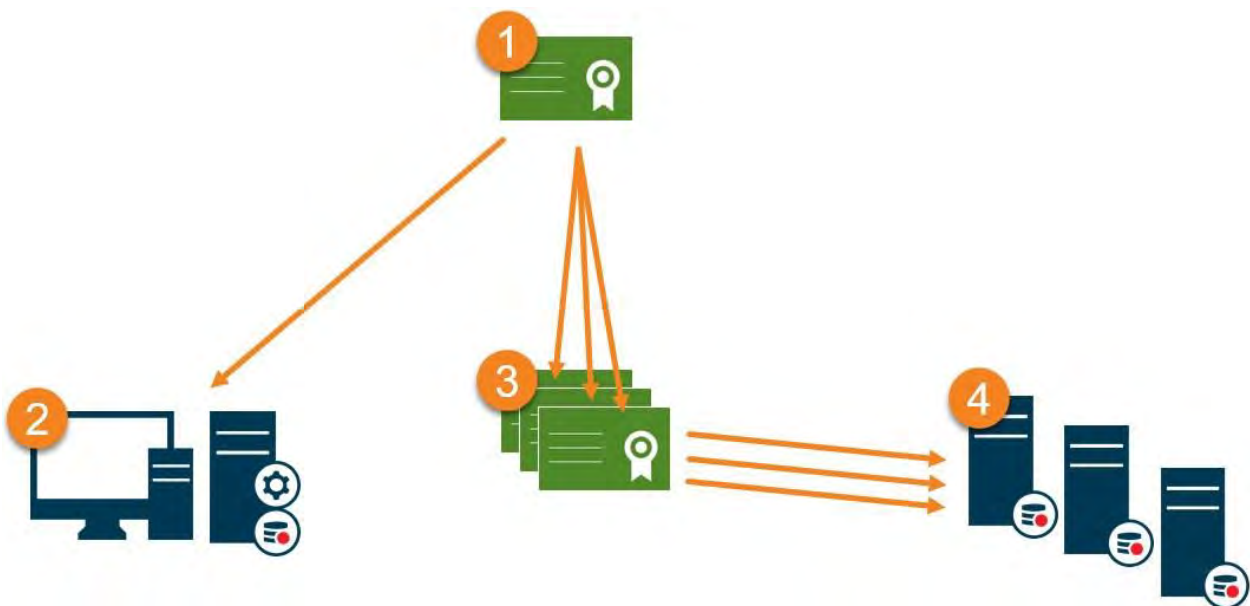
Per le soluzioni create con MIP SDK 2018 R3 o versioni precedenti che



- Se le integrazioni vengono effettuate utilizzando le librerie MIP SDK, devono essere ricomilate con
- Se le integrazioni comunicano direttamente con le API del server di registrazione senza
- In caso di dubbi, chiedi al tuo fornitore che ha fornito

Distribuzione dei certificati

L'immagine illustra il concetto di base di come i certificati vengono firmati, considerati attendibili e distribuiti nelle VM HUB MOBOTIX.



❶ Un'autorità di certificazione (CA) è chiunque sia in grado di emettere certificati radice. Un certificato CA funge da terza parte attendibile, considerata attendibile sia dal soggetto/proprietario (server) che dalla parte che verifica il certificato (client) (vedere [Creazione di un certificato CA a pagina 17](#)).

❷ Il certificato pubblico deve essere considerato attendibile in tutti i computer client. In questo modo i client possono verificare la validità dei certificati emessi dalla CA (vedere [Installazione dei certificati sui client a pagina 19](#)).

❸ Il certificato CA viene utilizzato per emettere certificati di autenticazione del server privato ai server (vedere [Creazione di un certificato SSL a pagina 27](#)).

4 I certificati SSL privati creati devono essere importati nell'archivio certificati di Windows su tutti i server (vedere [Importazione di certificati SSL a pagina 29](#)).

Requisiti per il certificato SSL privato:

- Rilasciato al server in modo che il nome host del server sia incluso nel certificato, come soggetto (proprietario) o nell'elenco dei nomi DNS a cui viene rilasciato il certificato
- Attendibile in tutti i computer che eseguono servizi o applicazioni che comunicano con il servizio nei server, considerando attendibile il certificato CA utilizzato per emettere il certificato SSL
- L'account del servizio che esegue il server deve avere accesso alla chiave privata del certificato sul server.



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.

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:

- 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](#)

- 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.

- 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](#)

- 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](#)

- 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

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:

- 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 ricomilate 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](#)

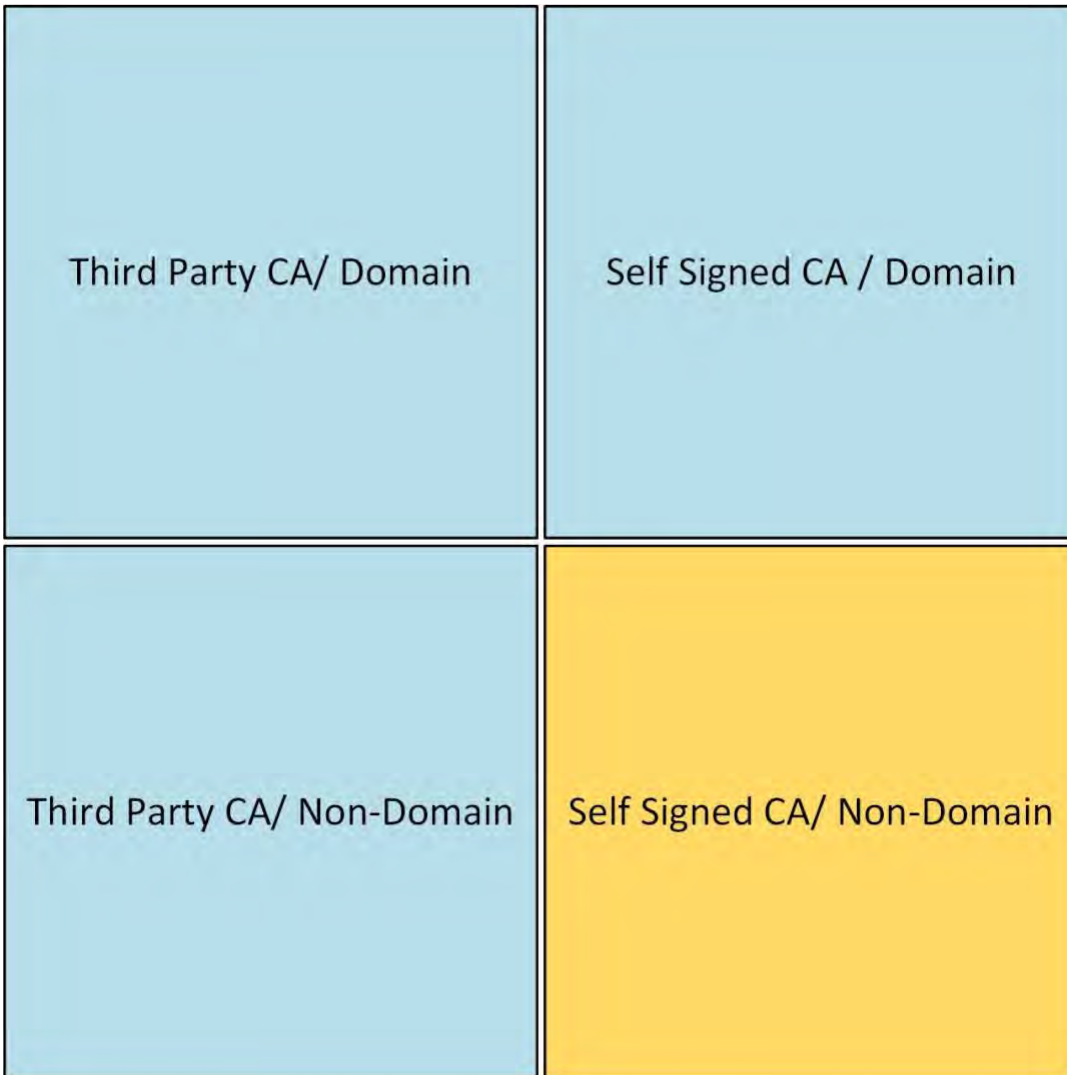
[Importare i certificati client nella pagina 129](#)



Quali client hanno bisogno di certificati?

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

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](#).

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:

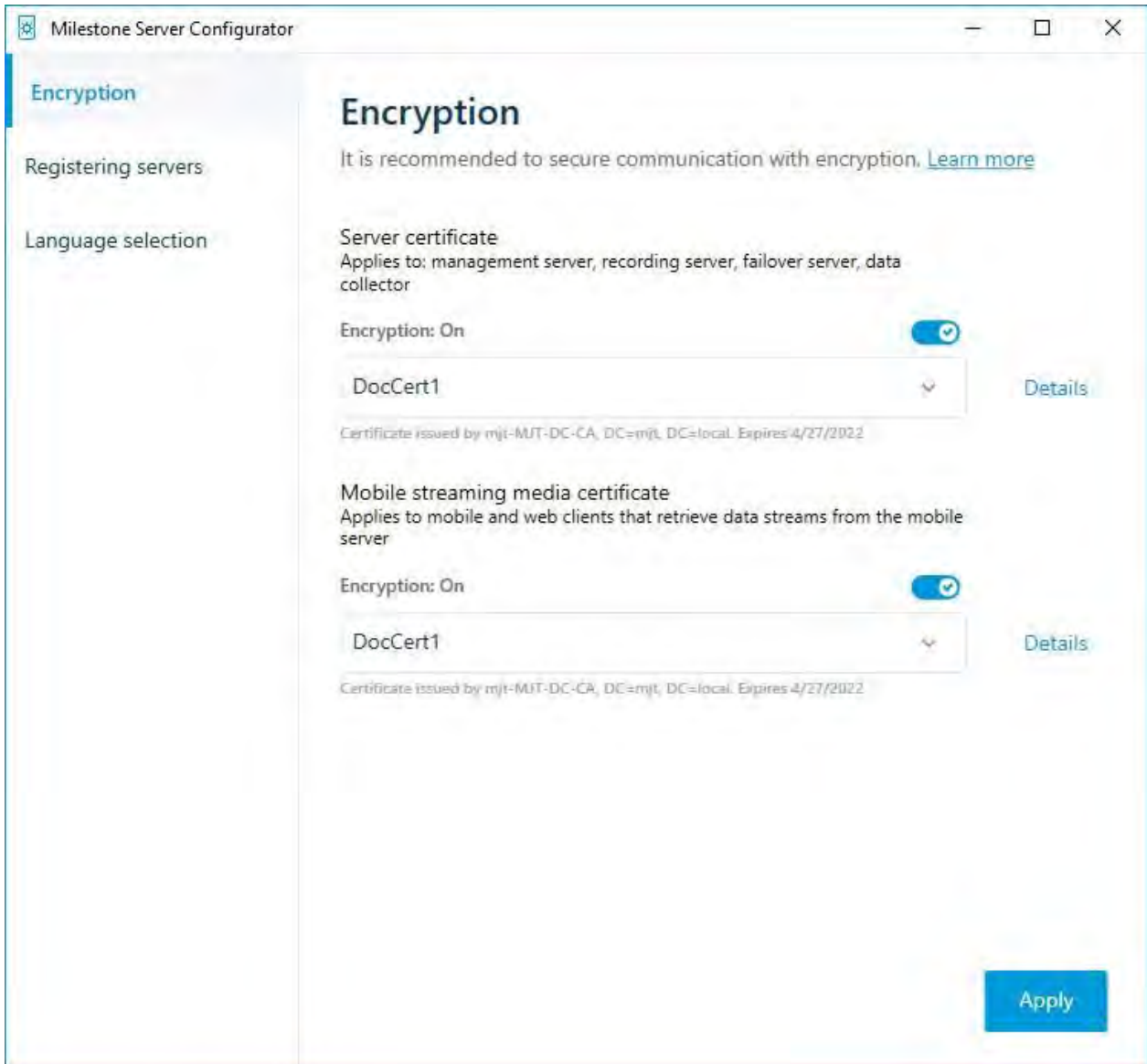
- Server di gestione
- Server di registrazione
- Server di eventi
- Server mobili

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
 - o
- 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



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.

Nella sezione **Crittografia** del Server Configurator, impostare la crittografia dei seguenti tipi:

- **Certificato server**

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

- **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.

- **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.

- **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**.

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.

Creazione e distribuzione manuale dei certificati

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**).
2. 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.

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.



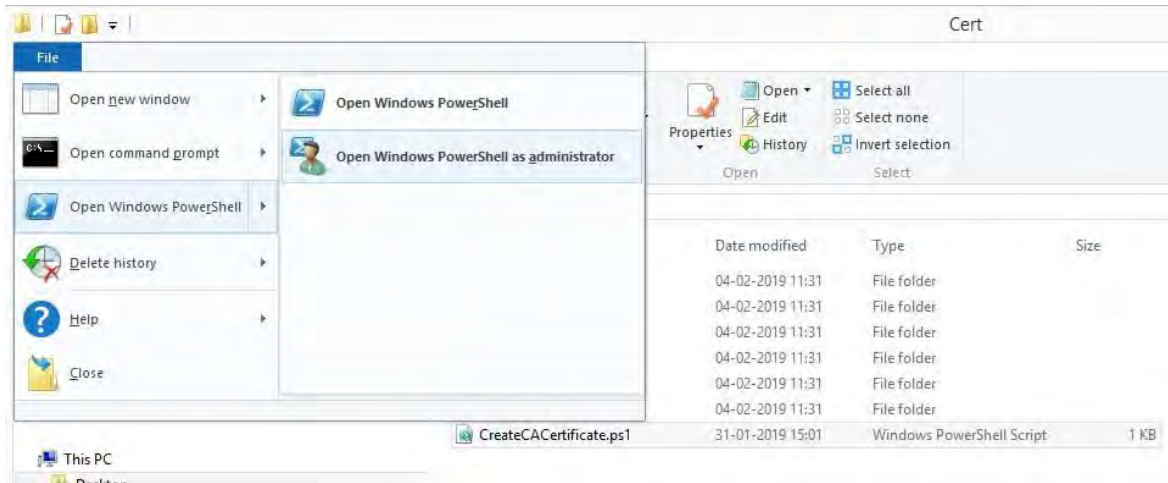
È molto importante che le righe si interrompano negli stessi punti dell'Appendice A. Puoi aggiungere le interruzioni di riga in Blocco note o, in alternativa, riaprire questo PDF con Google Chrome, copiare nuovamente il contenuto e incollarlo in Blocco note.

```

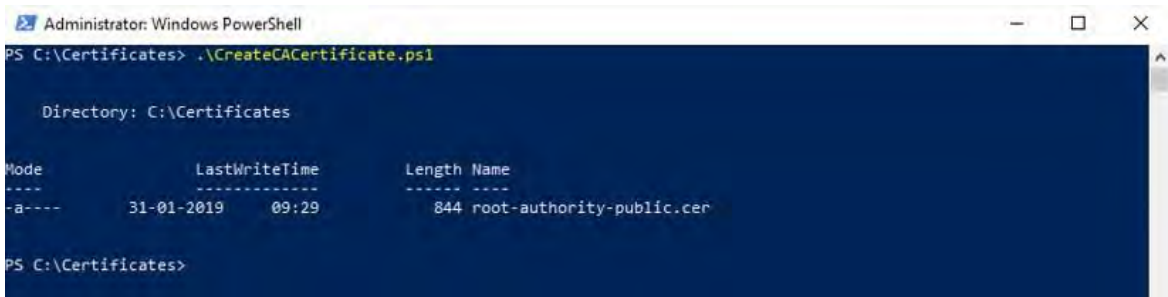
File Edit Format View Help
# Run this script once, to create a certificate that can sign multiple recording server certificates
# Private certificate for signing other certificates (in certificate store)
$ca_certificate = New-SelfSignedCertificate -CertStoreLocation cert:\CurrentUser\My -DnsName 'VMS Certificate Authority' -KeyUsageProperty All `
-KeyUsage CertSign, CRLSign, DigitalSignature -FriendlyName 'VMS CA Certificate'
# Thumbprint of private certificate used for signing other certificates
Set-Content -Path "$PSScriptRoot\ca_thumbprint.txt" -Value $ca_certificate.Thumbprint
# Public CA certificate to trust (Third-Party Root Certification Authorities)
Export-Certificate -Cert "Cert:\CurrentUser\My\${$ca_certificate.Thumbprint}" -FilePath "$PSScriptRoot\root-authority-public.cer"
Ln 8, Col 130

```


3. 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**.



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




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

 Il computer potrebbe richiedere la modifica dei criteri di esecuzione di PowerShell. In caso affermativo, immettere **Set-ExecutionPolicy RemoteSigned**. Premere **Invio** e selezionare **A**.

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](#).

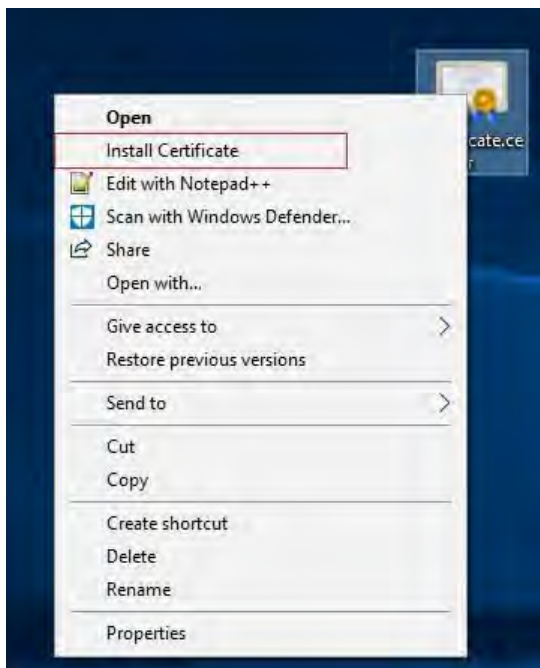
 Vedere [Importazione dei certificati client a pagina 129](#) per una procedura alternativa all'installazione manuale dei certificati sui client.

1. 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](#).

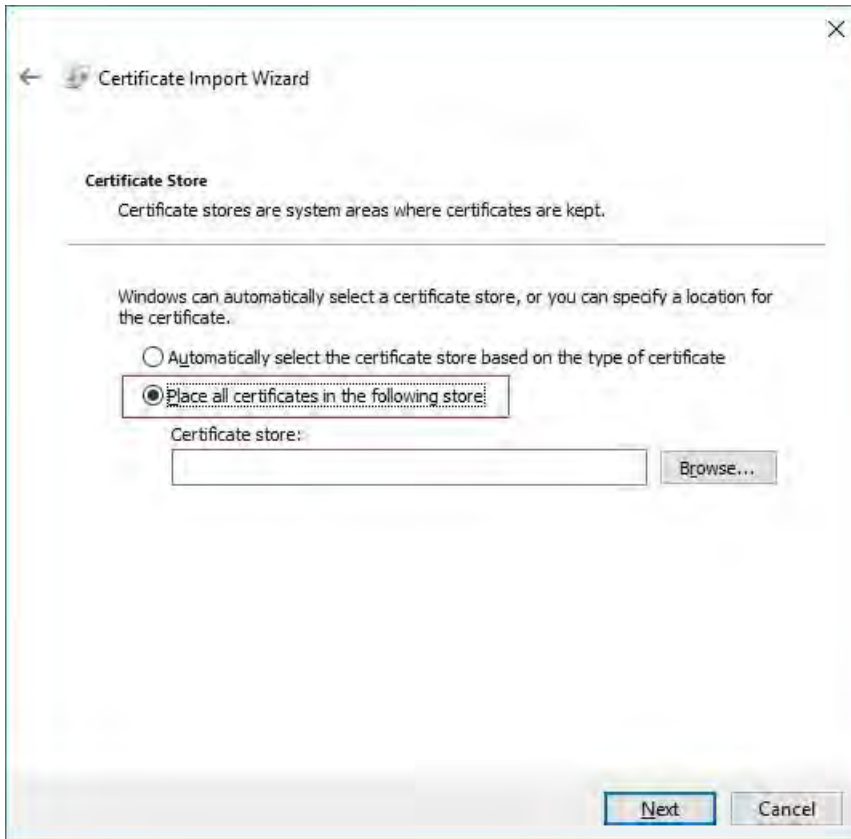
2. Fare clic con il pulsante destro del mouse sul certificato e selezionare **Installa certificato**.



3. Nell' **Importazione guidata certificati**, selezionare per installare il certificato nell'archivio del **computer locale** e fare clic su **Avanti**.



4. Selezionare questa opzione per individuare manualmente l'archivio in cui verrà installato il certificato.



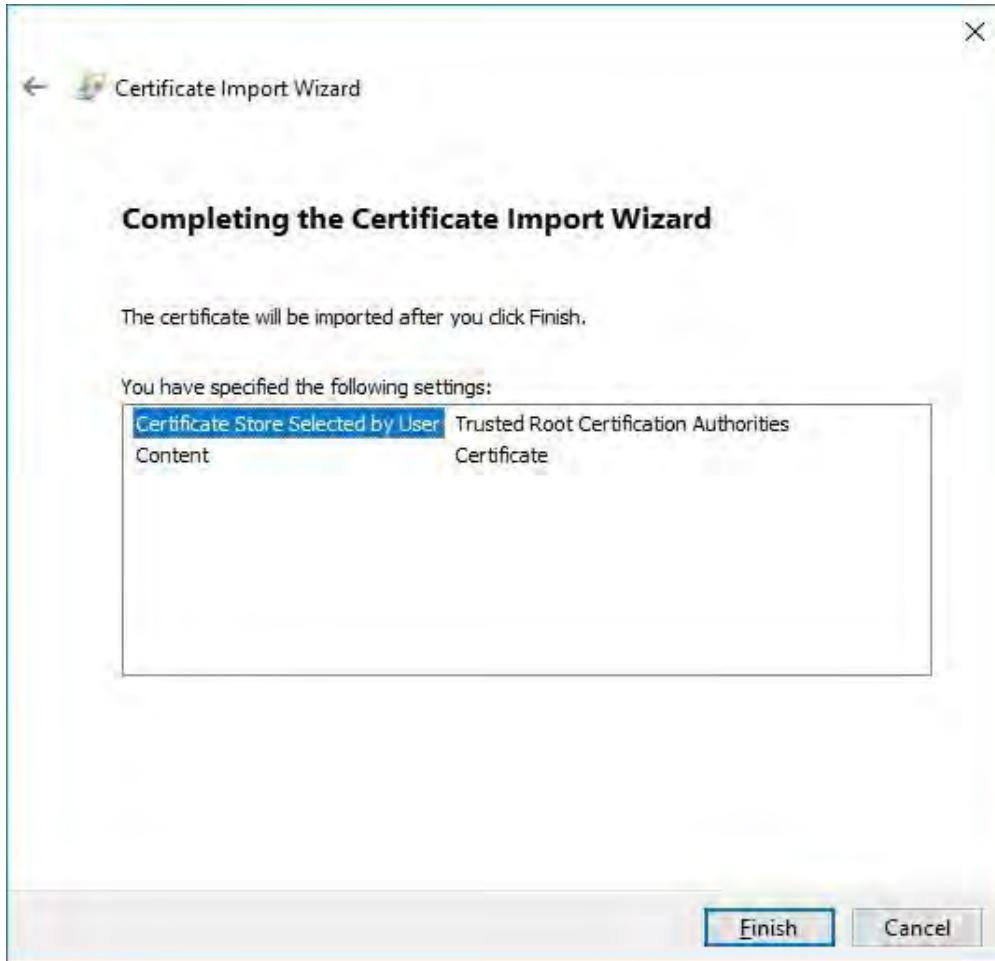
5. Fare clic su **Sfogli**, selezionare **Autorità di certificazione radice attendibili** e fare clic su **OK**. Quindi fare clic su **Avanti**.



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



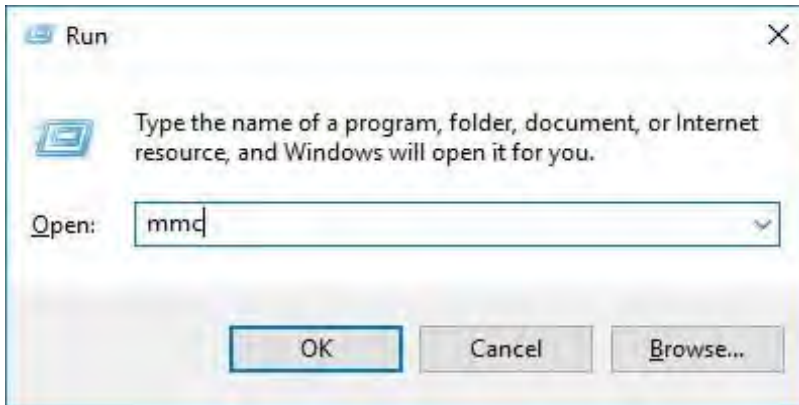
Se viene visualizzato un avviso di sicurezza che indica che si sta per installare un certificato radice, fare clic su **Sì** per continuare.



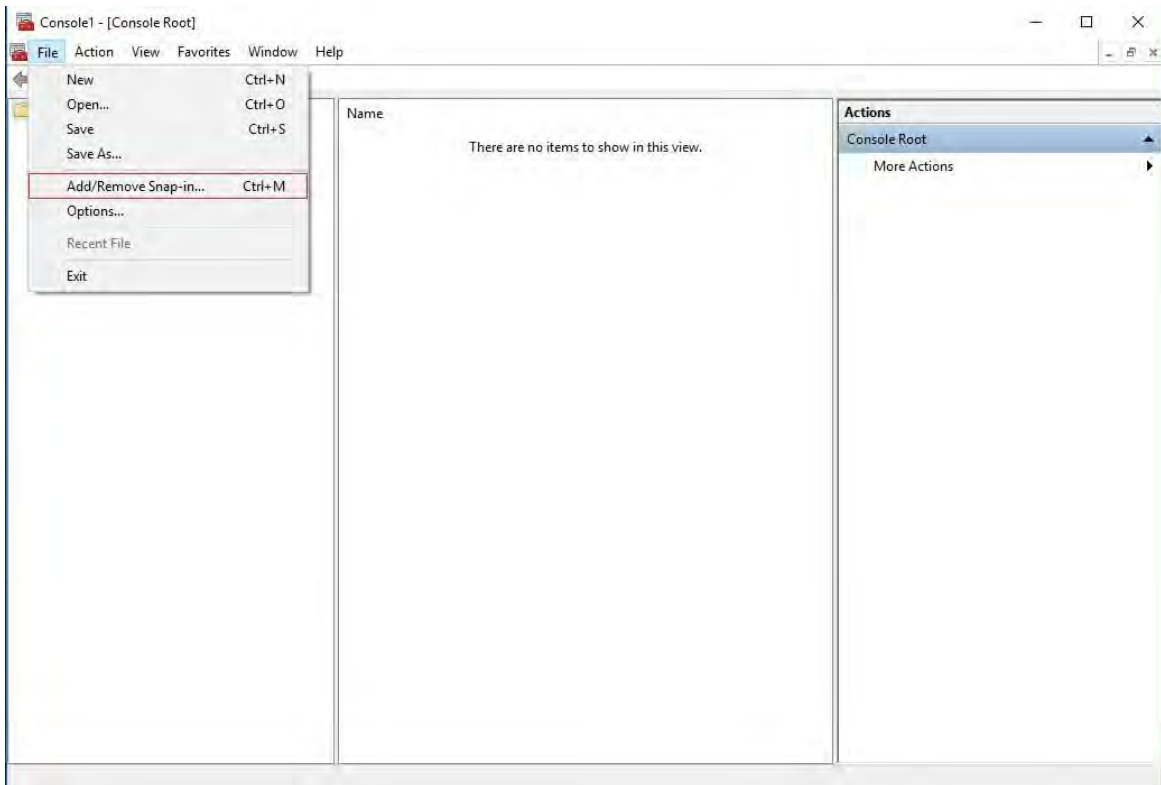
7. Riceverai una finestra di dialogo di conferma dell'avvenuta importazione.



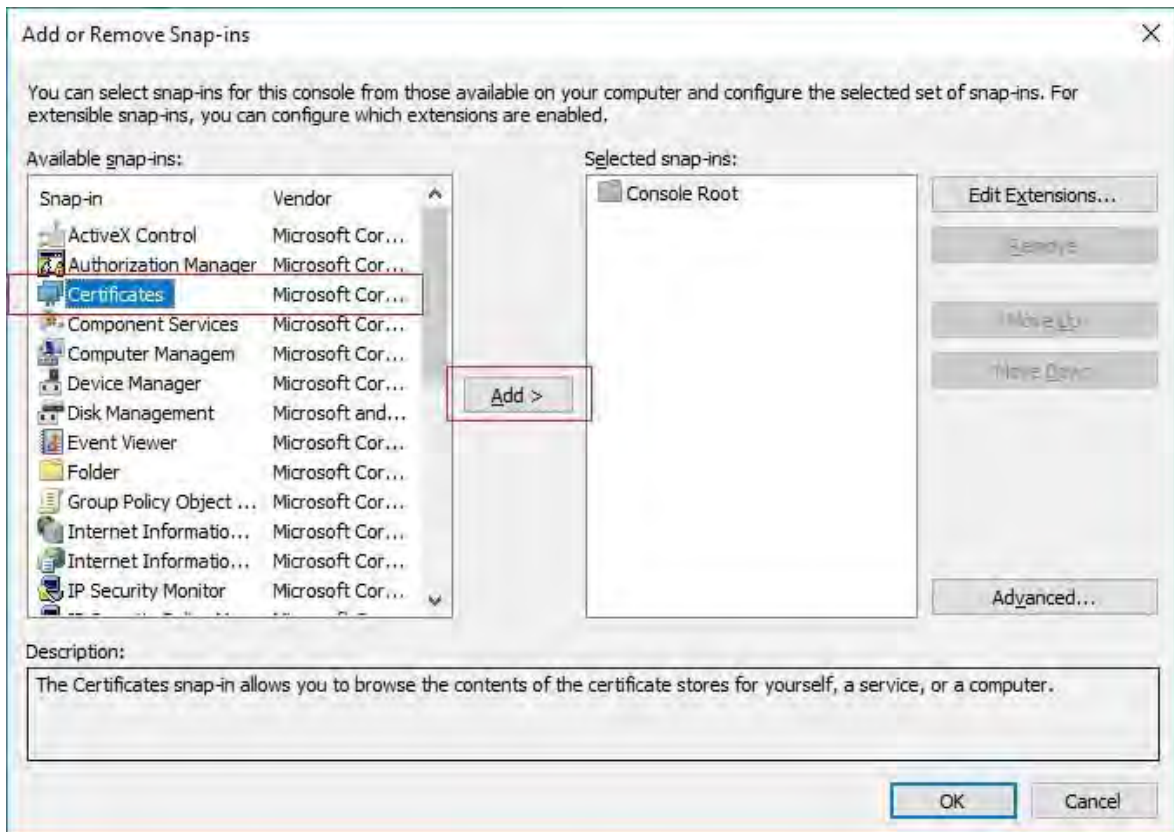
8. Per verificare che il certificato sia stato importato, avviare Microsoft Management Console.



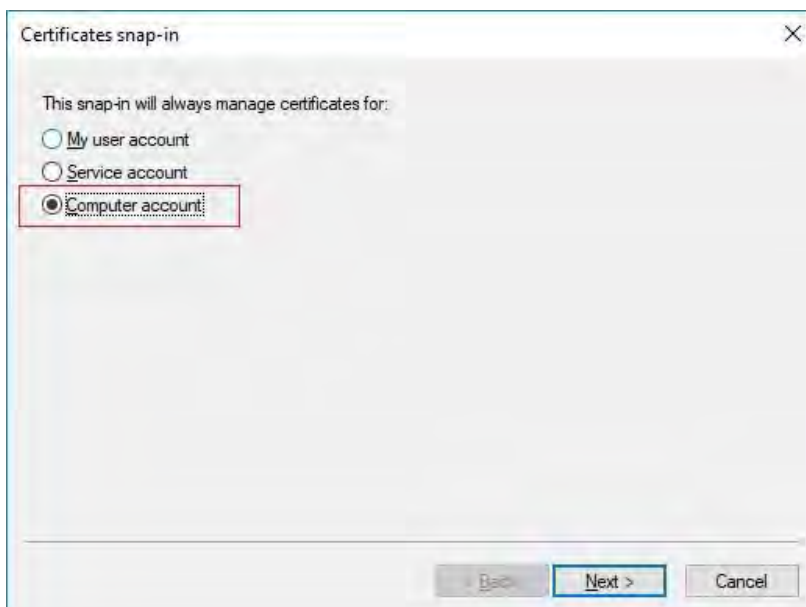
9. In Microsoft Management Console, dal menu **File** selezionare **Aggiungi/Rimuovi snap-in....**



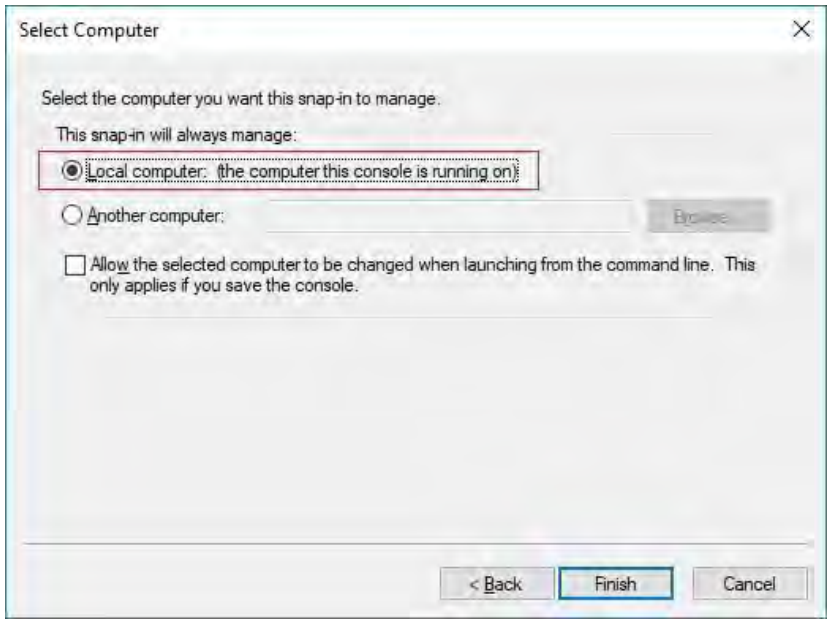
10. Selezionare lo snap-in Certificati e fare clic su **Aggiungi**.



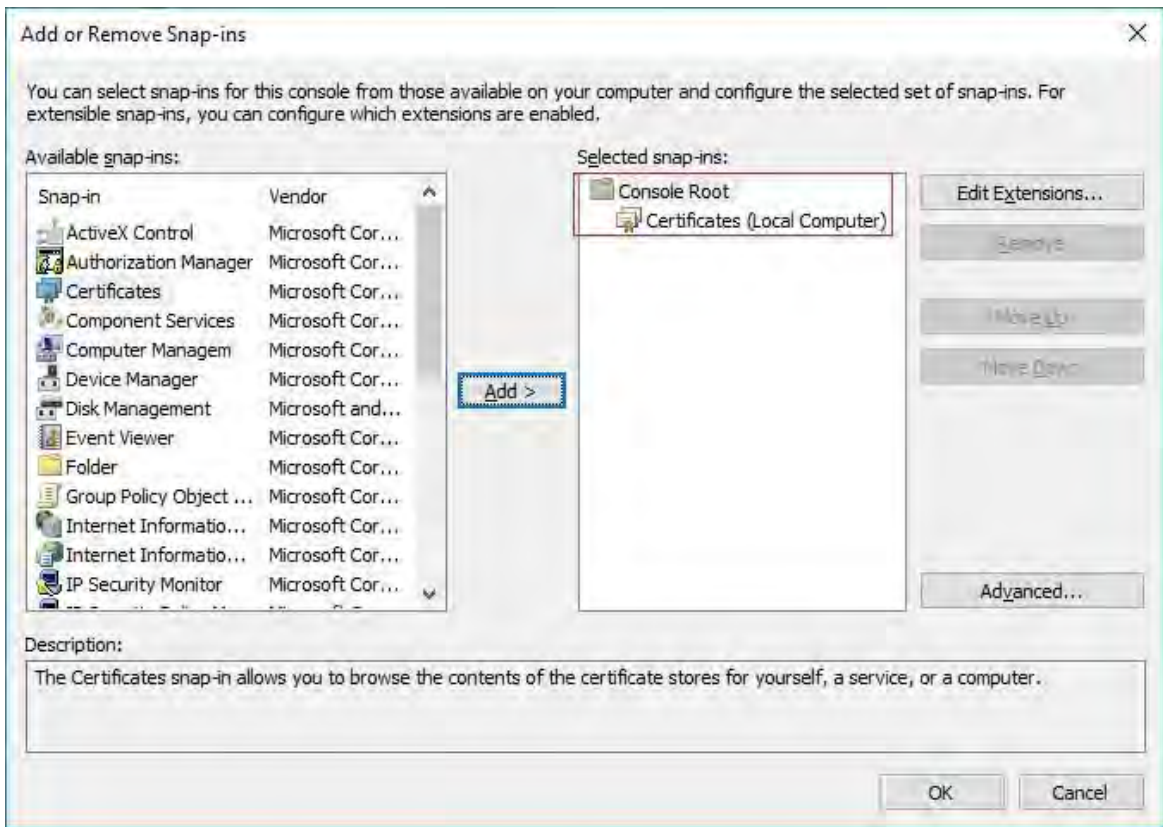
11. Selezionare l'opzione che lo snap-in deve gestire i certificati per l' **account computer**.



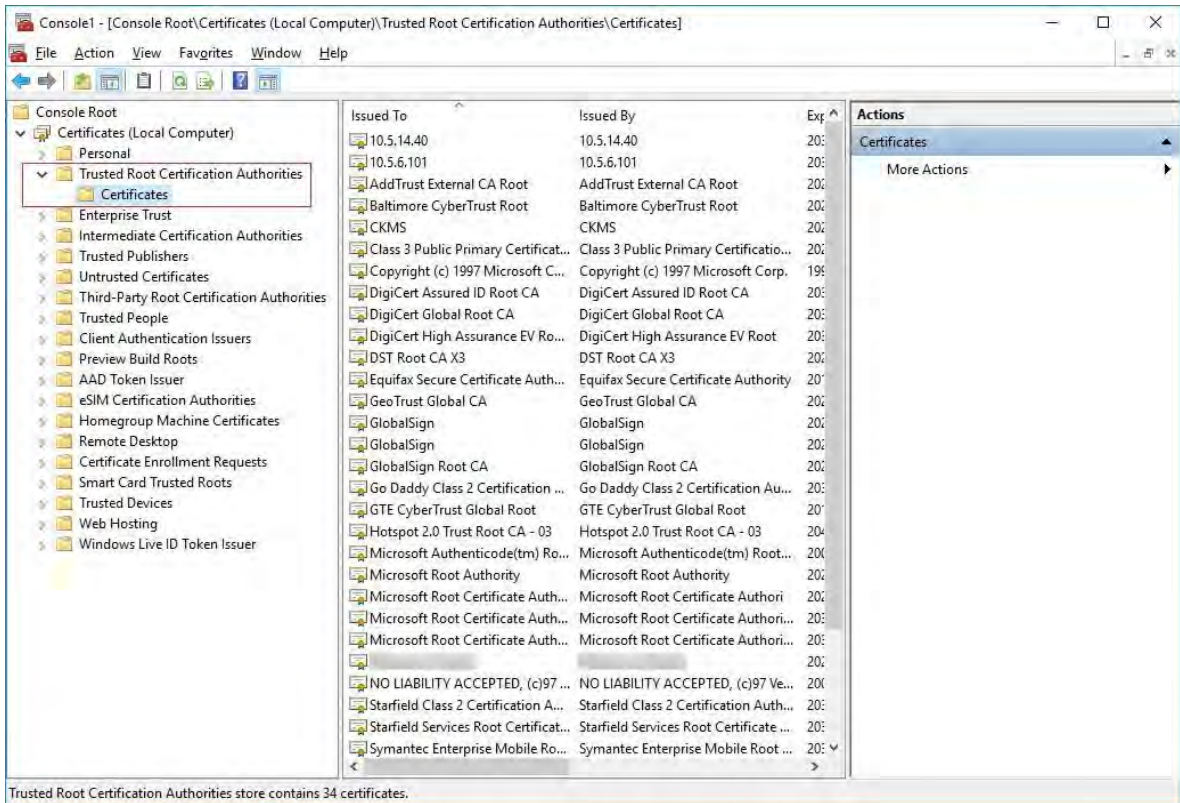
12. Selezionare **Computer locale** come computer che si desidera gestire con lo snap-in e fare clic su **Fine**.



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



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



- 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.

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).




Se si desidera configurare un server di gestione del failover, è necessario creare un certificato SSL diverso. Per ulteriori informazioni, vedere [Creazione di un certificato SSL per il server di gestione failover a pagina 38](#).

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.

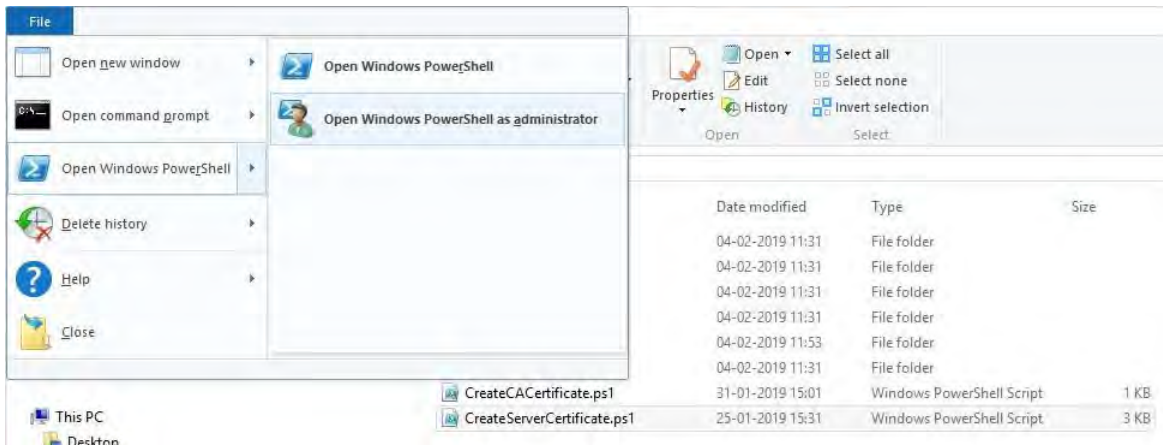


Il computer usato per la creazione dei certificati deve eseguire Windows 10 o Windows Server 2016 o versioni successive.


1. Nell'Appendice B alla fine di questa guida, è disponibile uno script per la creazione di certificati server.
2. Apri Blocco note e incolla il contenuto.

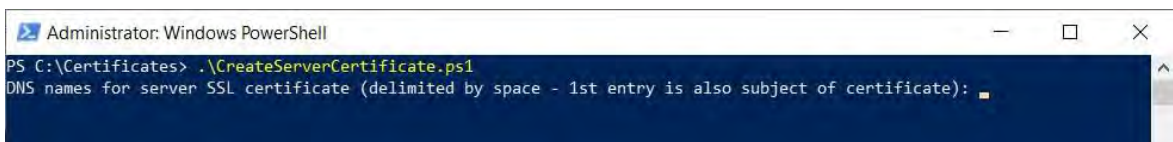
 È molto importante che le linee si interrompano negli stessi punti dell'Appendice B. Puoi aggiungere le interruzioni di riga in Blocco note o, in alternativa, riaprire questo PDF con Google Chrome, copiare nuovamente il contenuto e incollarlo in Blocco note.

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



6. In PowerShell al prompt immettere `.\CreateServerCertificate.ps1` e premere **INVIO**.
7. 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**.



8. 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**.

9. 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.

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

Importa certificato SSL

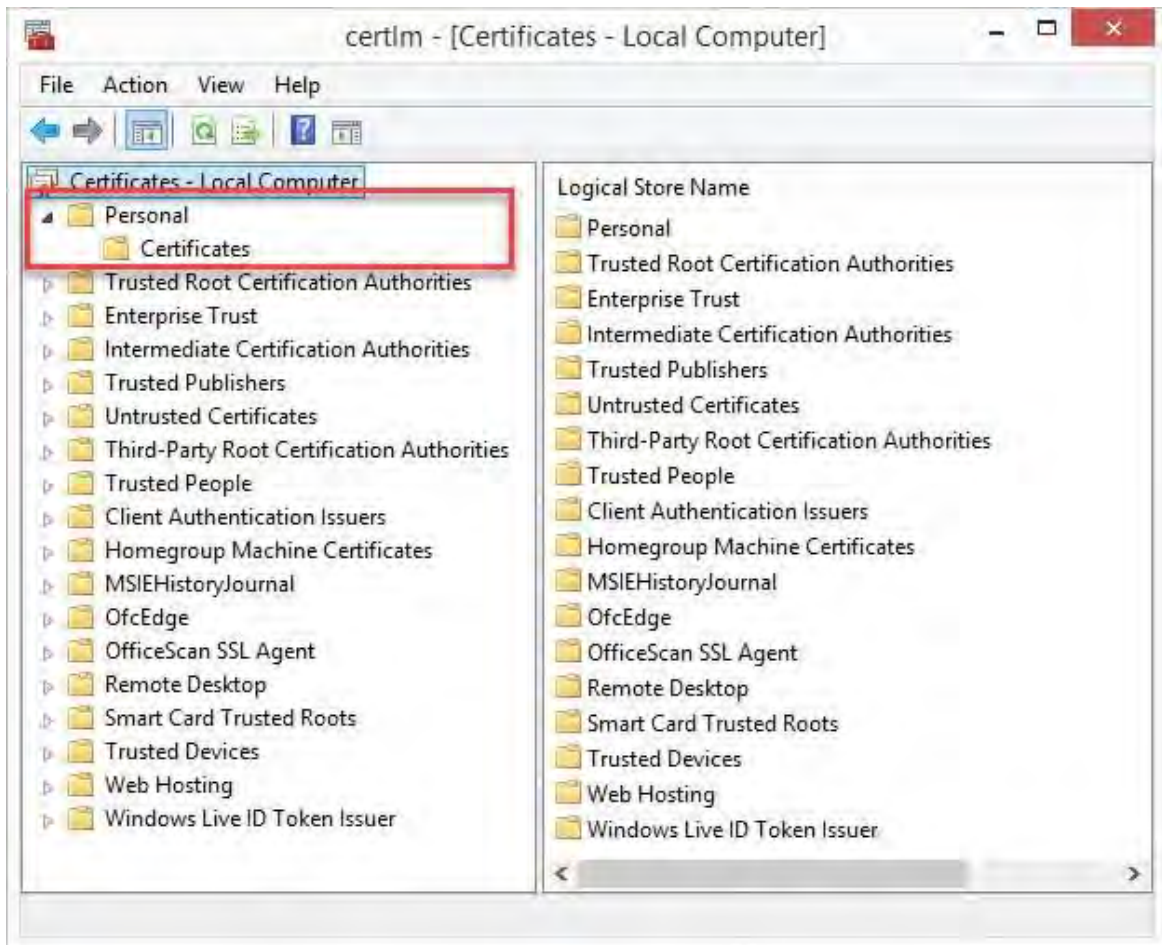
Dopo aver creato i certificati SSL, installarli nei computer che eseguono il servizio server.

1. Copiare il file Subjectname.pfx pertinente dal computer in cui è stato creato il certificato al computer del servizio server corrispondente.



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

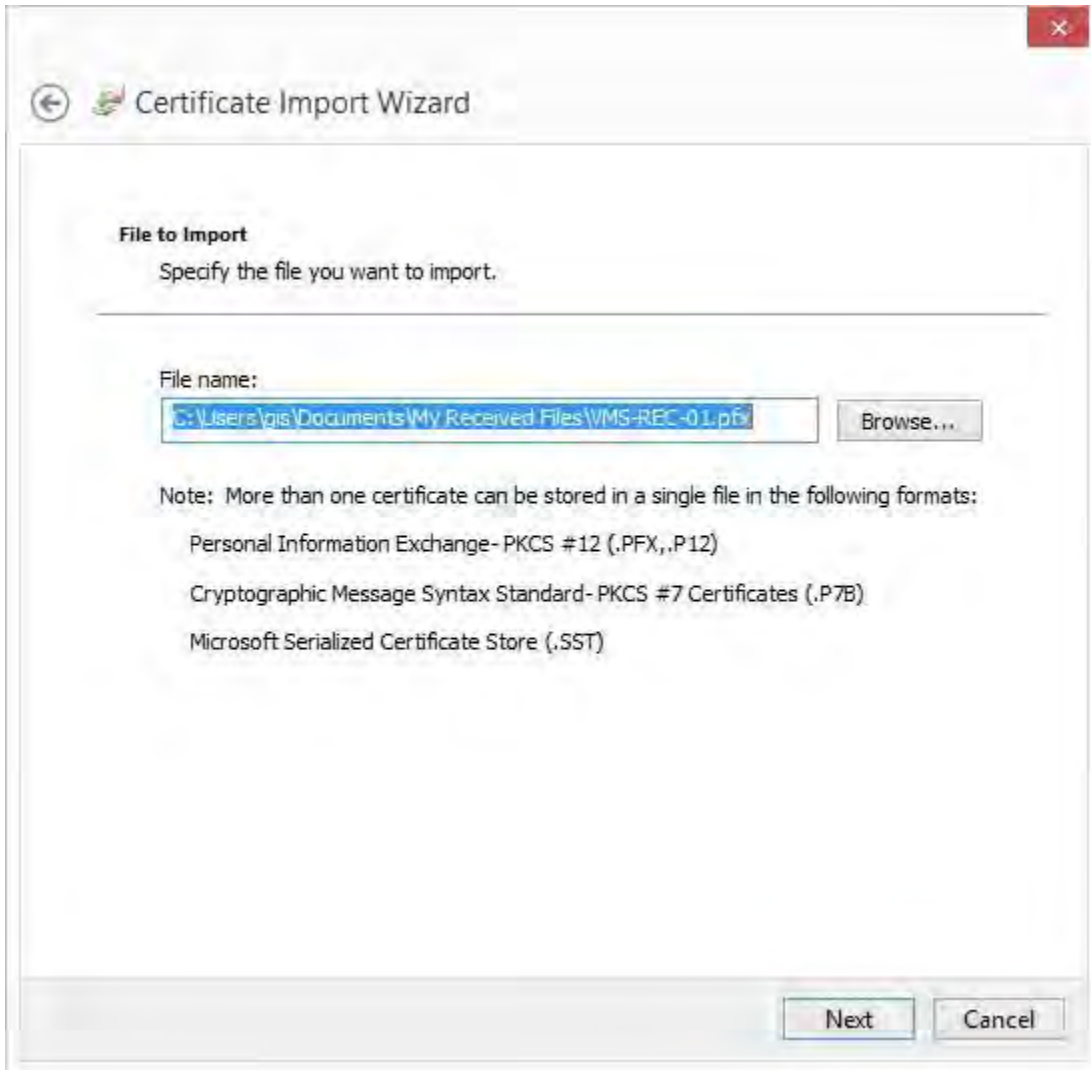
2. Nel computer del servizio server avviare Gestisci **certificati computer**.
3. Fare clic su **Personale**, fare clic con il pulsante destro del mouse su **Certificati** e selezionare **Tutte le attività** > **importare**.



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



5. Individuare il file del certificato e fare clic su **Avanti**.



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



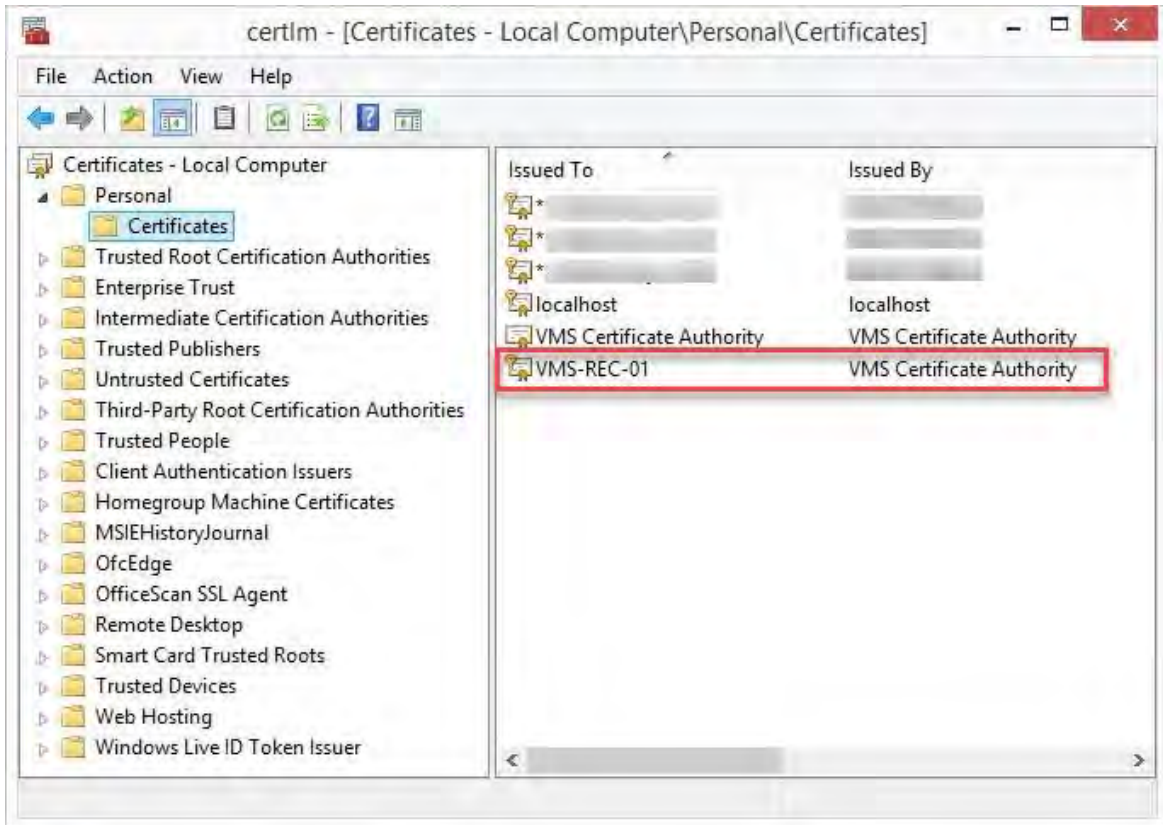
7. Inserire il file nell'**archivio certificati: Personale**, quindi fare clic su **Avanti**.



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

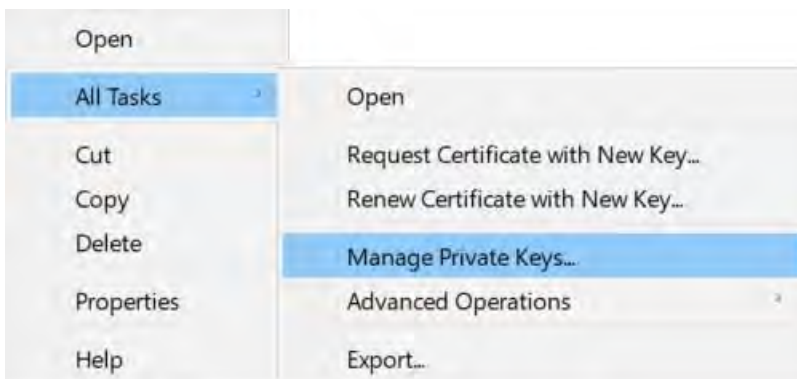


9. Il certificato importato viene visualizzato nell'elenco.

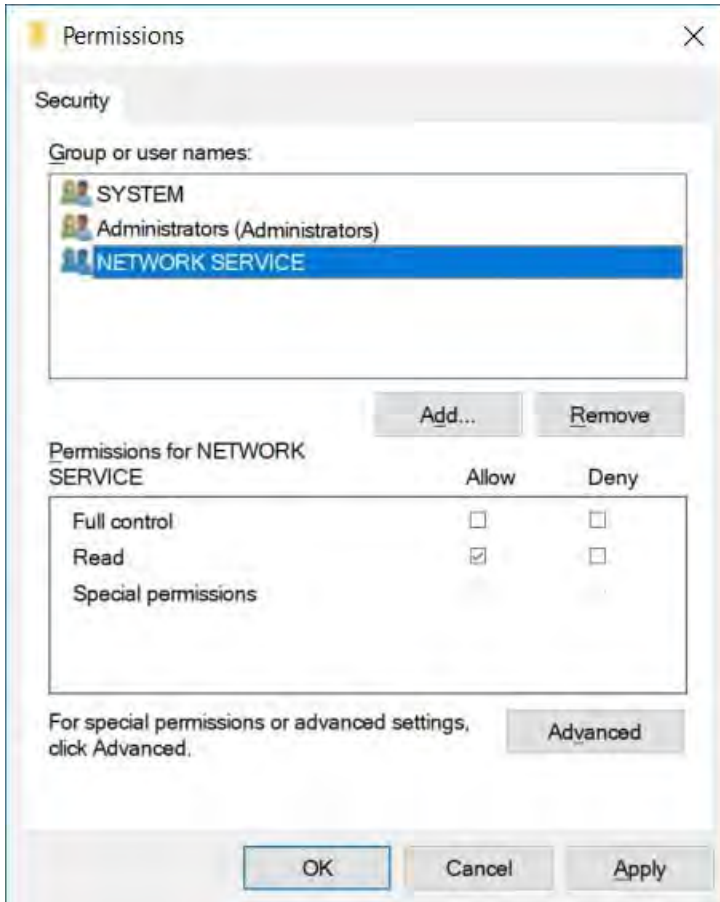


10. Per consentire a un servizio di utilizzare la chiave privata del certificato, fare clic con il pulsante destro del mouse sul certificato e selezionare **Tutte le attività** >

Gestisci le chiavi private.



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



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

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.



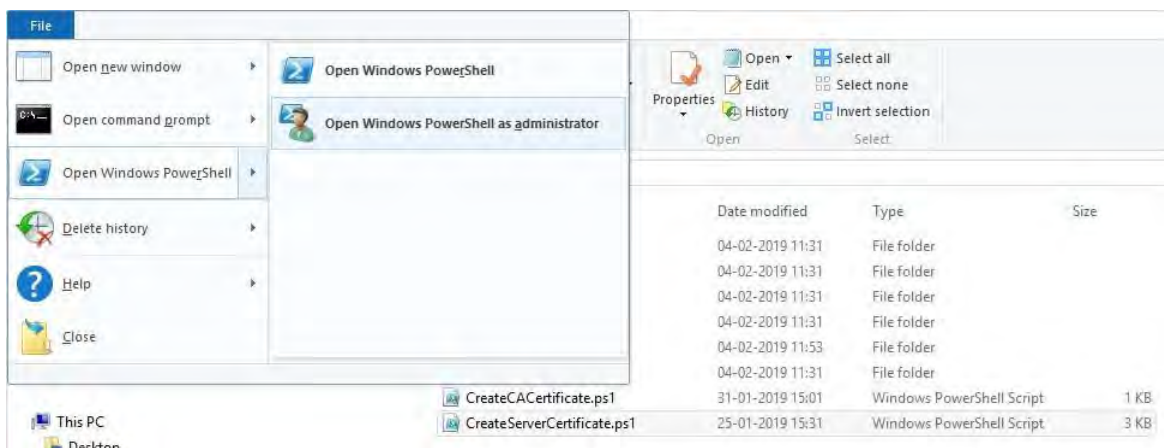
Il computer usato per la creazione dei certificati deve eseguire Windows 10 o Windows Server 2016 o versioni successive.

1. Nell'Appendice C di questa guida copiare lo script per la creazione dei certificati del server di gestione del failover.
2. 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.

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



6. In PowerShell immettere `.\CreateFailoverCertificate.ps1` al prompt e premere **INVIO**.

7. 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.

Premere **Invio**.

8. Specificare l'indirizzo IP virtuale del cluster di failover. Premere **Invio**.
9. 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.

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.



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 sono gratuiti.

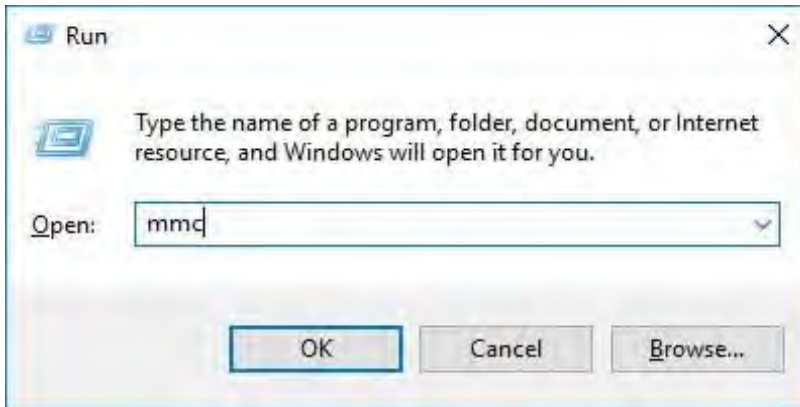
Aggiungere un certificato CA al server

Aggiungere il certificato CA al server mobile effettuando le seguenti operazioni.

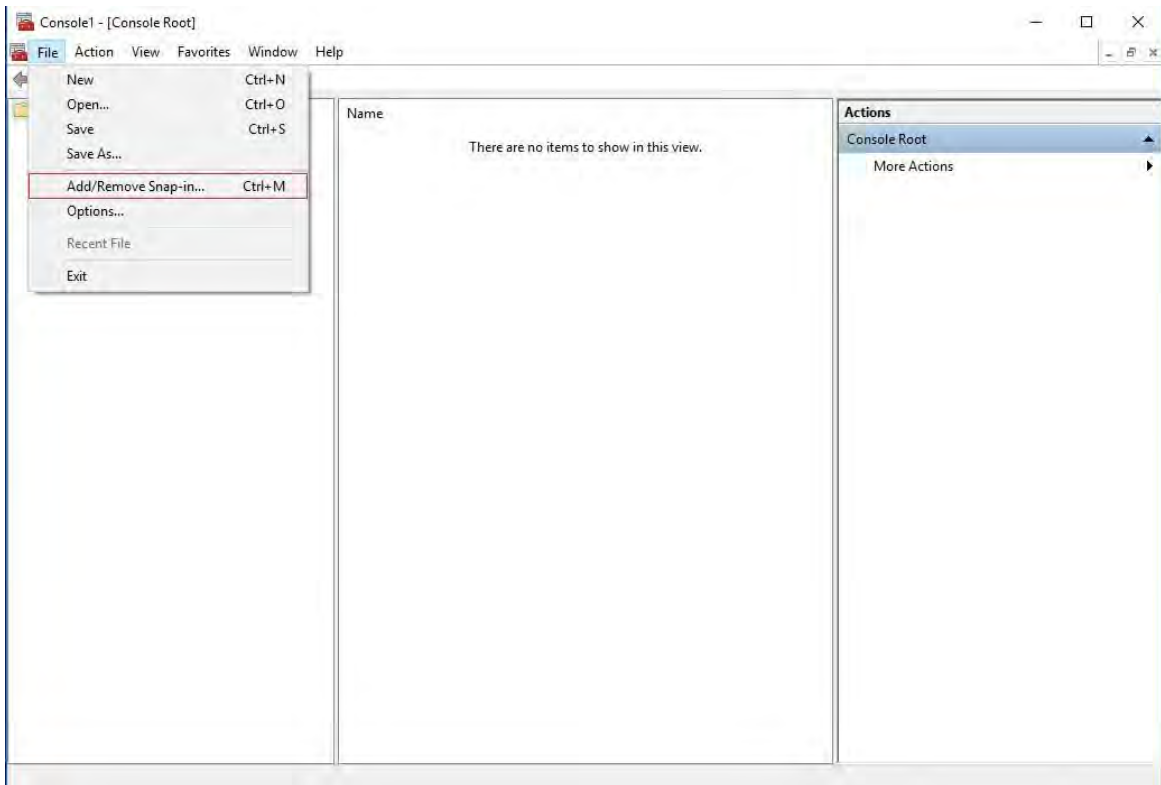


I parametri specifici dipendono dalla CA. Fare riferimento alla documentazione della CA prima di procedere.

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

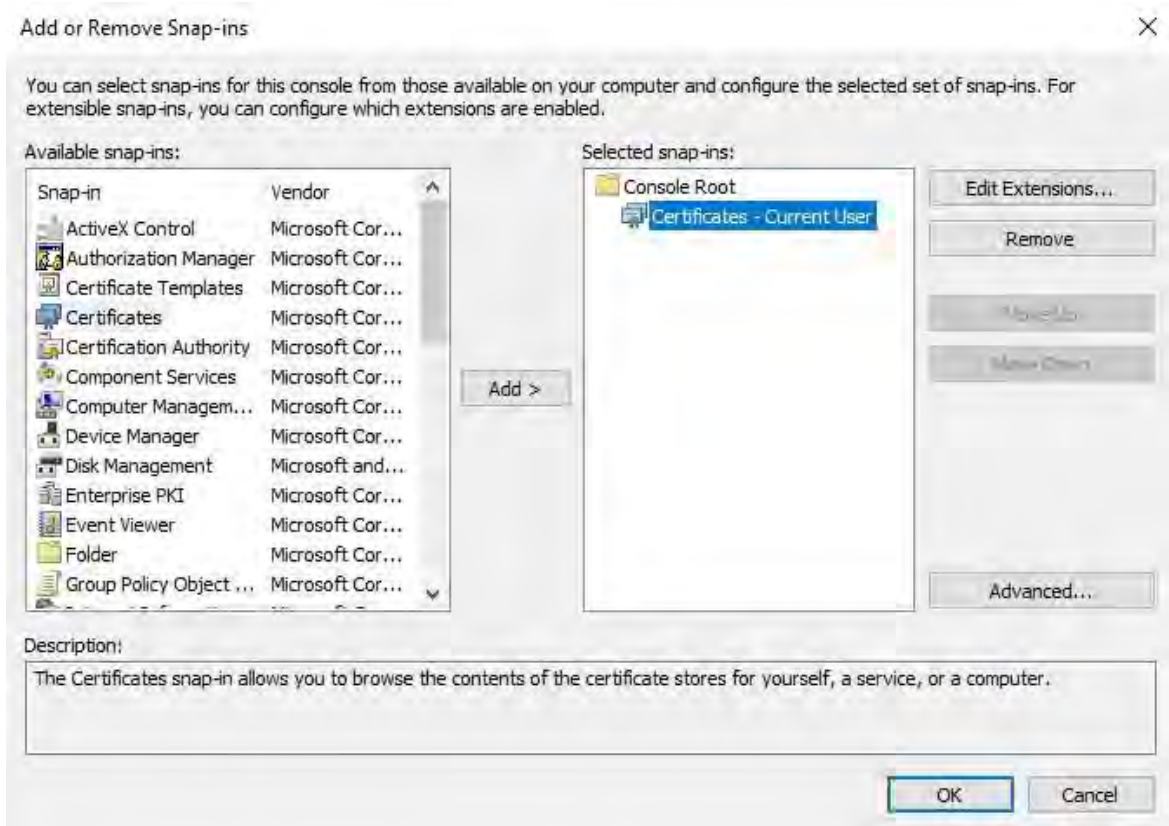


2. In Microsoft Management Console, dal menu **File** selezionare **Aggiungi/Rimuovi snap-in....**

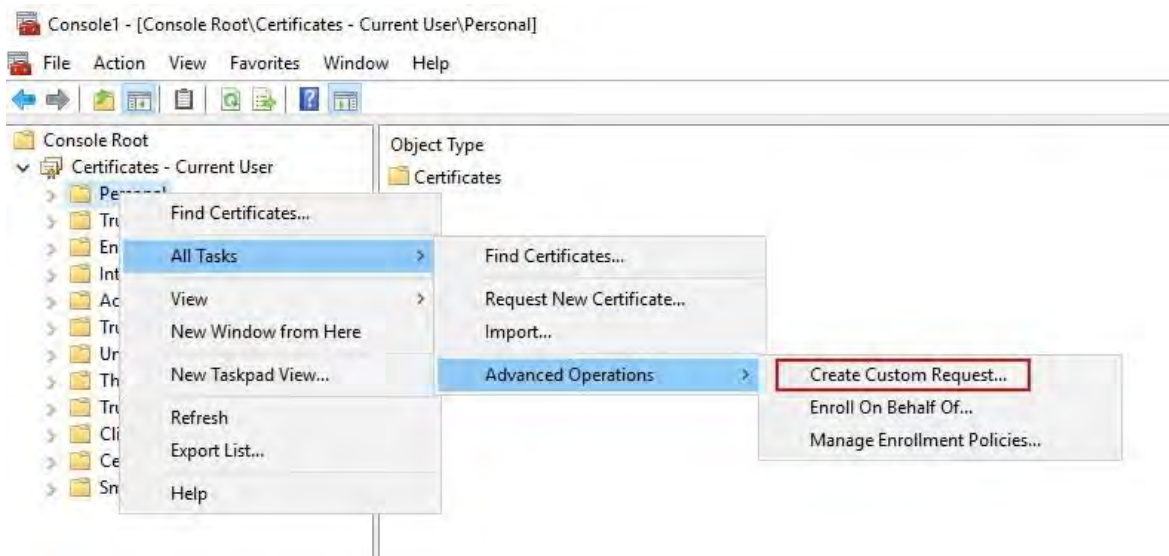


3. Selezionare lo snap-in Certificati e fare clic su **Aggiungi**.

Fare clic su **OK**.

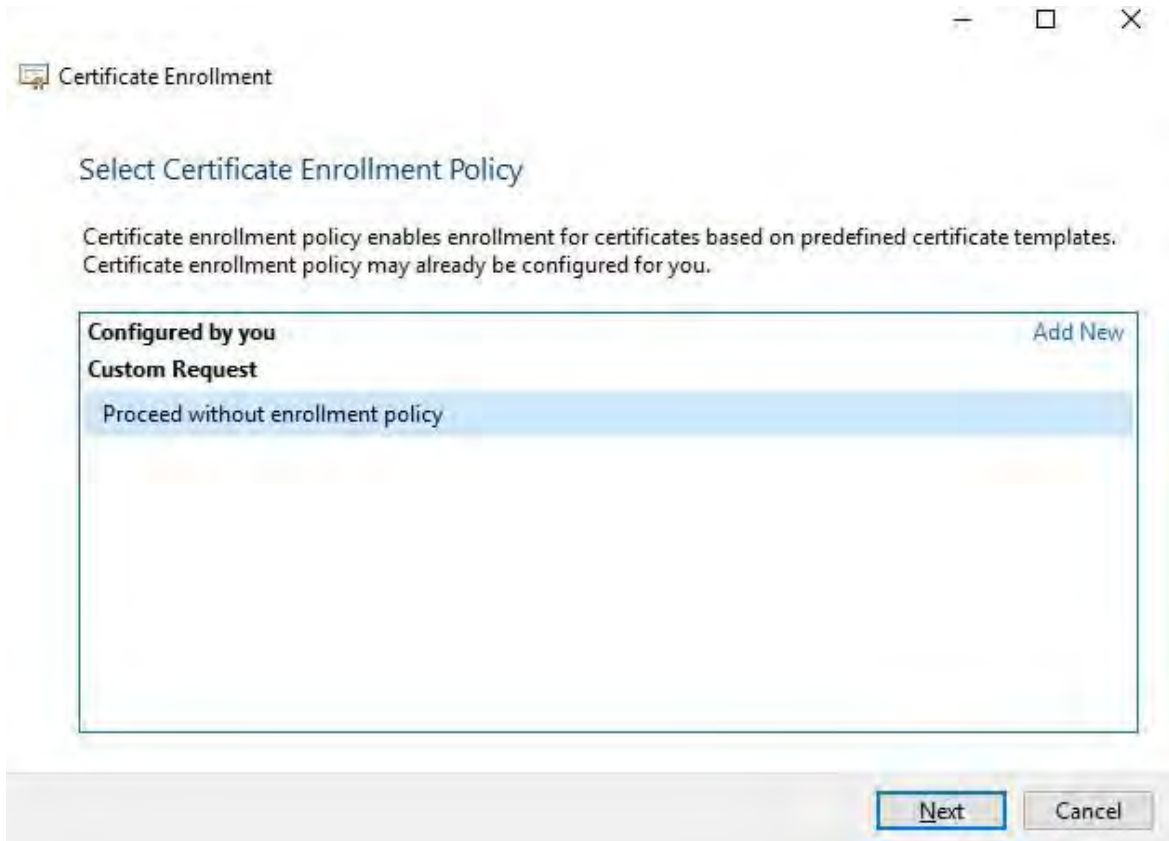


4. Espandere l'oggetto Certificati. Fare clic con il pulsante destro del mouse sulla **cartella Personale** e selezionare **Tutte le attività > Operazioni avanzate > Crea richiesta personalizzata**.

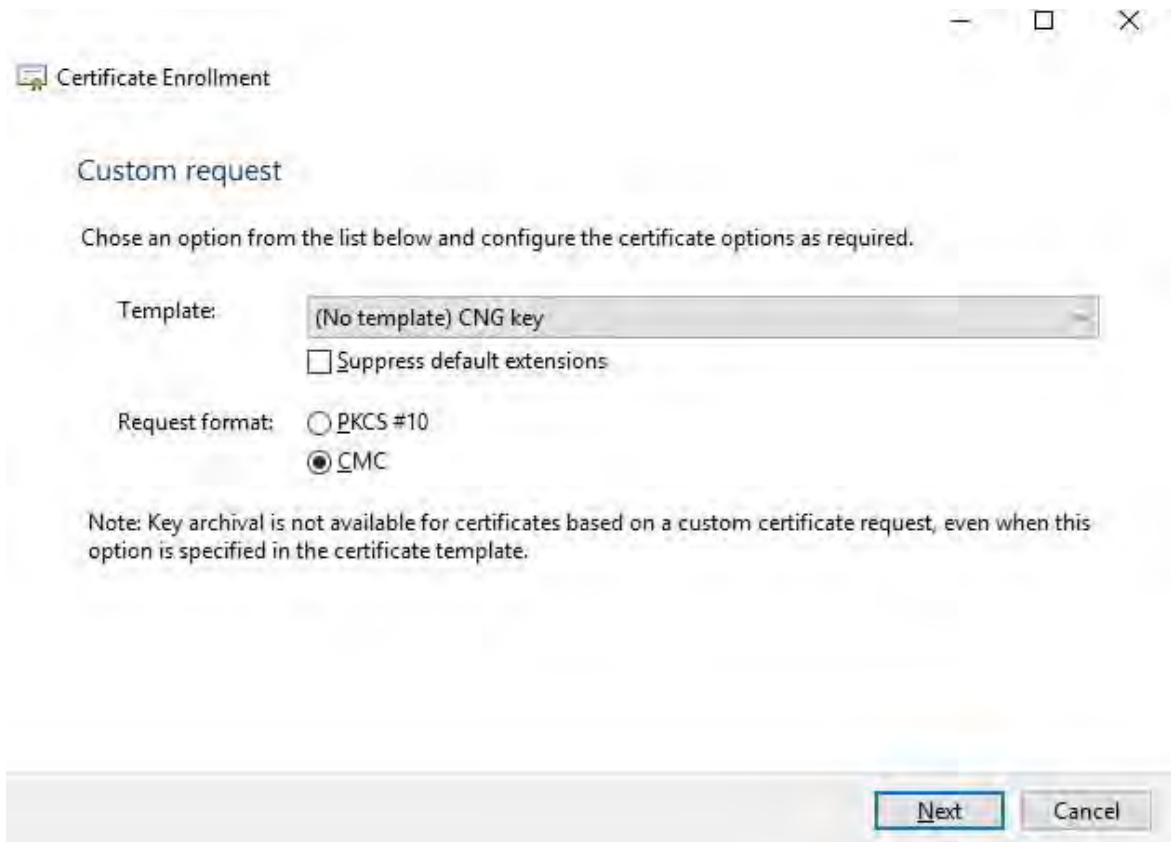



5. Fare clic su **Avanti** nella procedura guidata **Registrazione certificati** e selezionare **Procedi senza criteri di registrazione**.

Fare clic su **Avanti**.



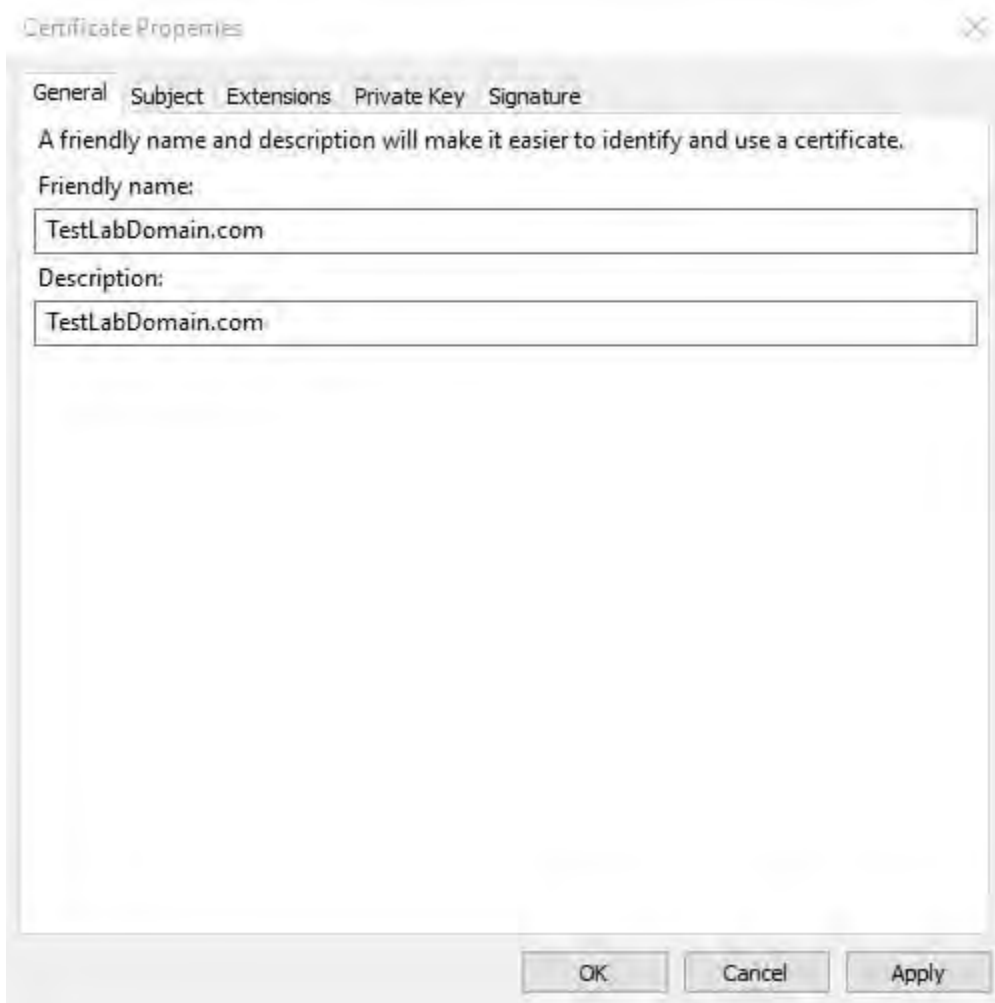
6. Selezionare il modello **di chiave CNG (Nessun modello)** e il formato di richiesta **CMC**, quindi fare clic su **Avanti**.



 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.

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

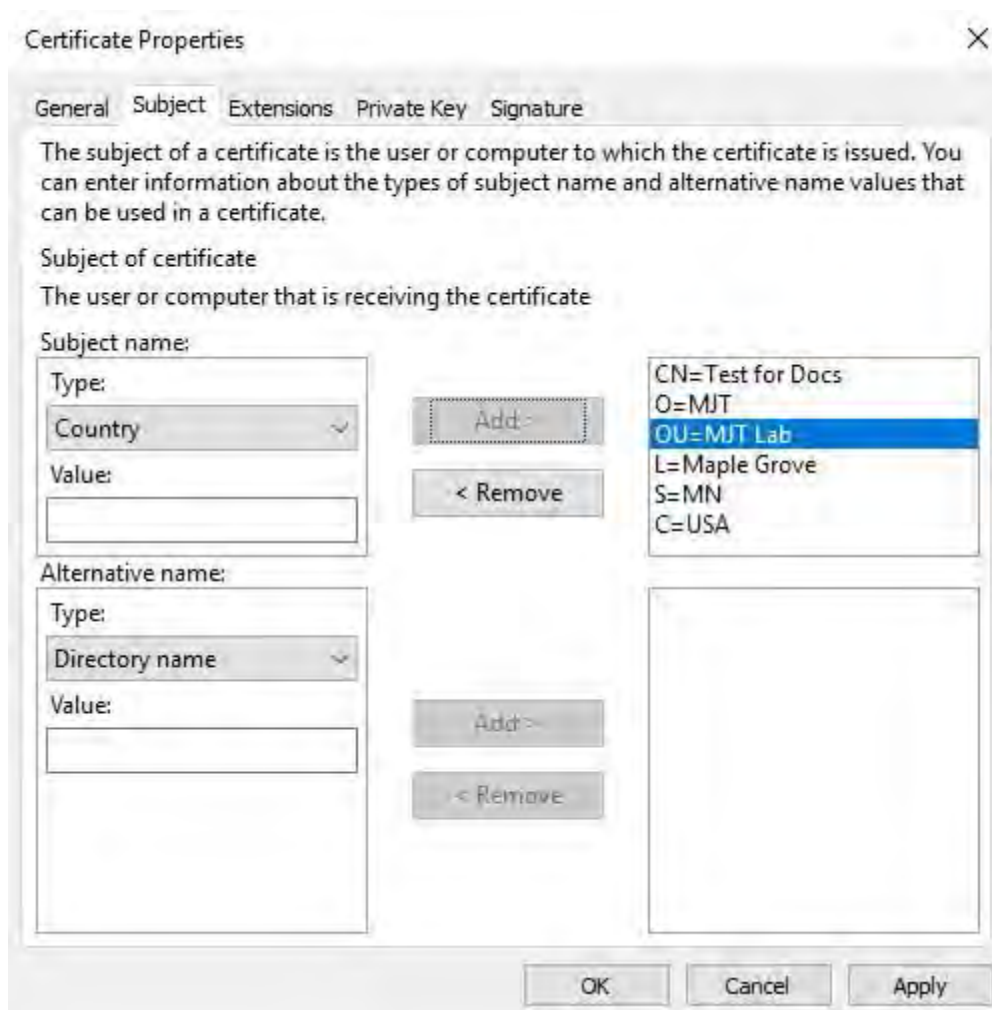
8. Nella scheda **Generale**, compila i campi **Nome descrittivo** e **Descrizione** con il nome di dominio registrato con la CA.



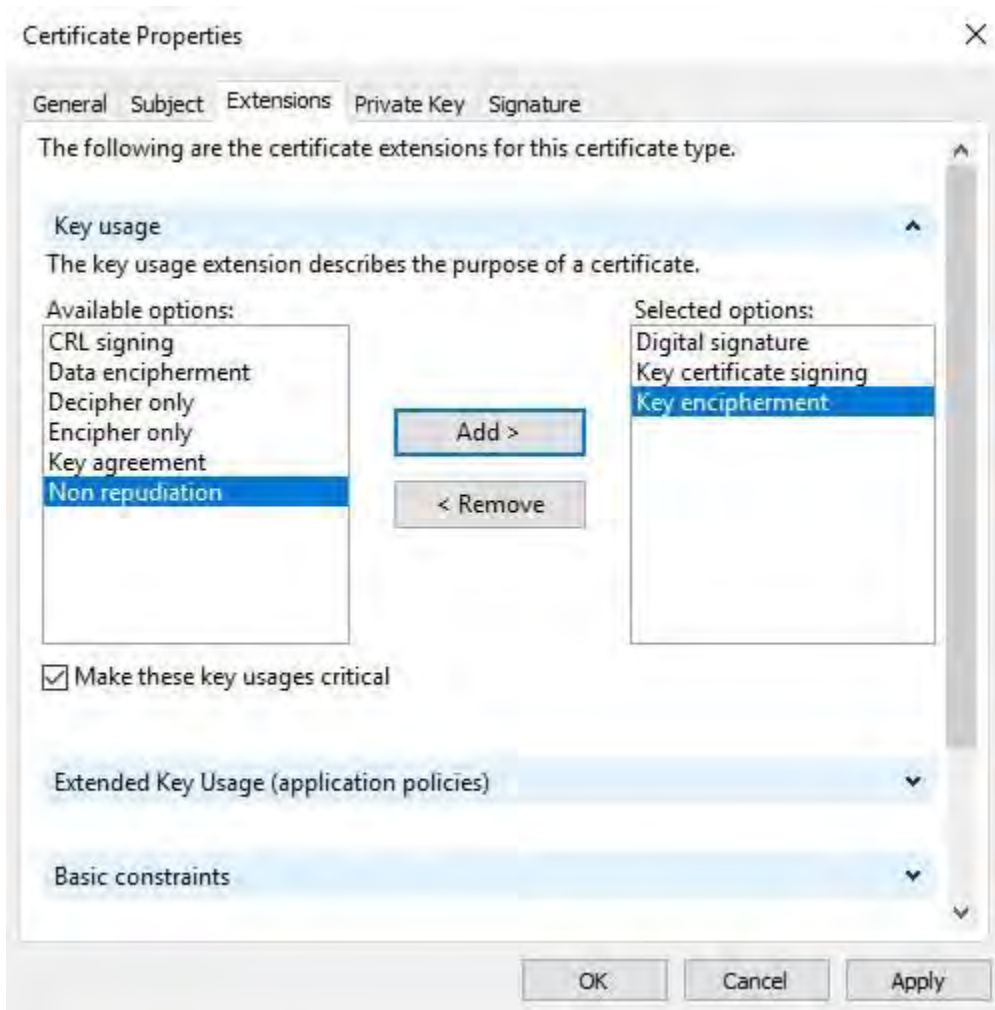
9. Nella scheda **Oggetto** immettere i parametri richiesti dalla CA specifica.

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:




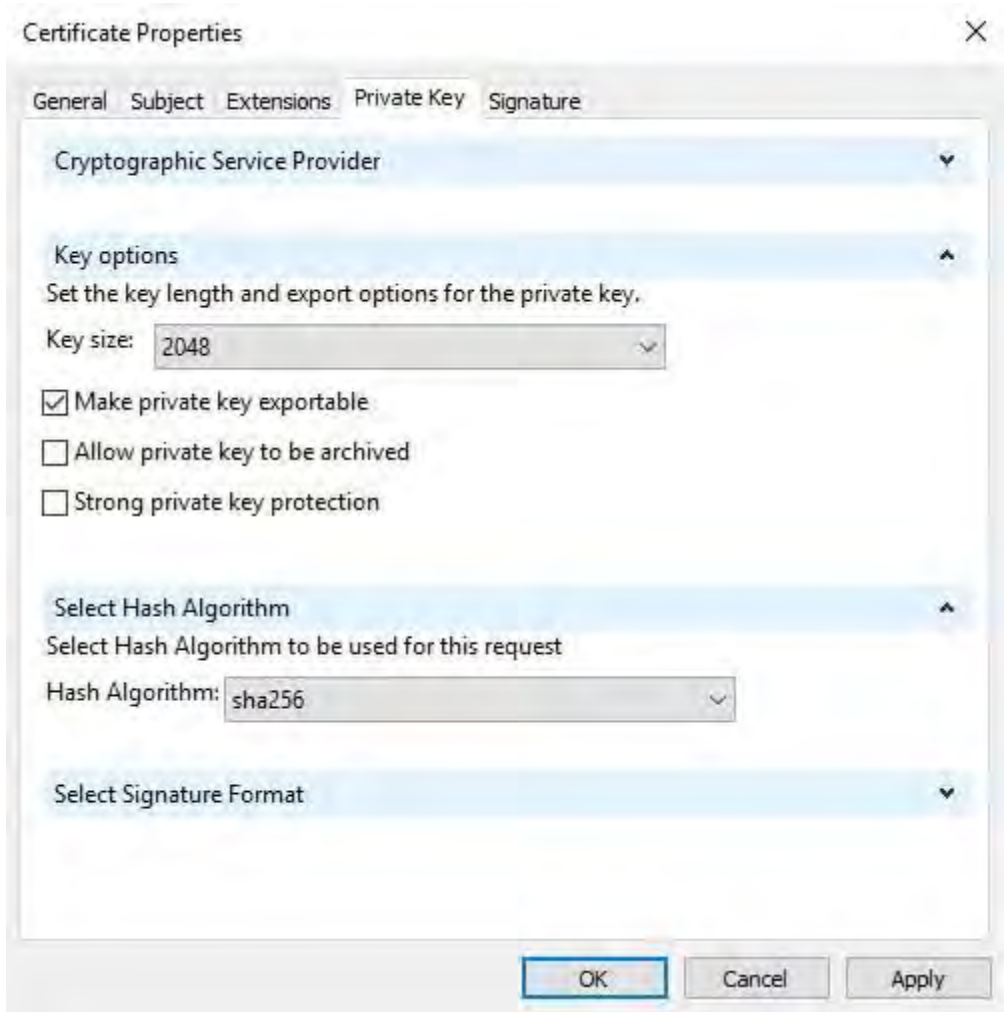
10. Alcune CA non richiedono estensioni. Tuttavia, se necessario, vai alla **scheda Estensioni** ed espandi il menu **Utilizzo chiavi** . Aggiungere le opzioni richieste dall'elenco Opzioni **disponibili** all' elenco **Opzioni selezionate**.



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

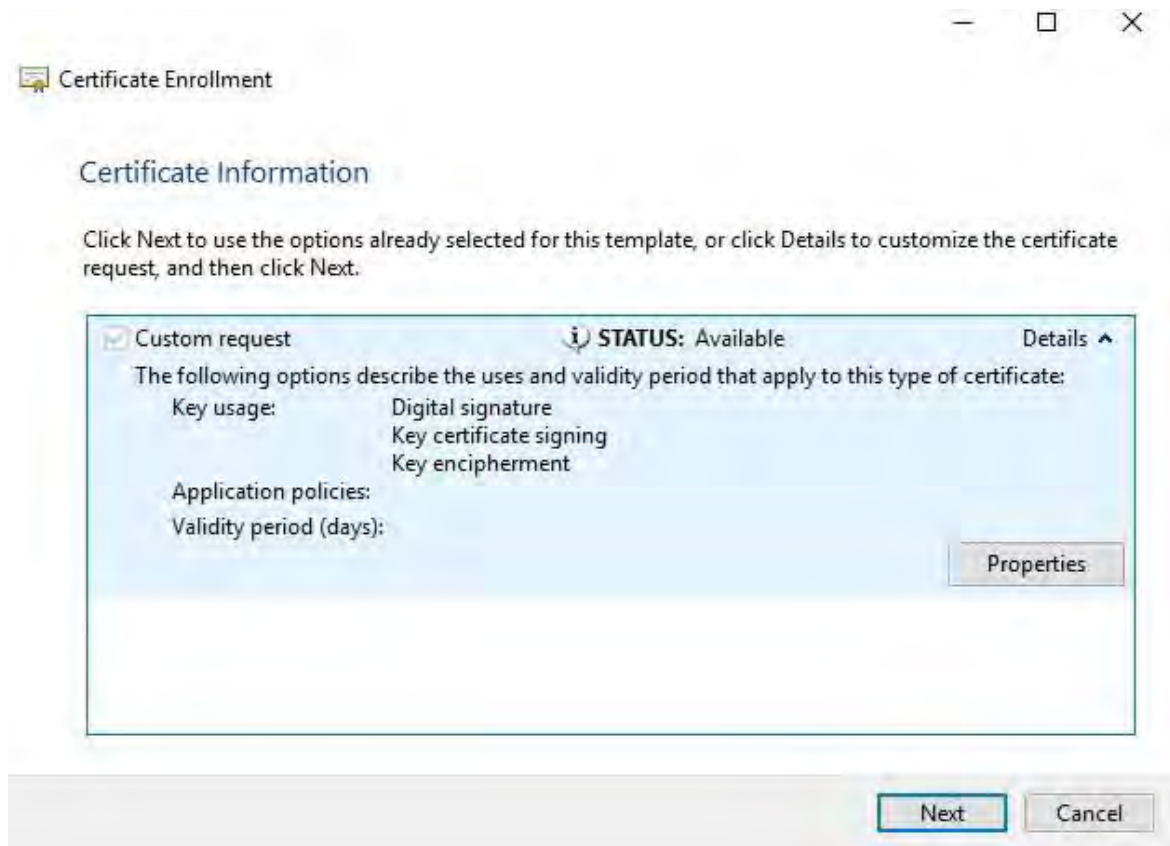
Imposta la dimensione della chiave su 2048 e seleziona l'opzione per rendere esportabile la chiave privata.

 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 prima di procedere al passaggio successivo.



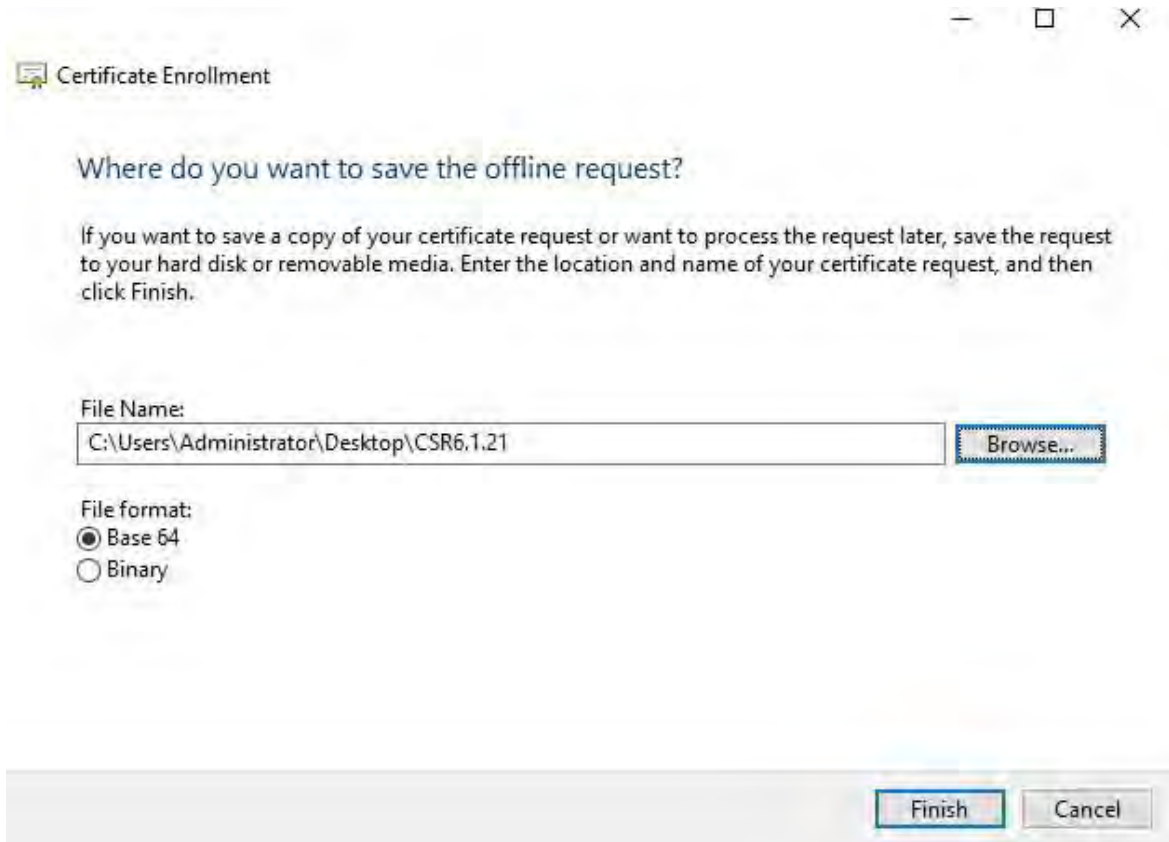
12. A meno che la CA non richieda una firma, il passaggio successivo consiste nel fare clic su **OK**.

- Quando tutte le proprietà del certificato sono state definite, fare clic su **Avanti** nella finestra di dialogo **Registrazione certificati** mago.



- 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.

15. Fare clic su **Fine**.



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

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.

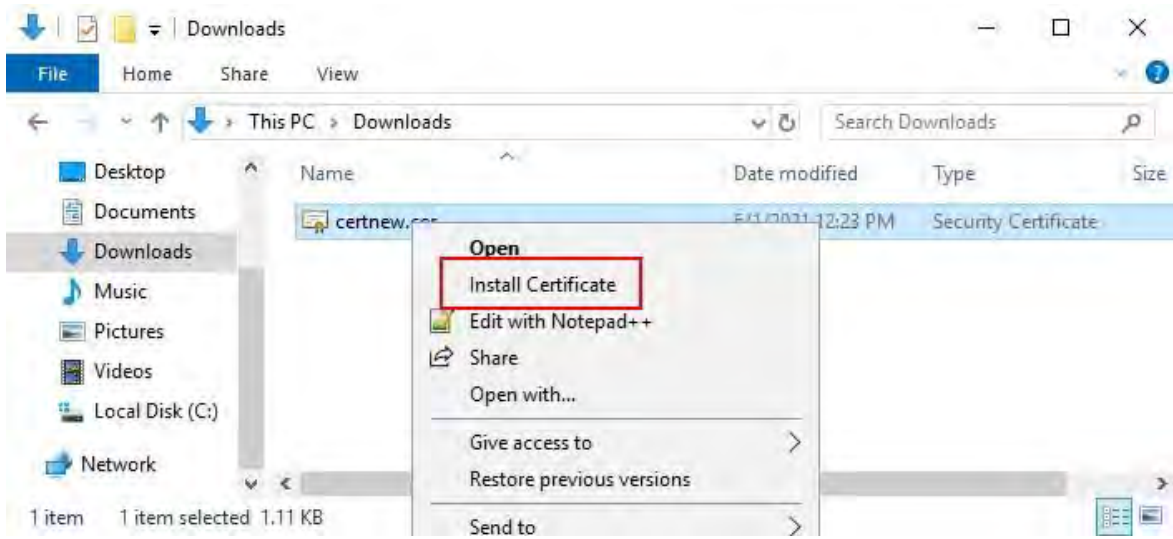
Nei passaggi seguenti viene utilizzato un file . CER da una CA interna.

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.

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.



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**.

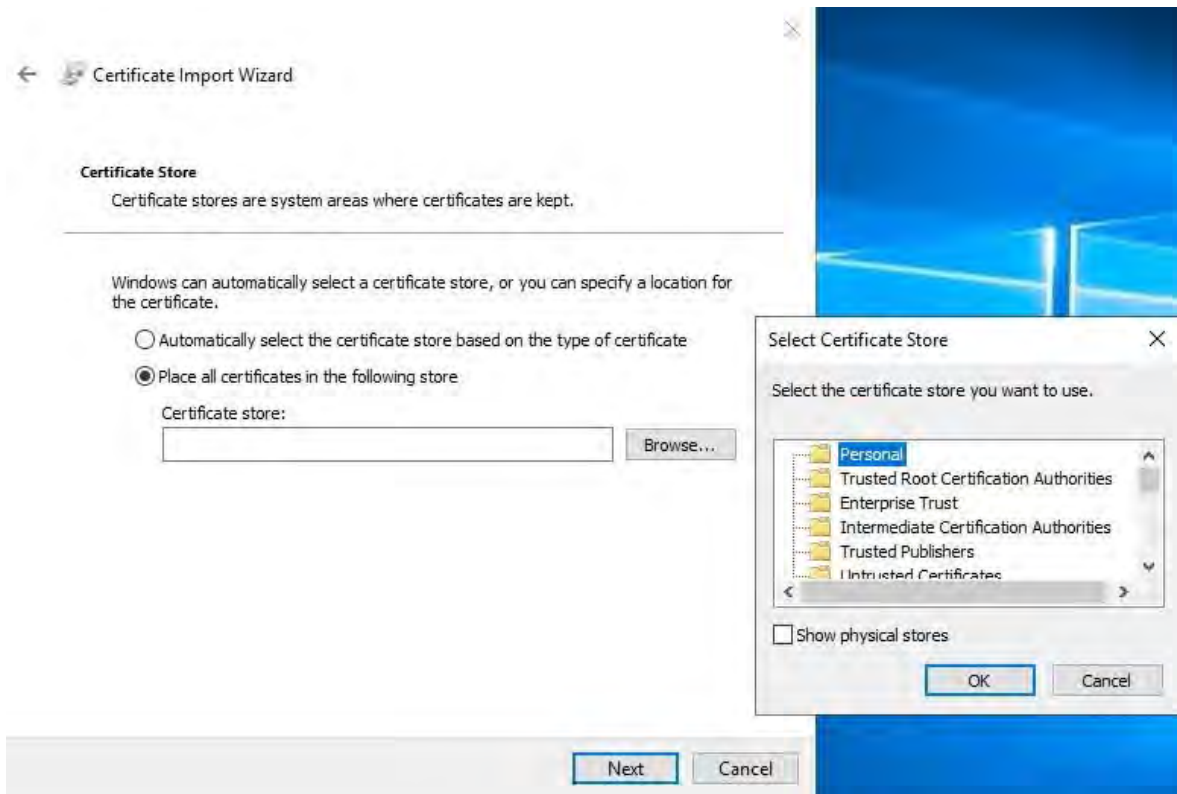


3. Accetta l'avviso di sicurezza, se visualizzato.

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



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



5. Completare la **procedura guidata** Installa certificato.

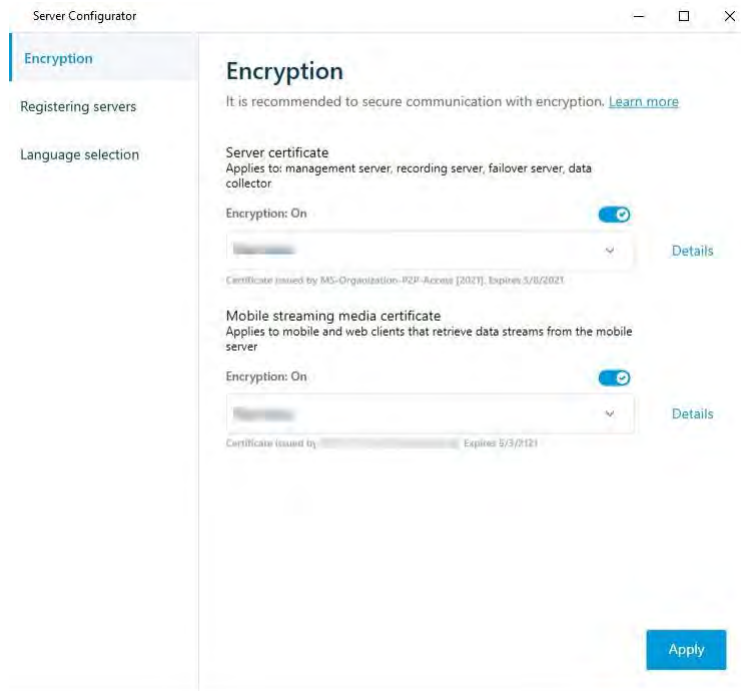
Abilitare la crittografia sul server mobile

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
 - o
 - 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.



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.](#)

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 sono gratuiti.

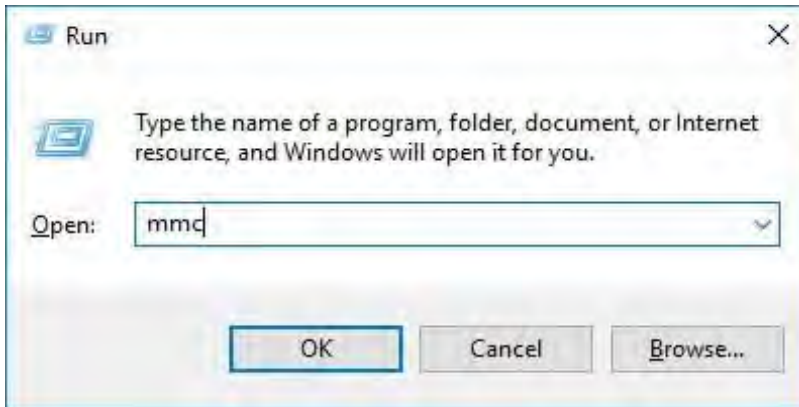
Aggiungere un certificato CA al server

Aggiungere il certificato CA al server effettuando le seguenti operazioni.

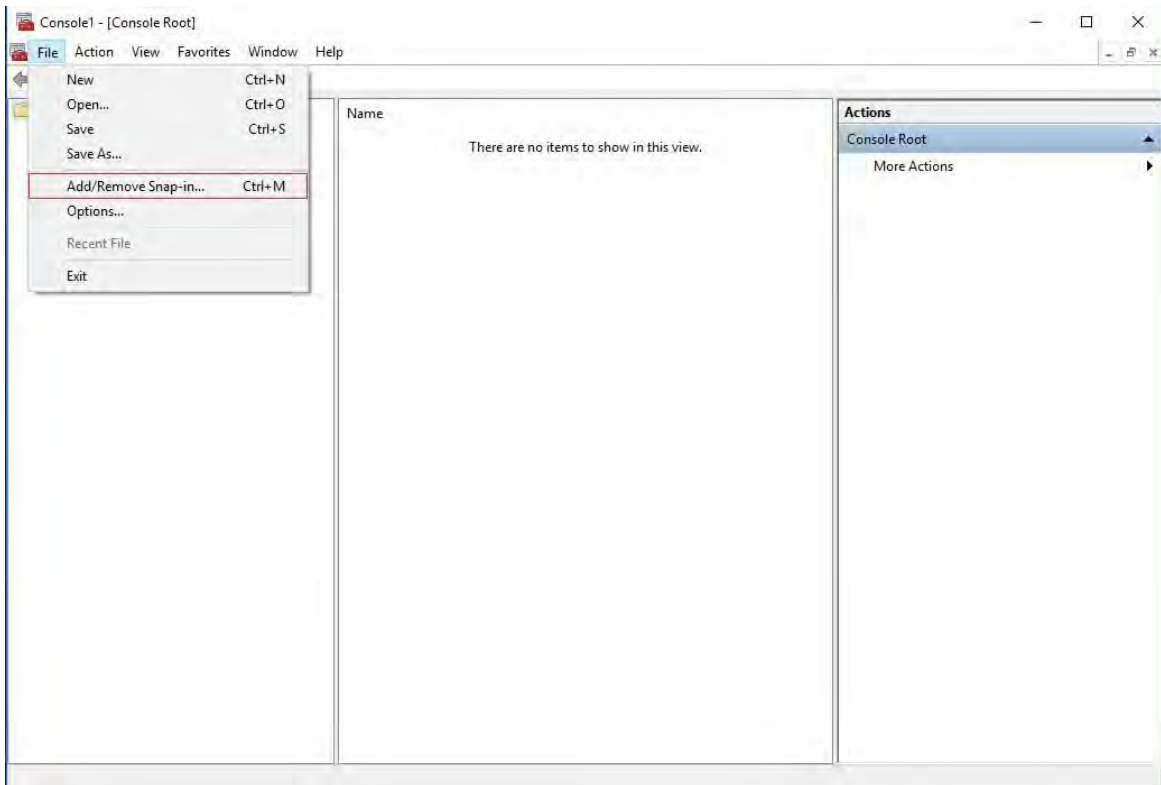


I parametri specifici dipendono dalla CA. Fare riferimento alla documentazione della CA prima di procedere.

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

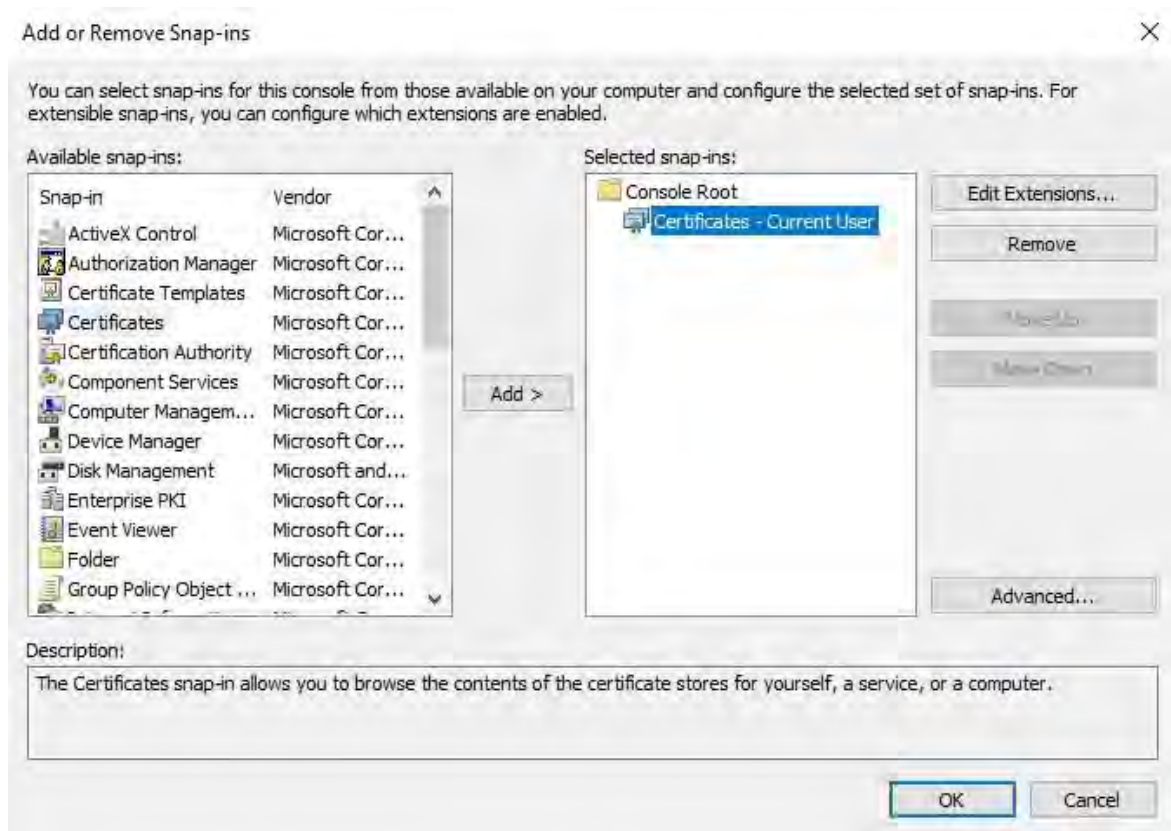


2. In Microsoft Management Console, dal menu **File** selezionare **Aggiungi/Rimuovi snap-in....**

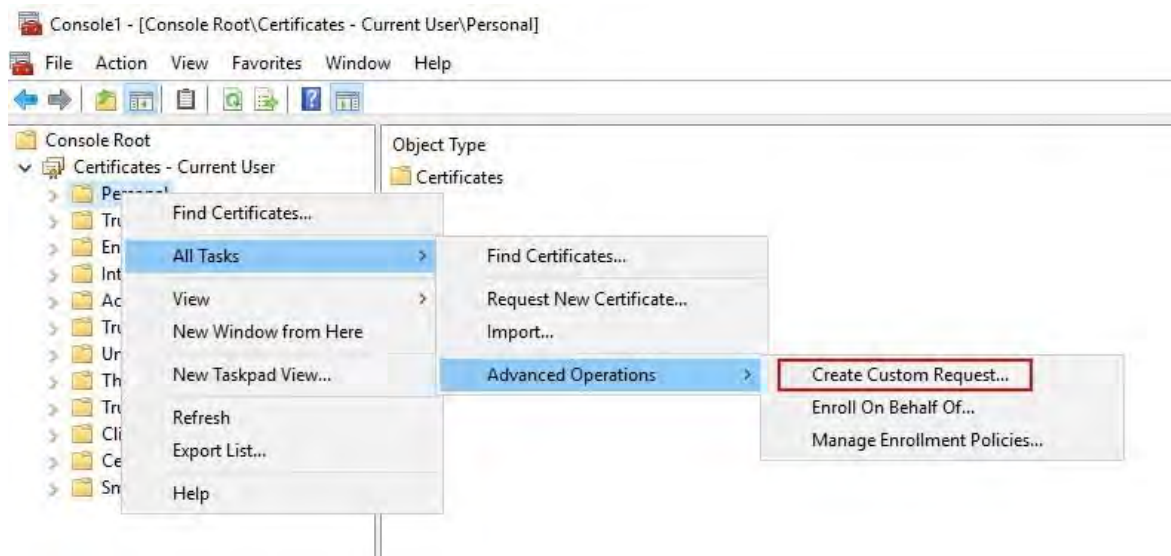


3. Selezionare lo snap-in Certificati e fare clic su **Aggiungi**.

Fare clic su **OK**.

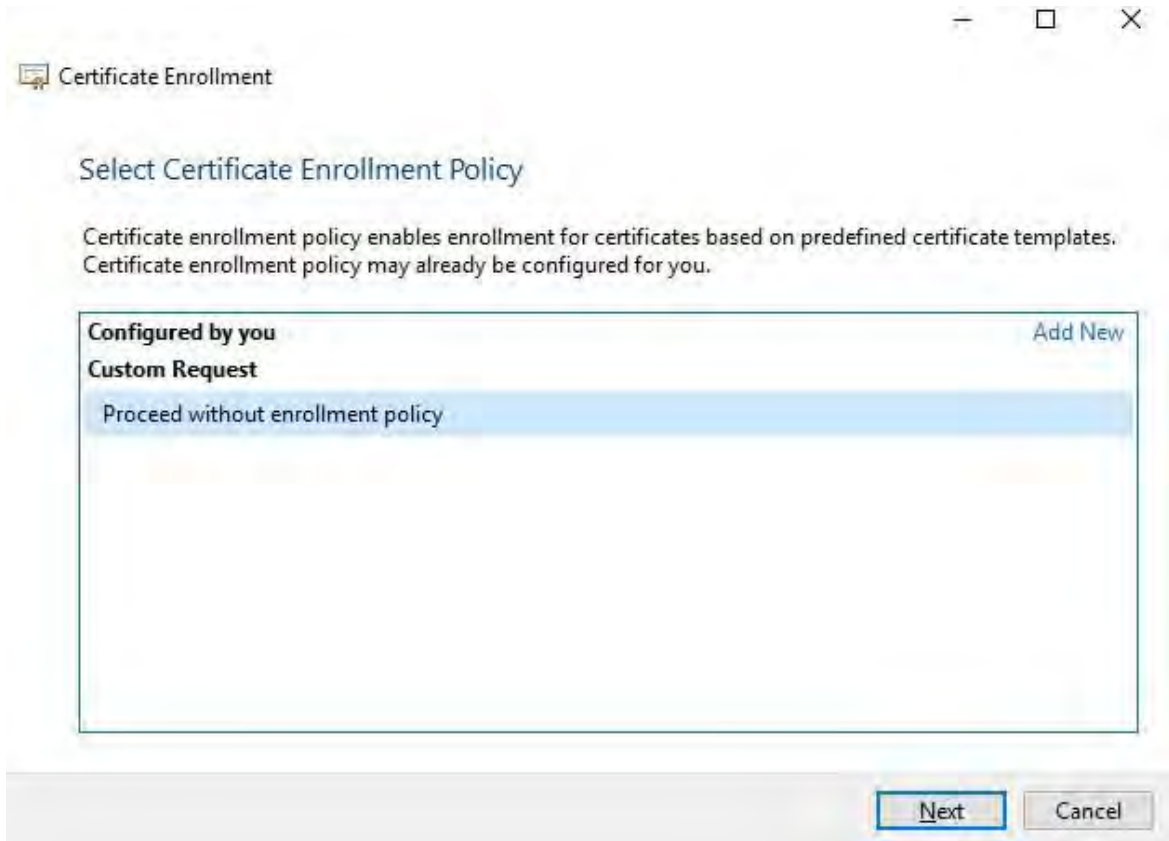


4. Espandere l'oggetto Certificati. Fare clic con il pulsante destro del mouse sulla **cartella Personale** e selezionare **Tutte le attività > Operazioni avanzate > Crea richiesta personalizzata**.

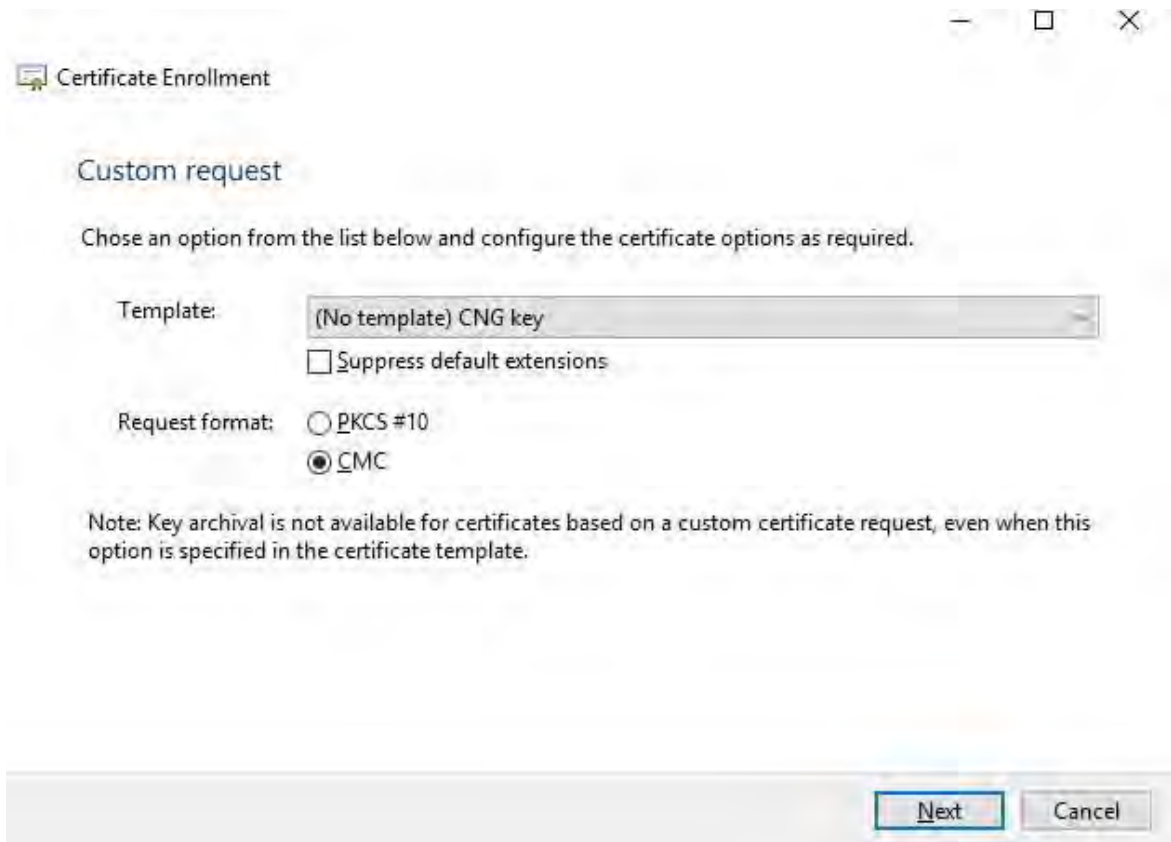



5. Fare clic su **Avanti** nella procedura guidata **Registrazione certificati** e selezionare **Procedi senza criteri di registrazione**.

Fare clic su **Avanti**.



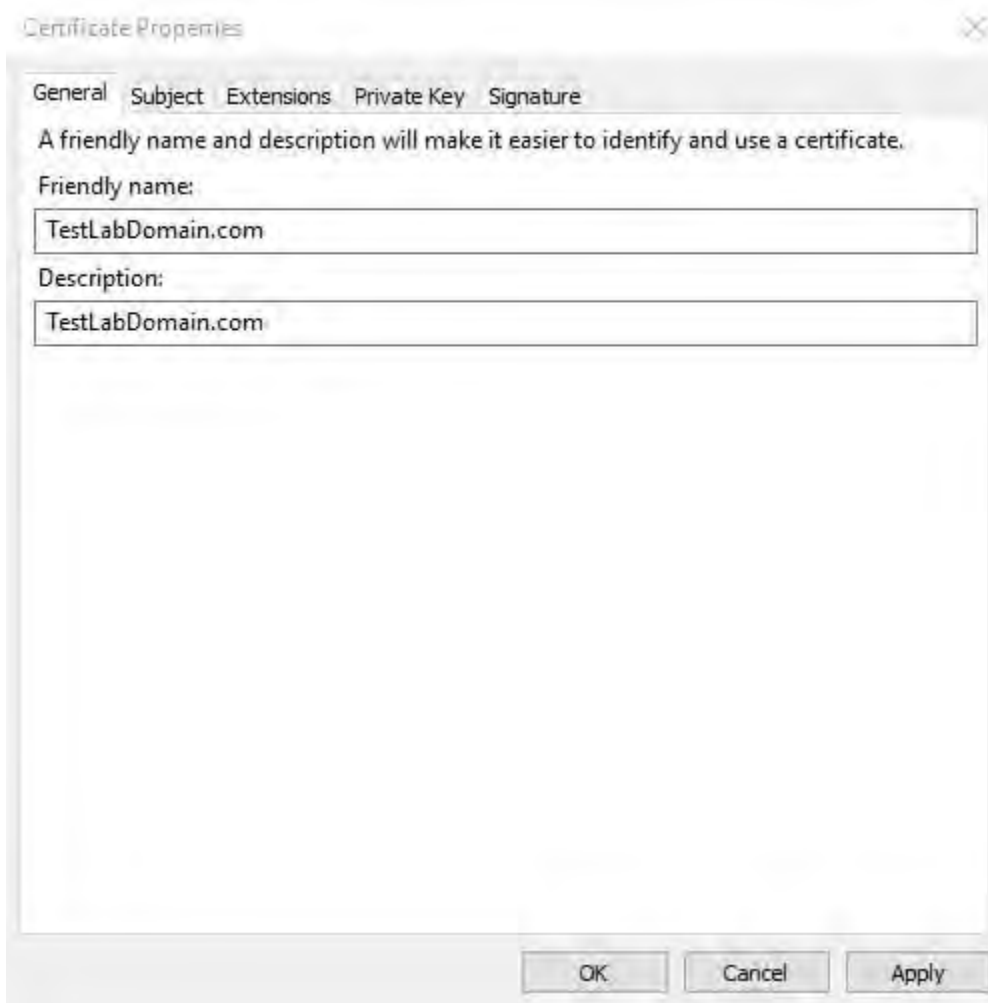
6. Selezionare il modello **di chiave CNG (Nessun modello)** e il formato di richiesta **CMC**, quindi fare clic su **Avanti**.



 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.

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

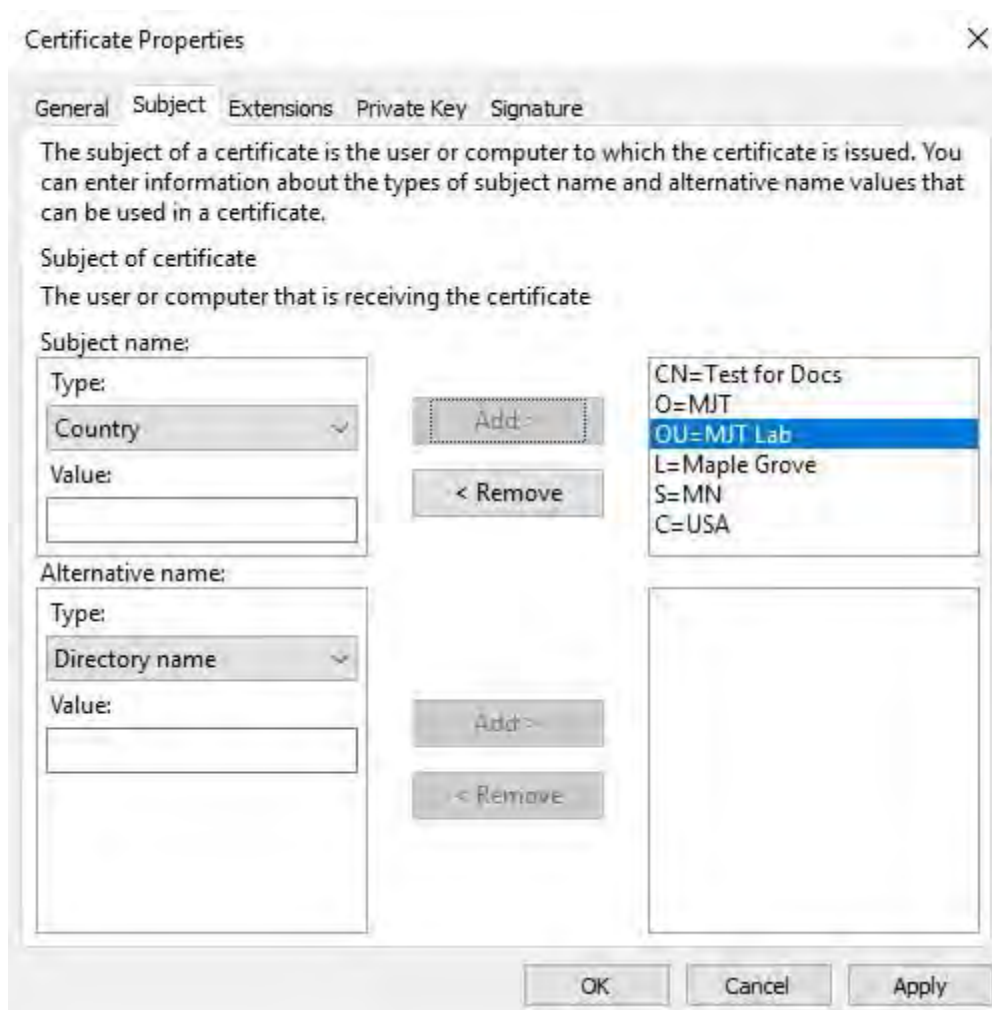
8. Nella scheda **Generale**, compila i campi **Nome descrittivo** e **Descrizione** con il nome di dominio registrato con la CA.



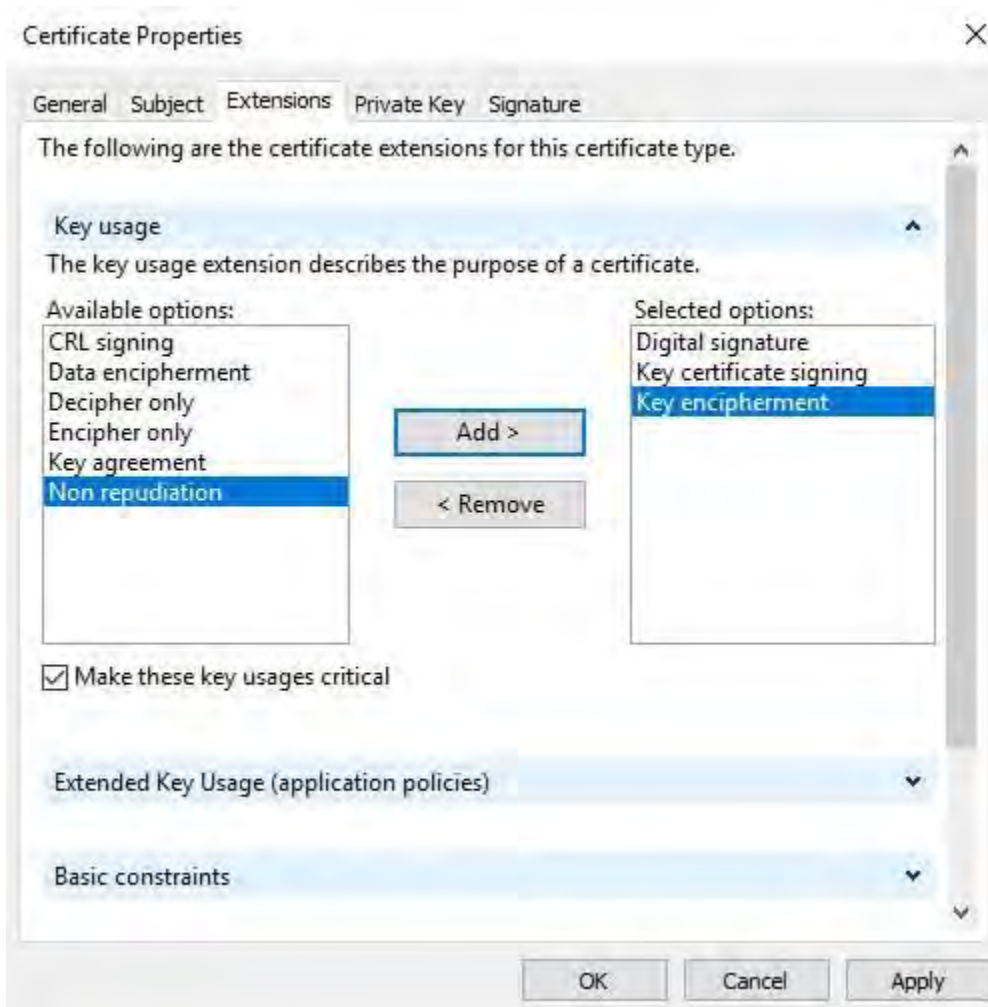
9. Nella scheda **Oggetto** immettere i parametri richiesti dalla CA specifica.

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:




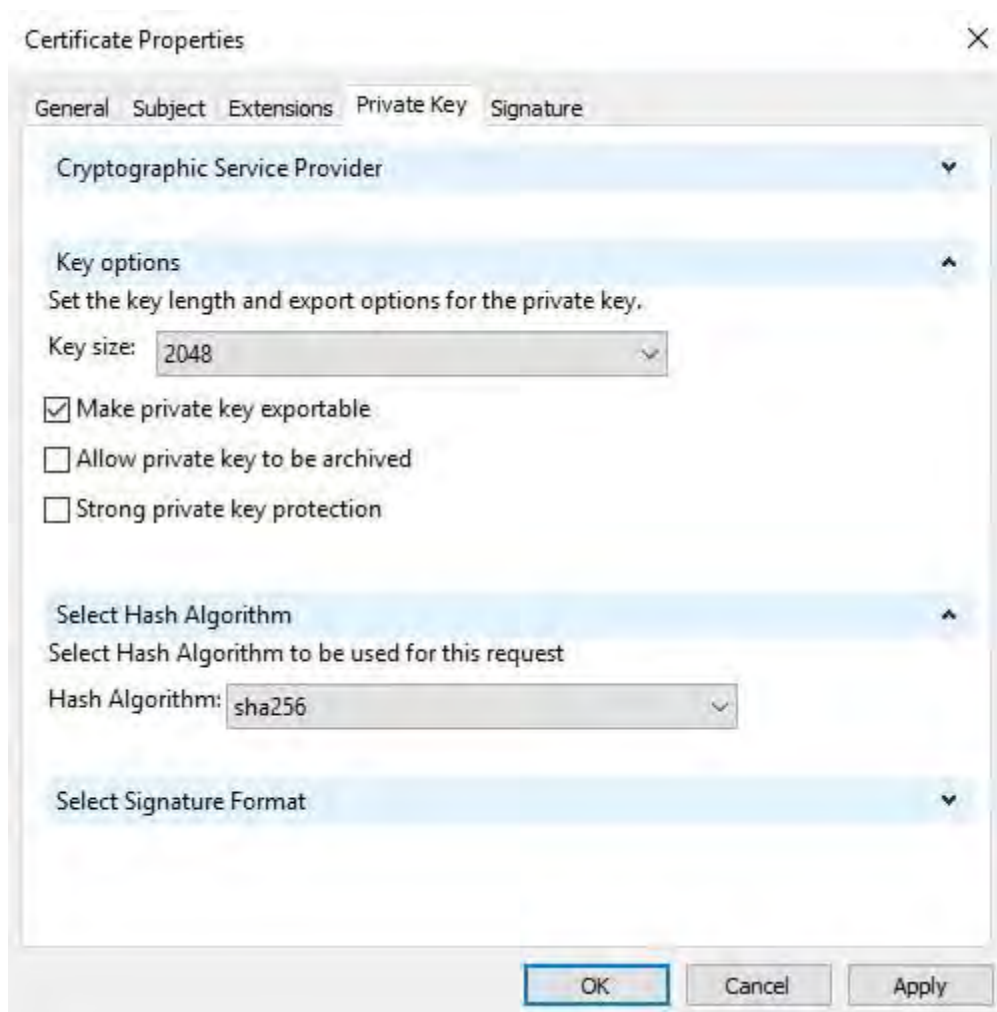
10. Alcune CA non richiedono estensioni. Tuttavia, se necessario, vai alla **scheda Estensioni** ed espandi il menu **Utilizzo chiavi** . Aggiungere le opzioni richieste dall'elenco Opzioni **disponibili** all' elenco **Opzioni selezionate**.



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

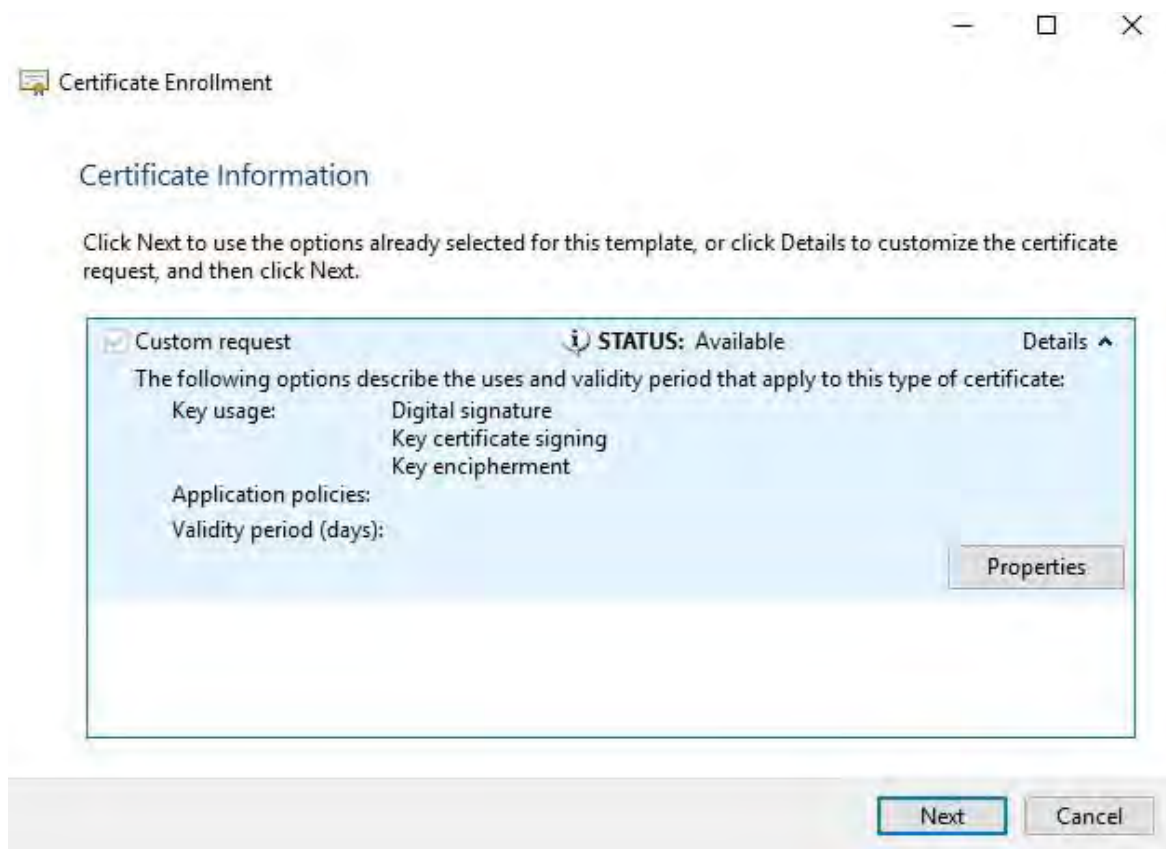
Imposta la dimensione della chiave su 2048 e seleziona l'opzione per rendere esportabile la chiave privata.

 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 prima di procedere al passaggio successivo.



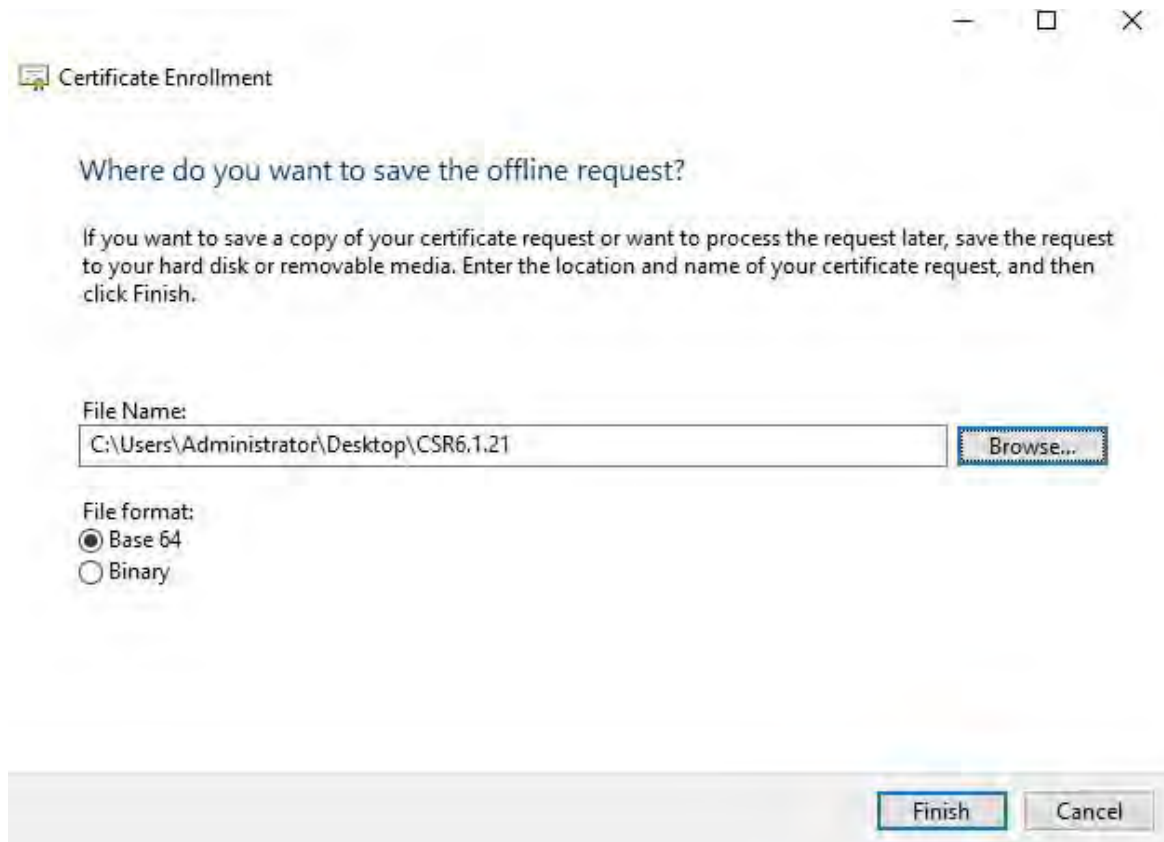
12. A meno che la CA non richieda una firma, il passaggio successivo consiste nel fare clic su **OK**.

- Quando tutte le proprietà del certificato sono state definite, fare clic su **Avanti** nella finestra di dialogo **Registrazione certificati** mago.



- 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.

15. Fare clic su **Fine**.



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

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.

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.

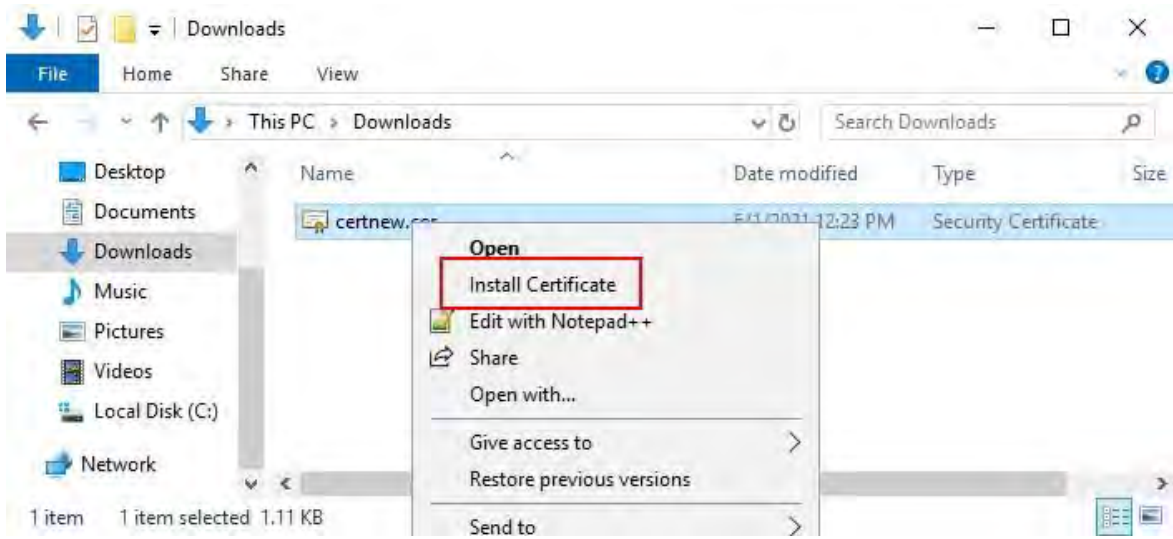
Nei passaggi seguenti viene utilizzato un file . CER da una CA interna.

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.



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**.

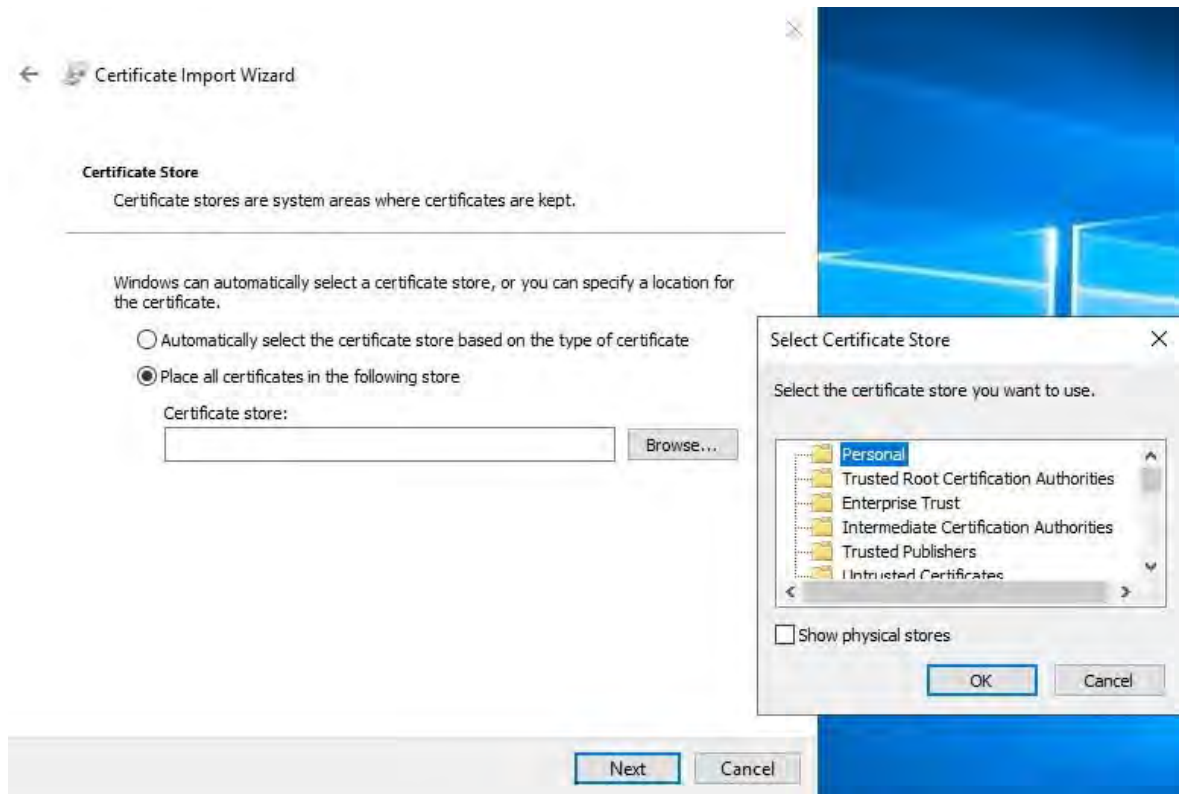


3. Accetta l'avviso di sicurezza, se visualizzato.

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



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



5. Completare la **procedura guidata** Installa certificato.

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.



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.

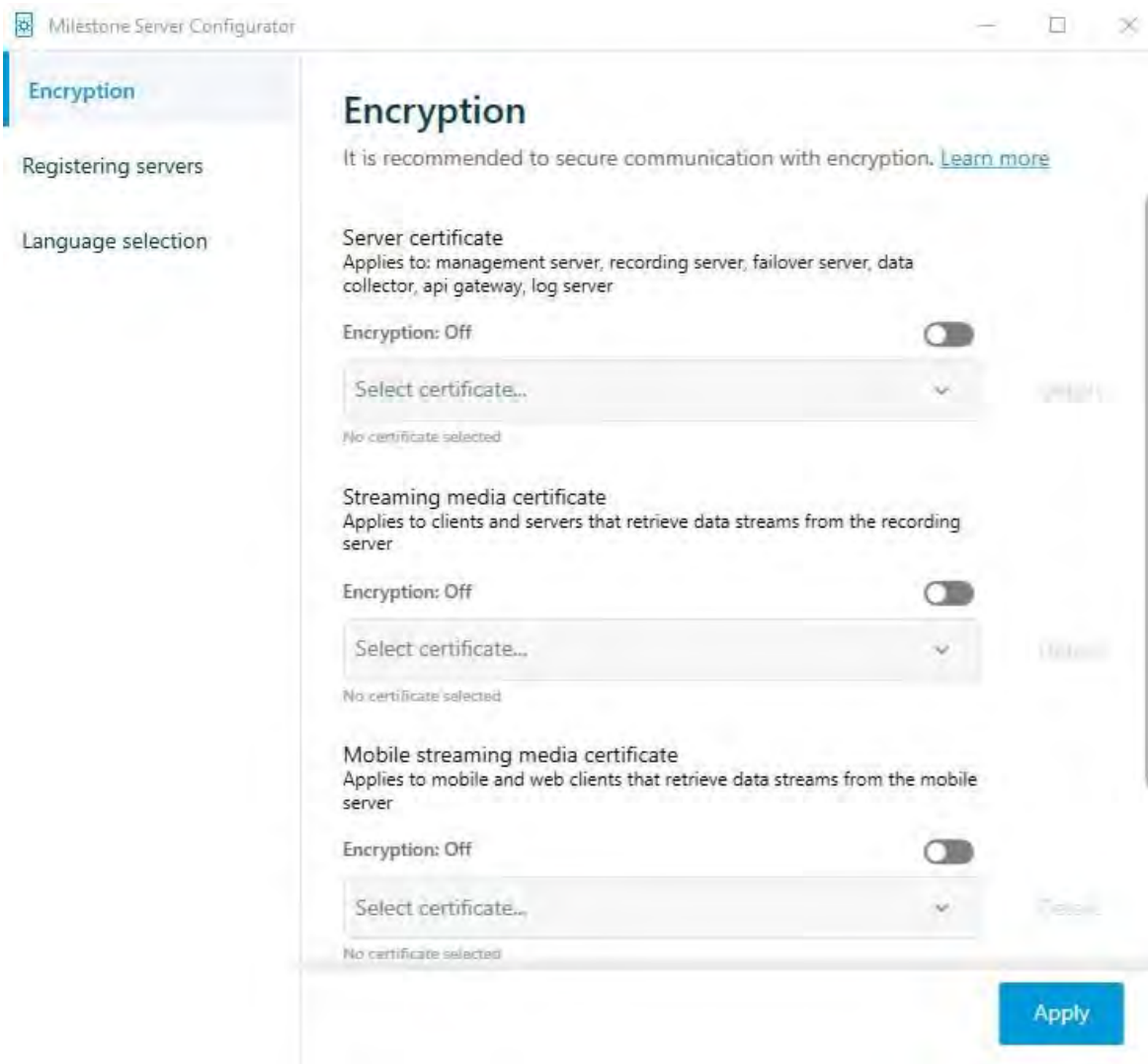
Prerequisiti:

- 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:

1. Su un computer con un server di gestione installato, aprire Server **Configurator** da:
 - Il menu Start di Windows
 - o
 - Management Server Manager facendo clic con il pulsante destro del mouse sull'icona Management Server Manager 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 dell'agente di raccolta dati.

Selezionare **Dettagli** per visualizzare le informazioni dell'archivio certificati di Windows sul certificato selezionato.



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

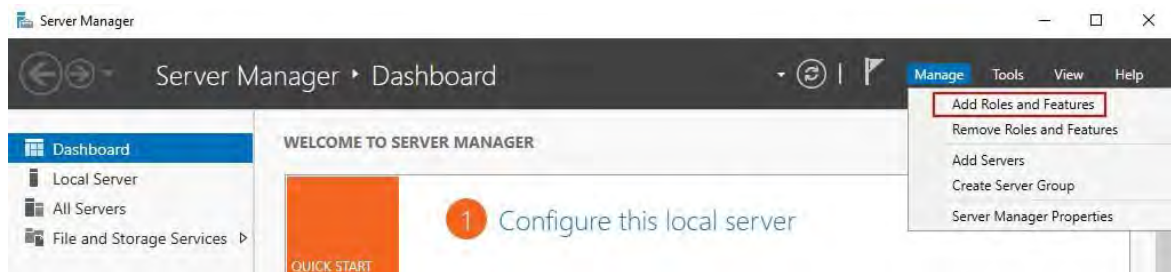
Servizi certificati Active Directory è un prodotto Microsoft che esegue funzionalità di infrastruttura a chiave pubblica (PKI). Funge da ruolo server che consente di costruire un'infrastruttura a chiave pubblica (PKI) e di fornire crittografia a chiave aperta, autenticazione computerizzata e funzionalità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

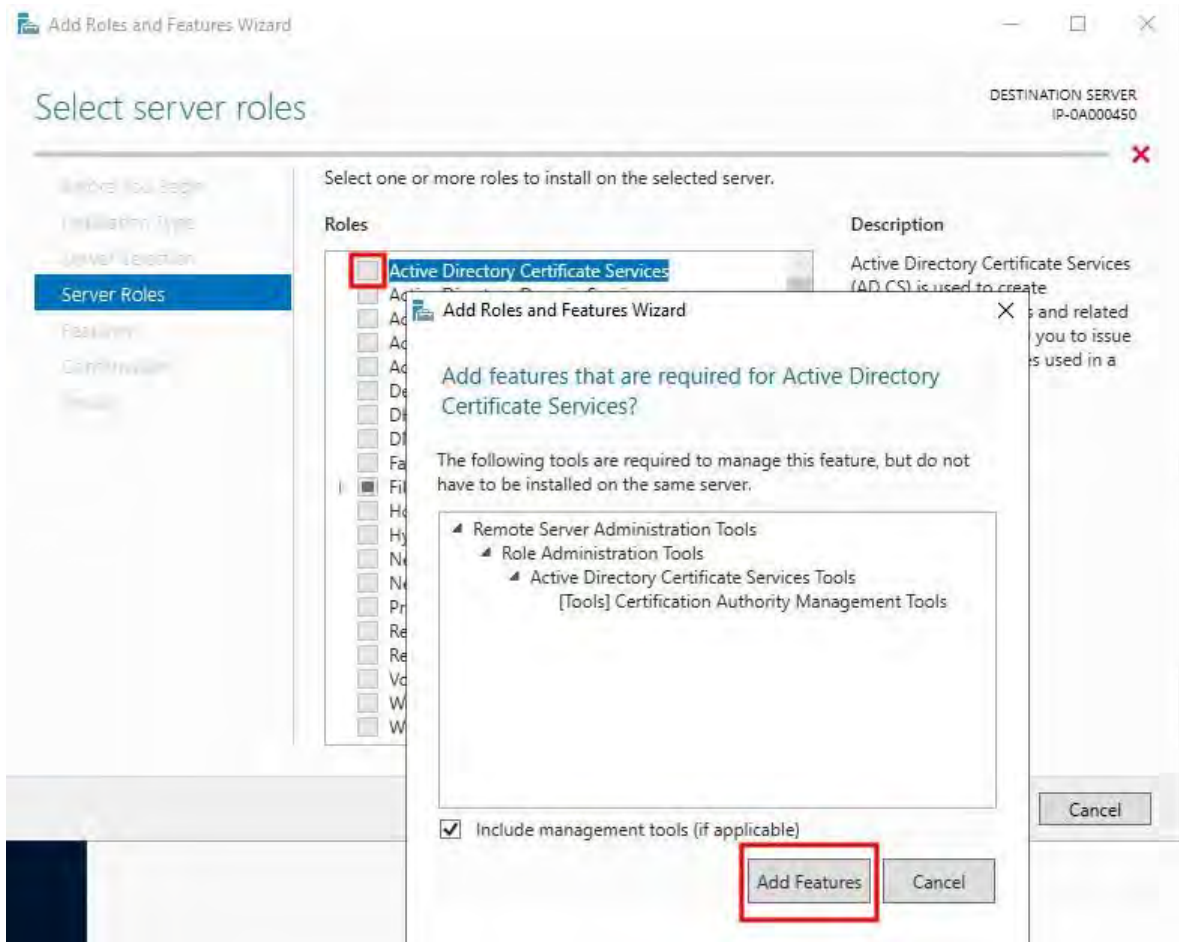
Per installare Servizi certificati Active Directory:

1. Nell' applicazione **Server Manager** selezionare **Gestisci > Aggiungi ruoli e funzionalità**.



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**.



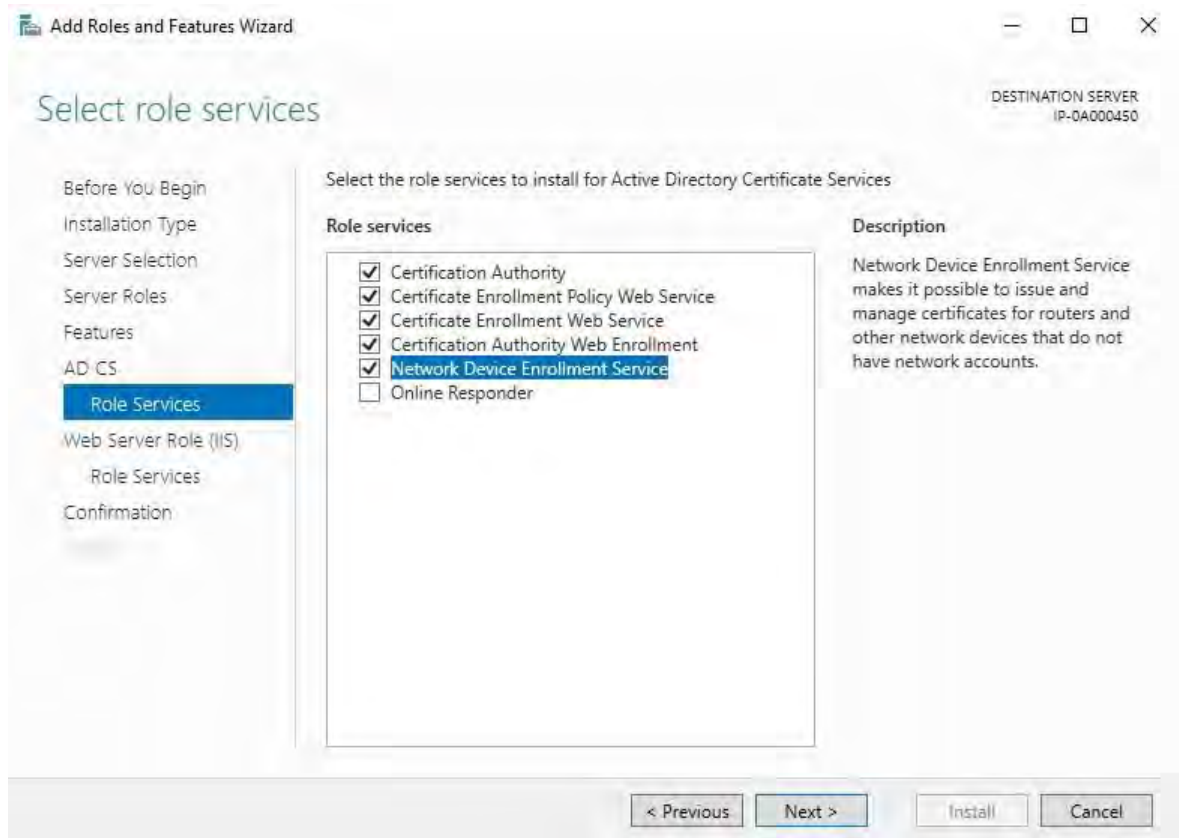
Fare clic su **Avanti**.

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

8. 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.

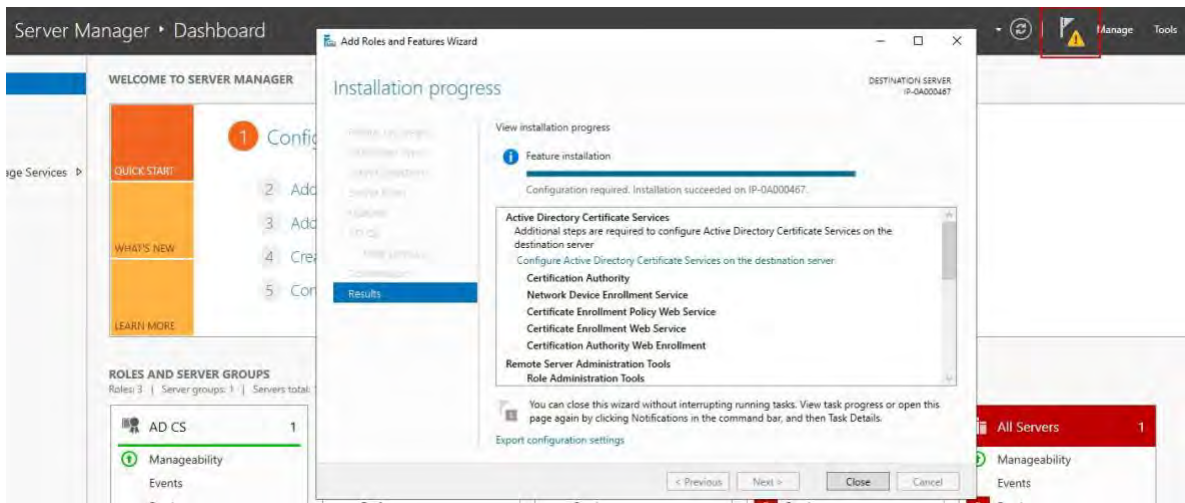


Fare clic su **Avanti**.

9. In **Conferma**, selezionare **Riavvia automaticamente il server di destinazione, se necessario**, e fare clic su **Installa**.

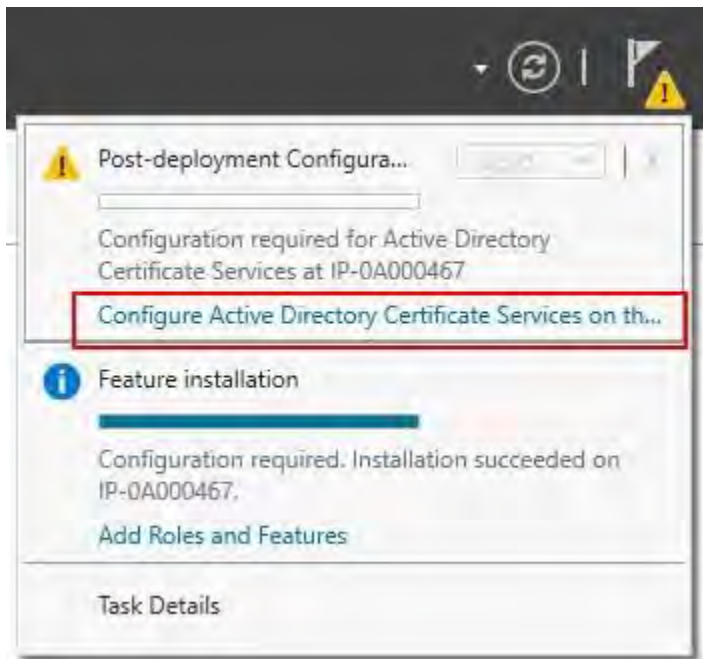
10. Al termine dell'installazione, fare clic sul **pulsante Chiudi**.

Selezionare il **flag di notifica** nell' applicazione **Server Manager**.



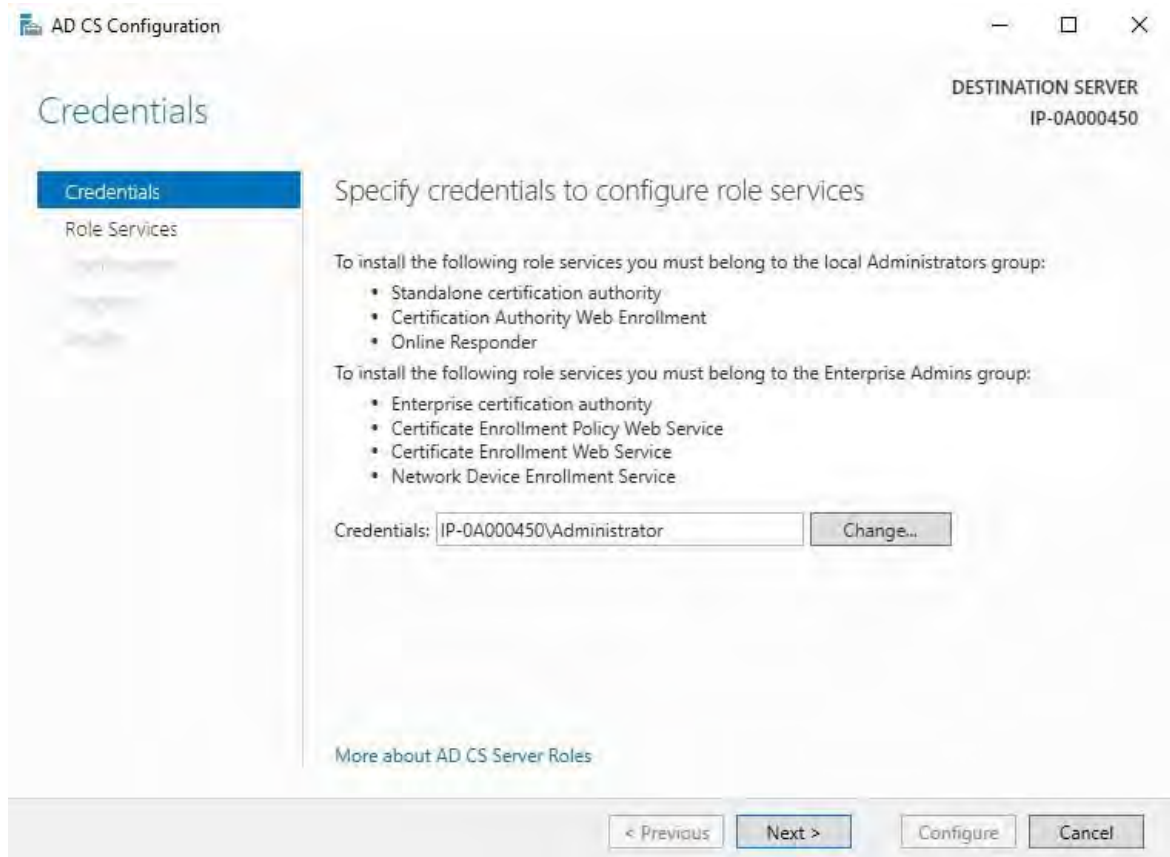
11. Un messaggio per iniziare la configurazione post-distribuzione è elencato sotto il **flag di notifica**.

Clicca sul link per iniziare la configurazione dei servizi installati.



12. Viene avviata la **configurazione guidata di Servizi certificati Active Directory**.

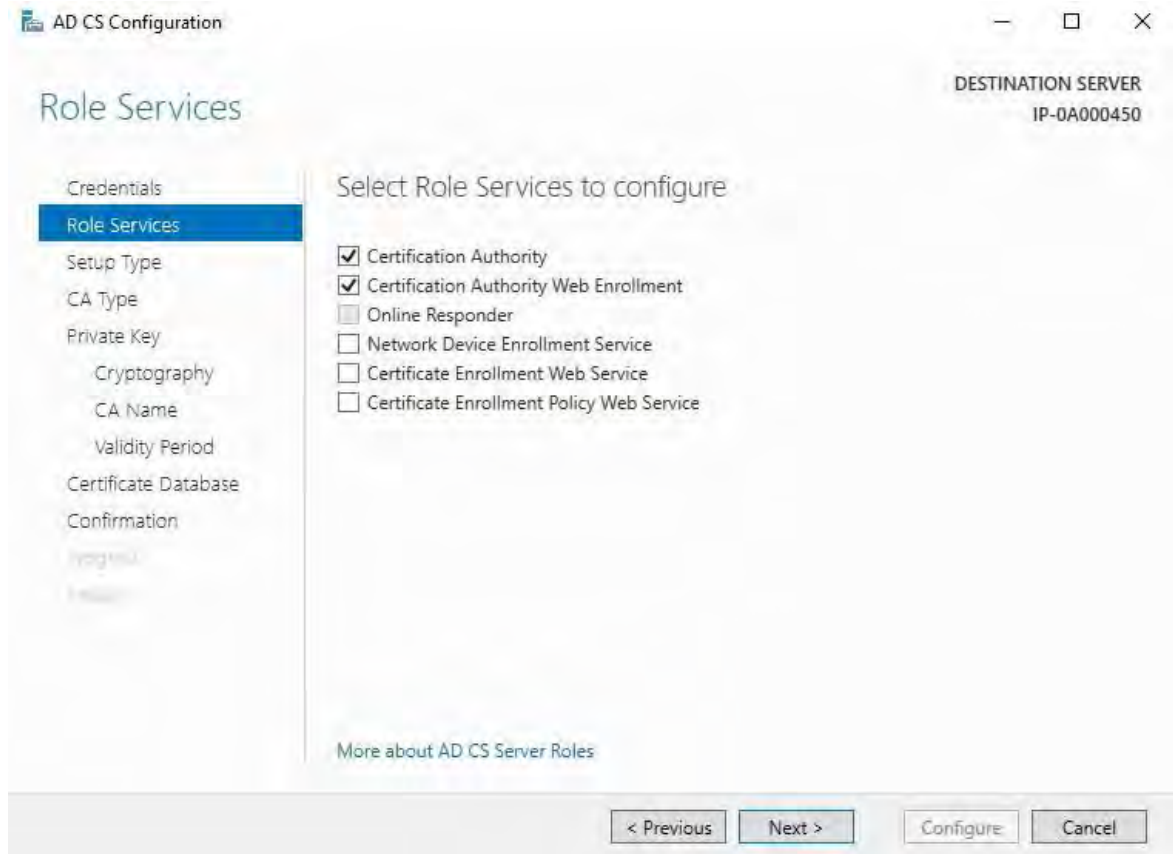
In **Credenziali** selezionare l'account utente necessario per eseguire i servizi installati. Come indicato nel testo, è richiesta l'appartenenza ai gruppi amministratore locale e amministratore dell'organizzazione. Immettere le informazioni sull'account richieste e fare clic su **Avanti**.



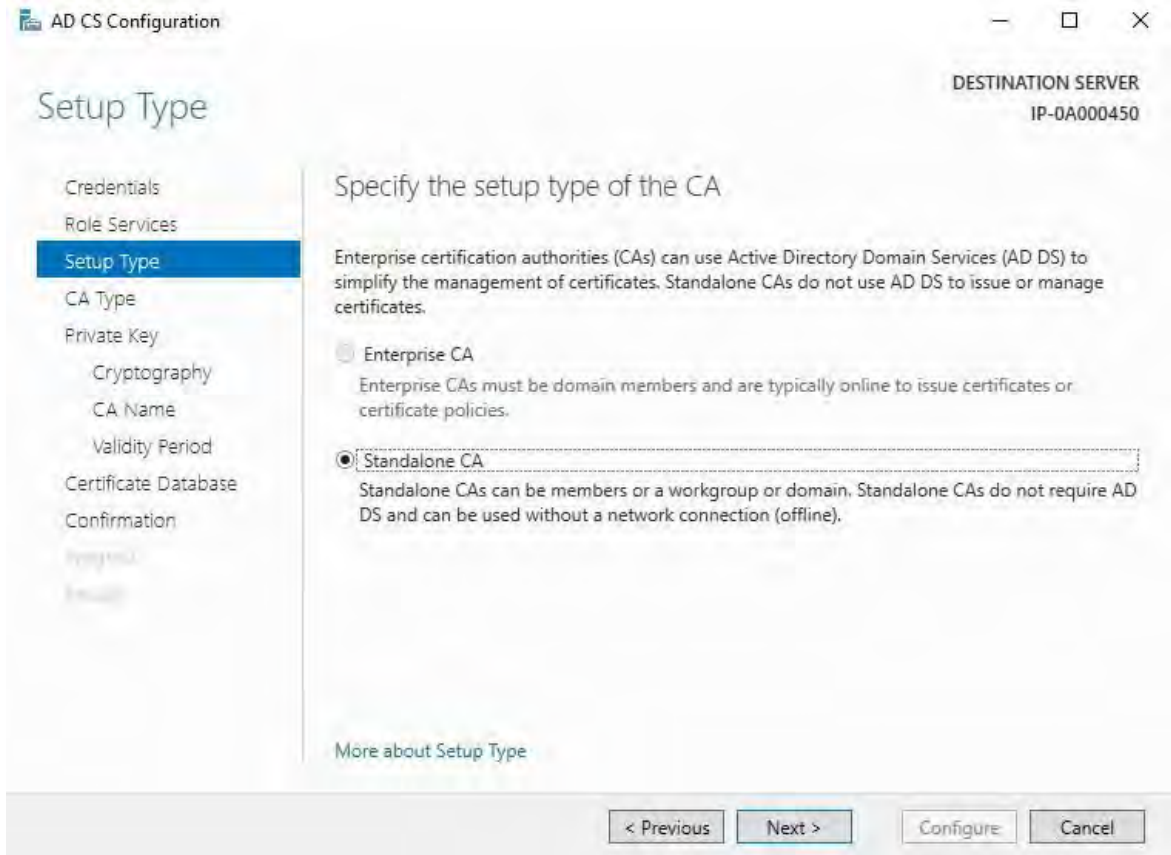
13. In **Servizi ruolo**, selezionare i seguenti servizi:

- **Autorità di certificazione**
- **Registrazione Web dell'Autorità di certificazione**

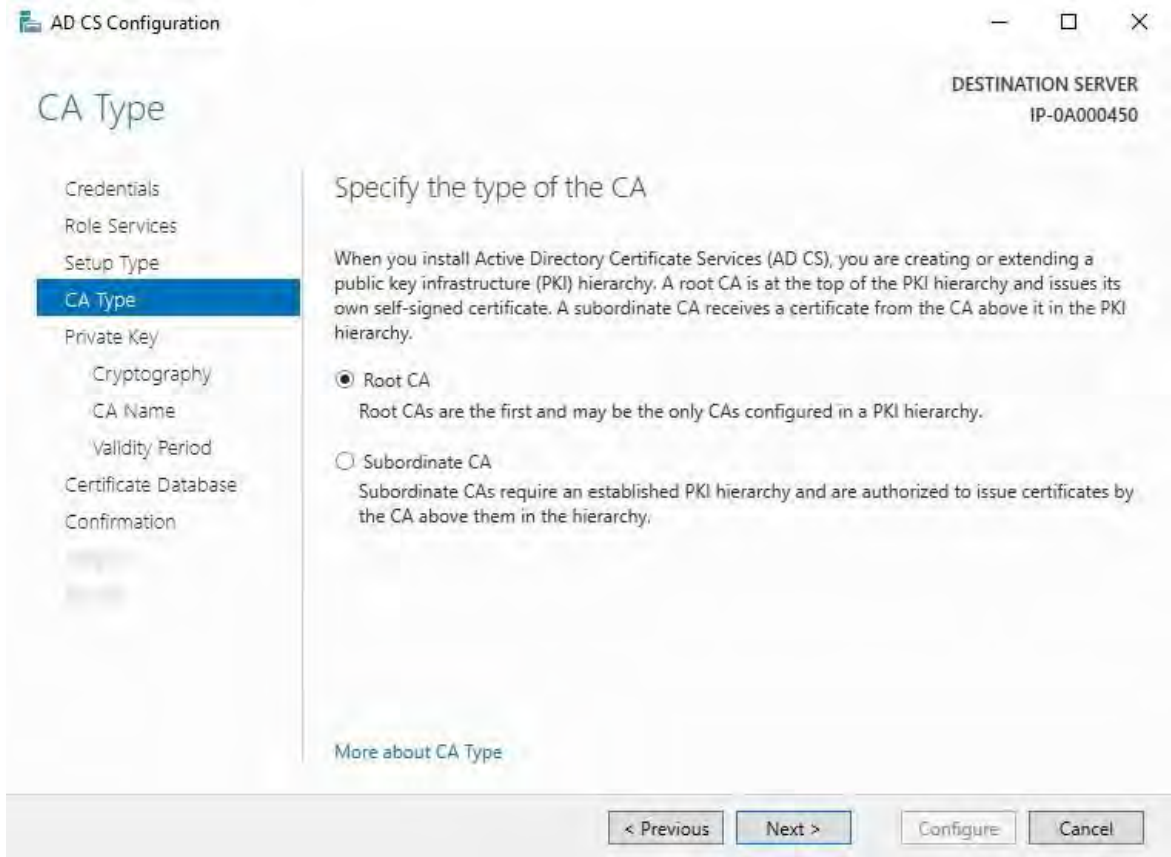
Fare clic su **Avanti**.



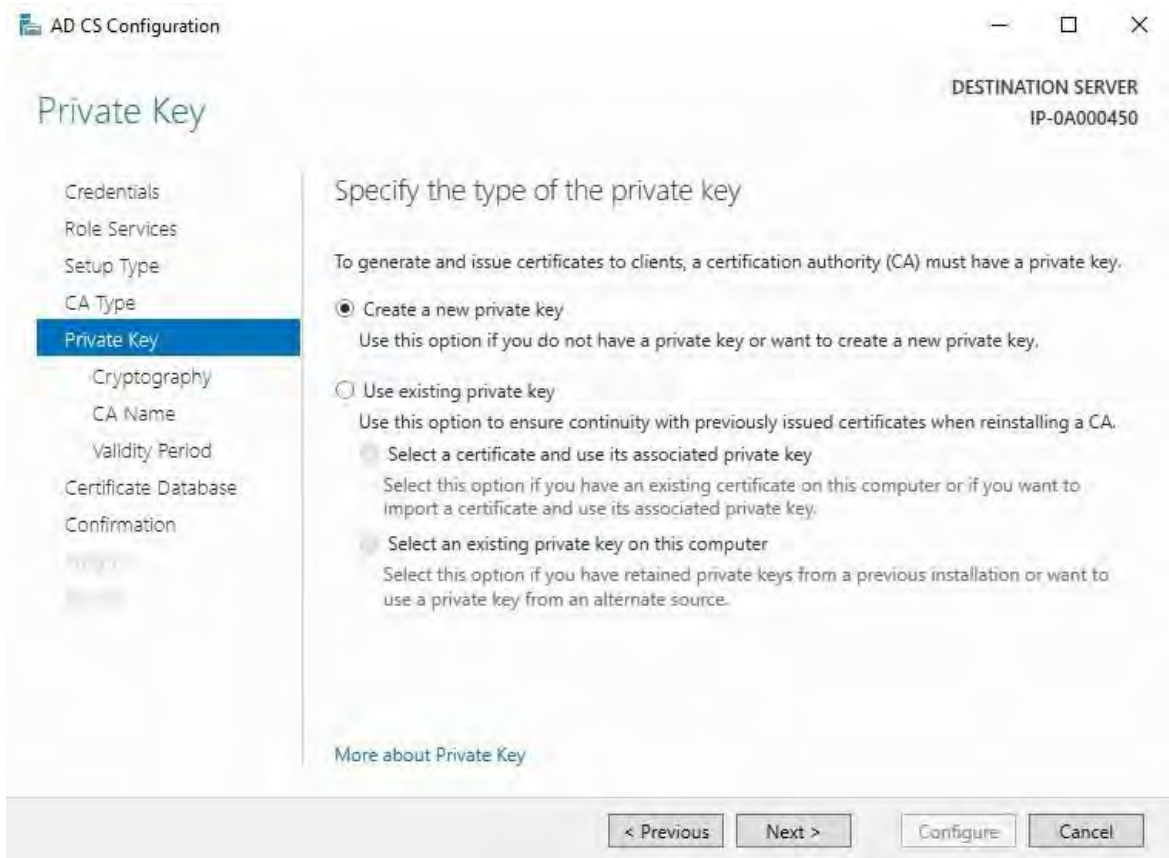
14. In **Tipo di installazione**, selezionare l' **opzione CA autonoma** e fare clic su **Avanti**.



15. In **Tipo di CA** selezionare l'opzione per installare una **CA radice** e fare clic su **Avanti**.

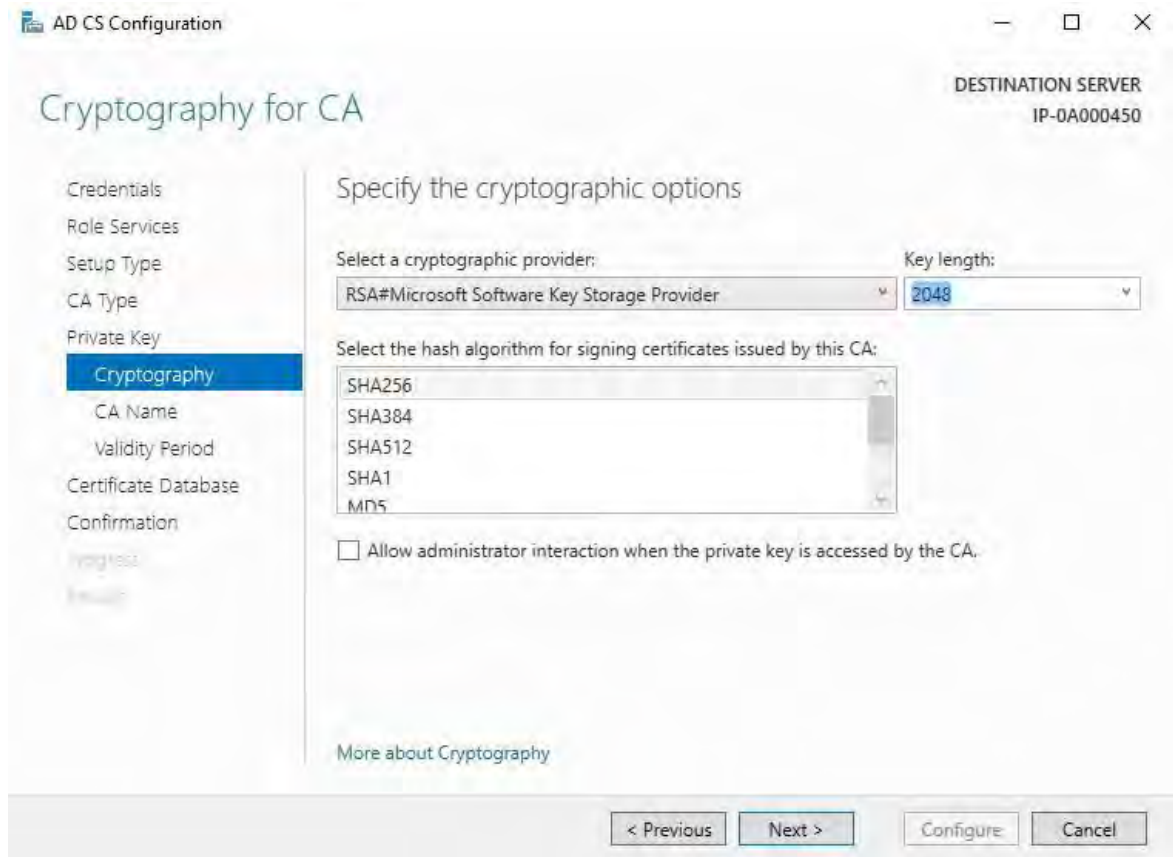


16. In **Chiave privata**, selezionare l'opzione per creare una nuova chiave privata e fare clic su **Avanti**.



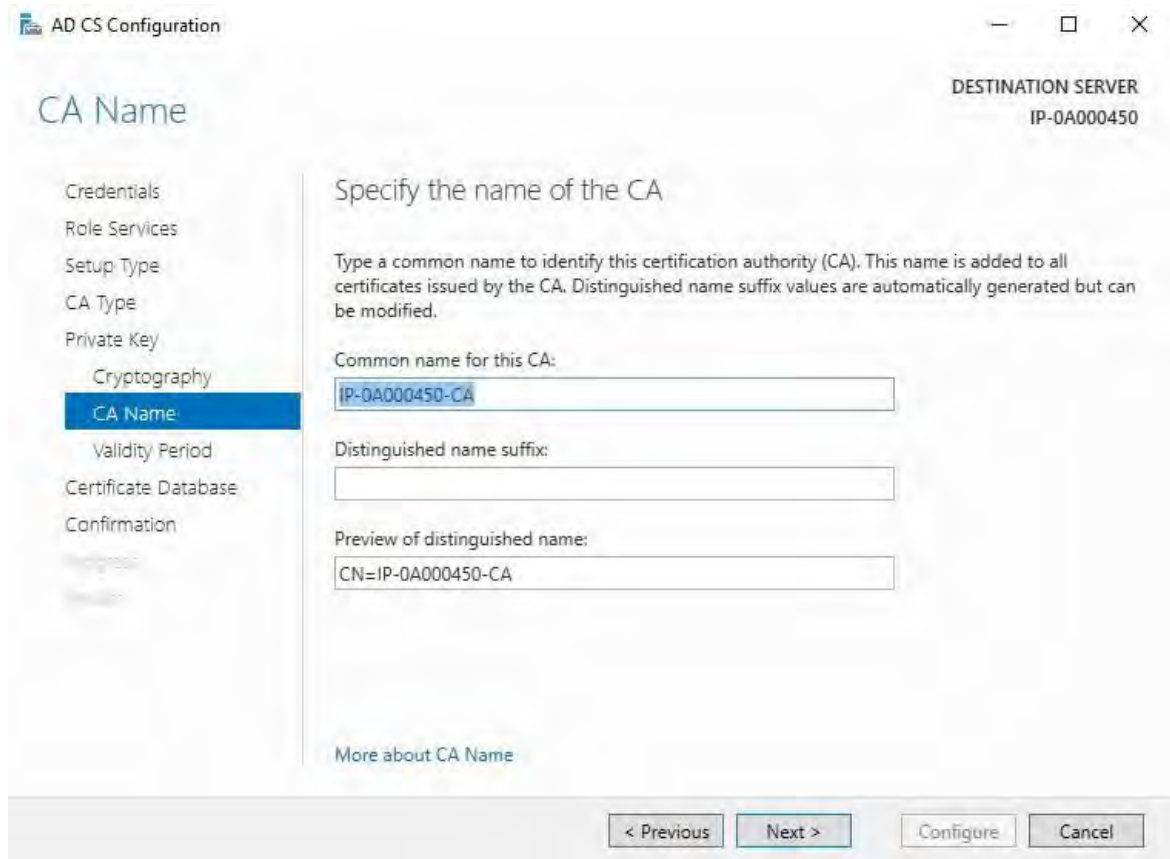
17. In **Crittografia** selezionare **RSA#Microsoft Software Key Storage Provider** per l'opzione del provider di crittografia con una **lunghezza della chiave** di 2048 e un algoritmo hash SHA256.

Fare clic su **Avanti**.

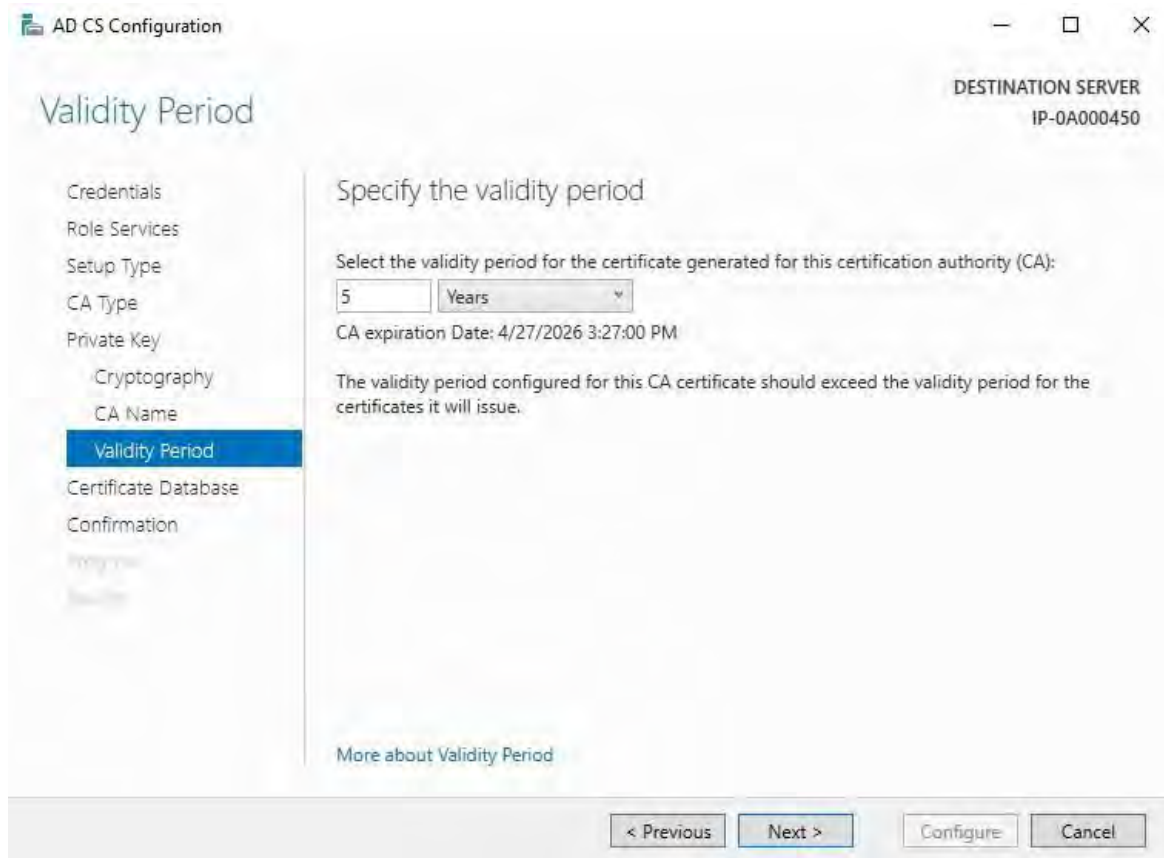


18. In **Nome CA**, immettere il nome della CA e fare clic su **Avanti**.

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



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



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

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.

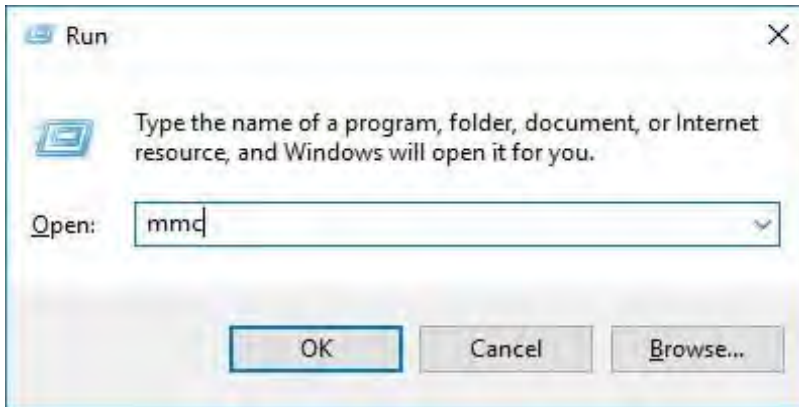


Microsoft fornisce una documentazione completa per i sistemi operativi Windows Server, che include modelli per i certificati server, l'installazione della CA e la distribuzione dei certificati è disponibile in [Panoramica della distribuzione dei certificati server di Microsoft](#).

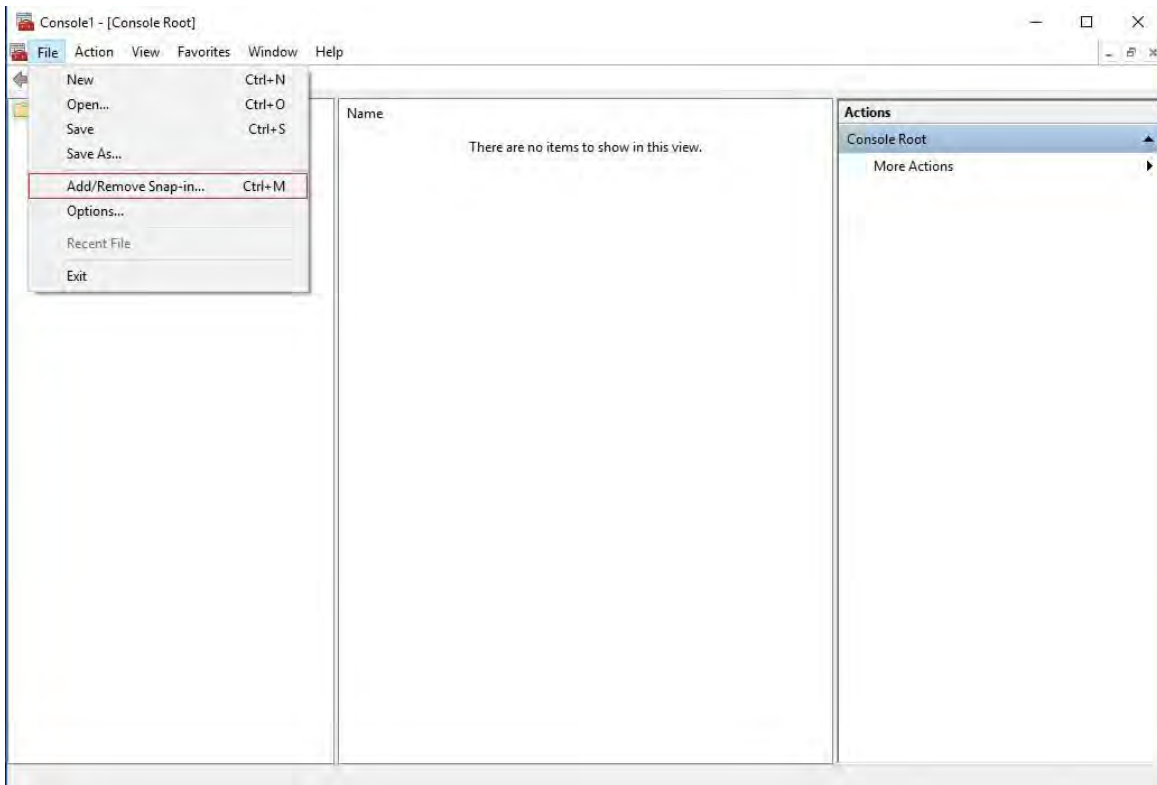
Aggiungere un certificato CA al server

Aggiungere il certificato CA al server effettuando le seguenti operazioni.

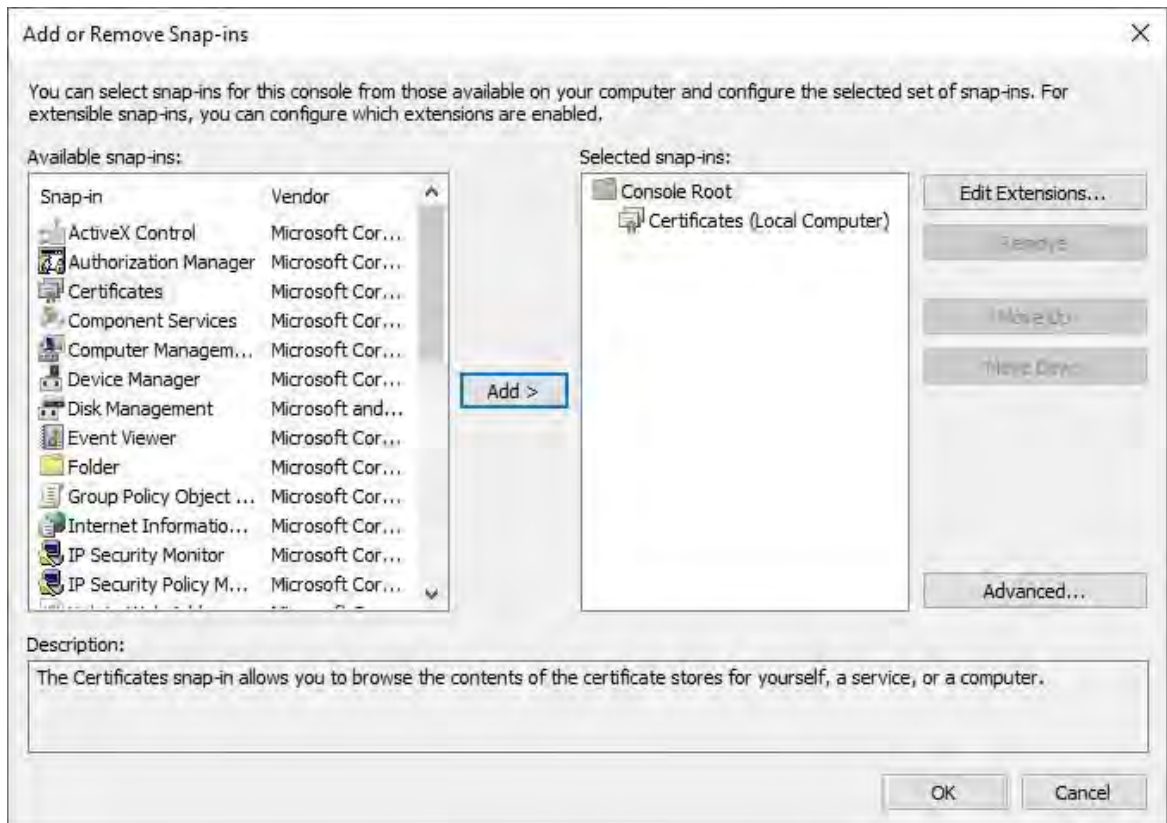
1. Sul computer che ospita il server MOBOTIX HUB, aprire Microsoft Management Console.



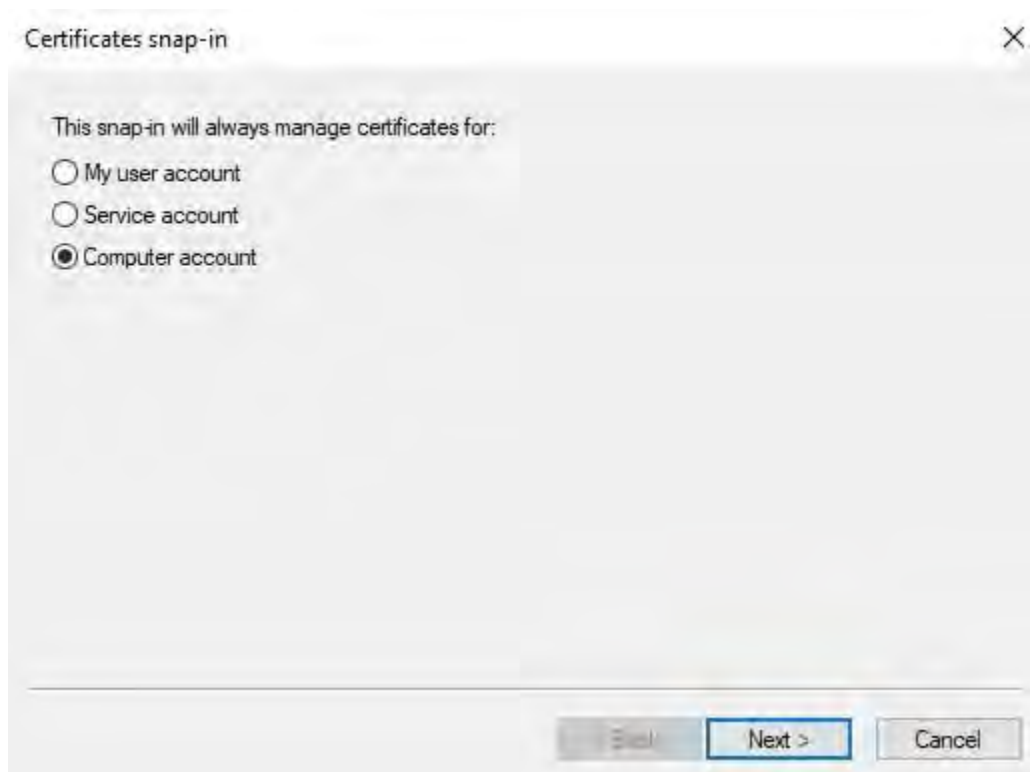
2. In Microsoft Management Console, dal menu **File** selezionare **Aggiungi/Rimuovi snap-in....**



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

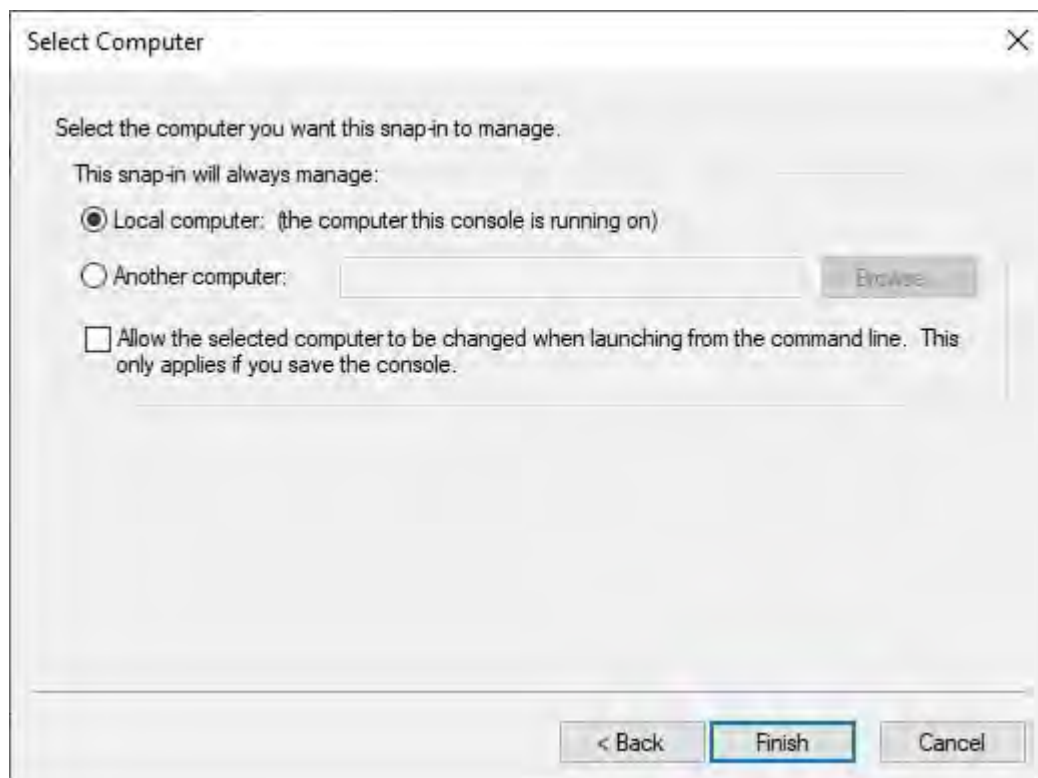


4. Nello **snap-in Certificati** selezionare **Account computer**.

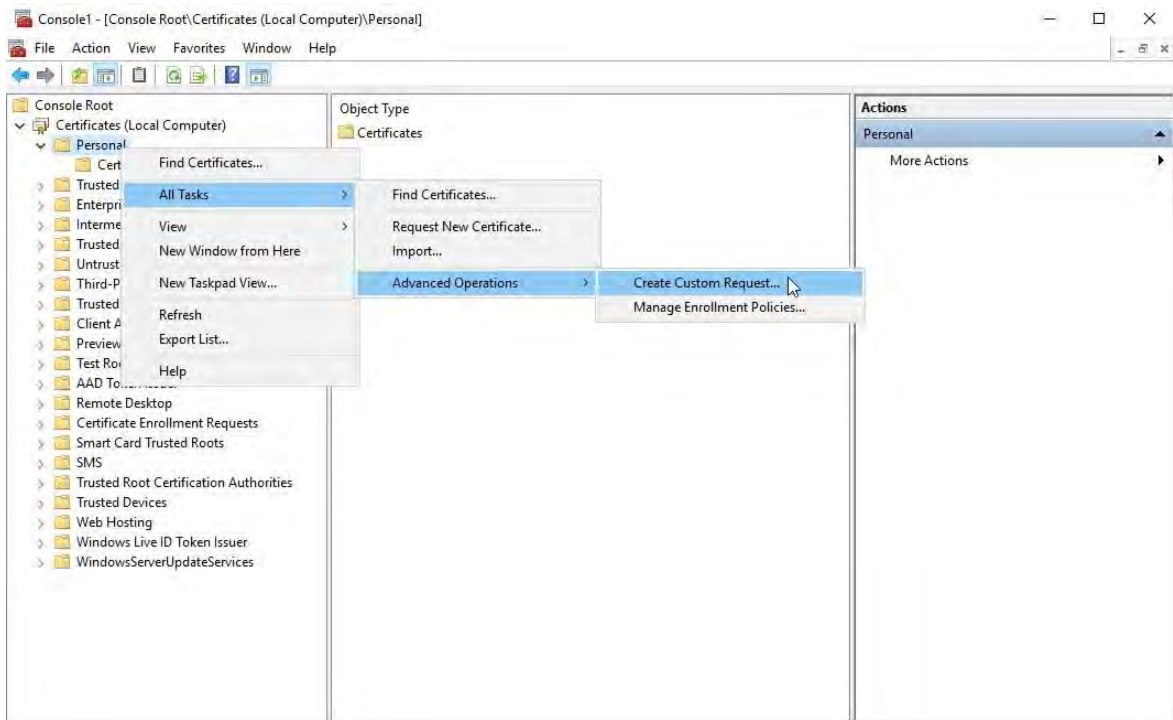


5. In **Seleziona computer** selezionare **Computer locale**.

Selezionare **Fine**, quindi **OK**.



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**.

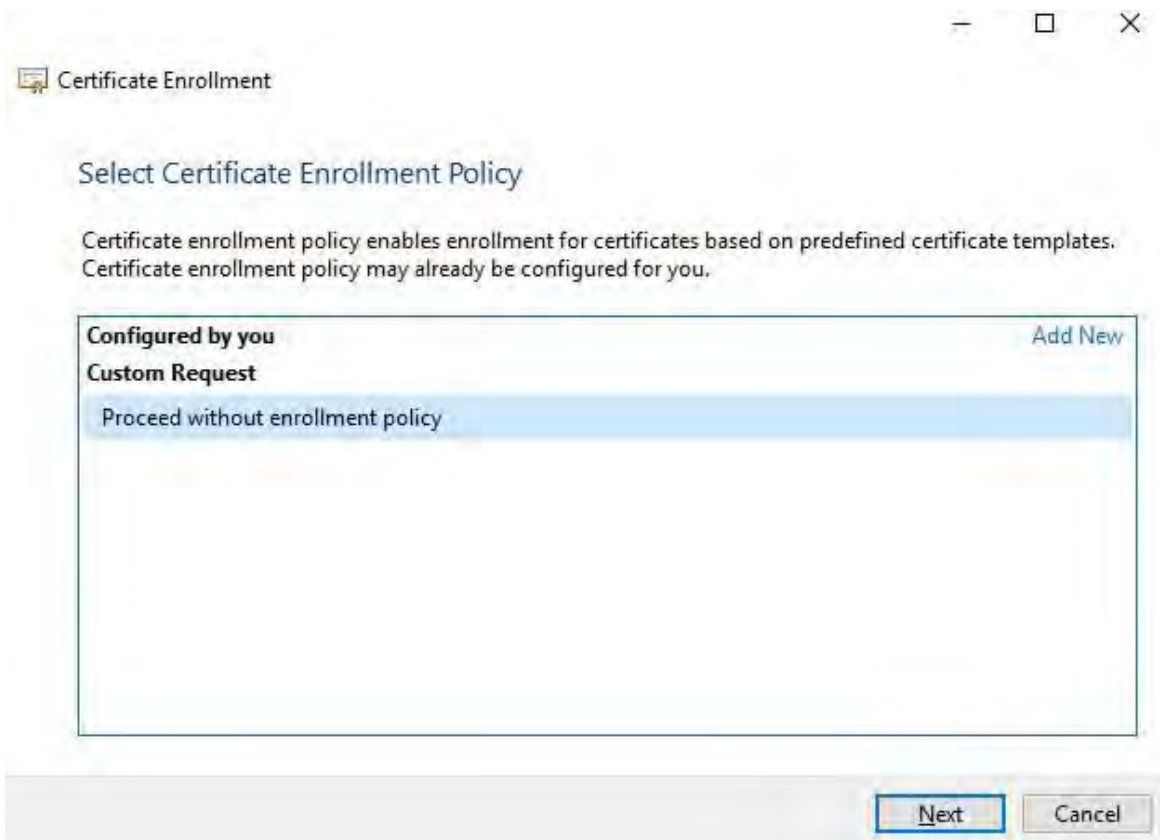


7. Fare clic su **Avanti** nella procedura guidata **Registrazione certificati** e selezionare **Procedi senza criteri di registrazione**.

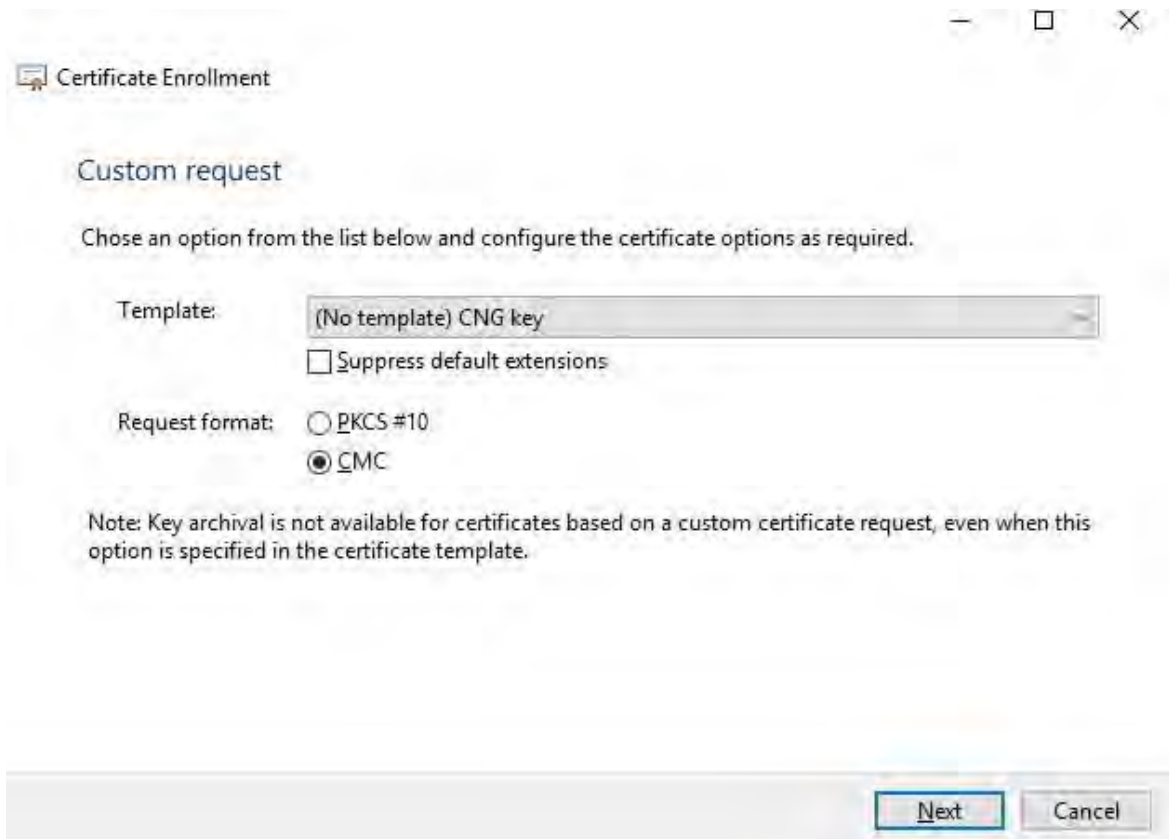


Se i Criteri di gruppo contengono già un criterio di registrazione dei certificati, è consigliabile confermare il resto di questo processo con il team di amministrazione del dominio prima di procedere.

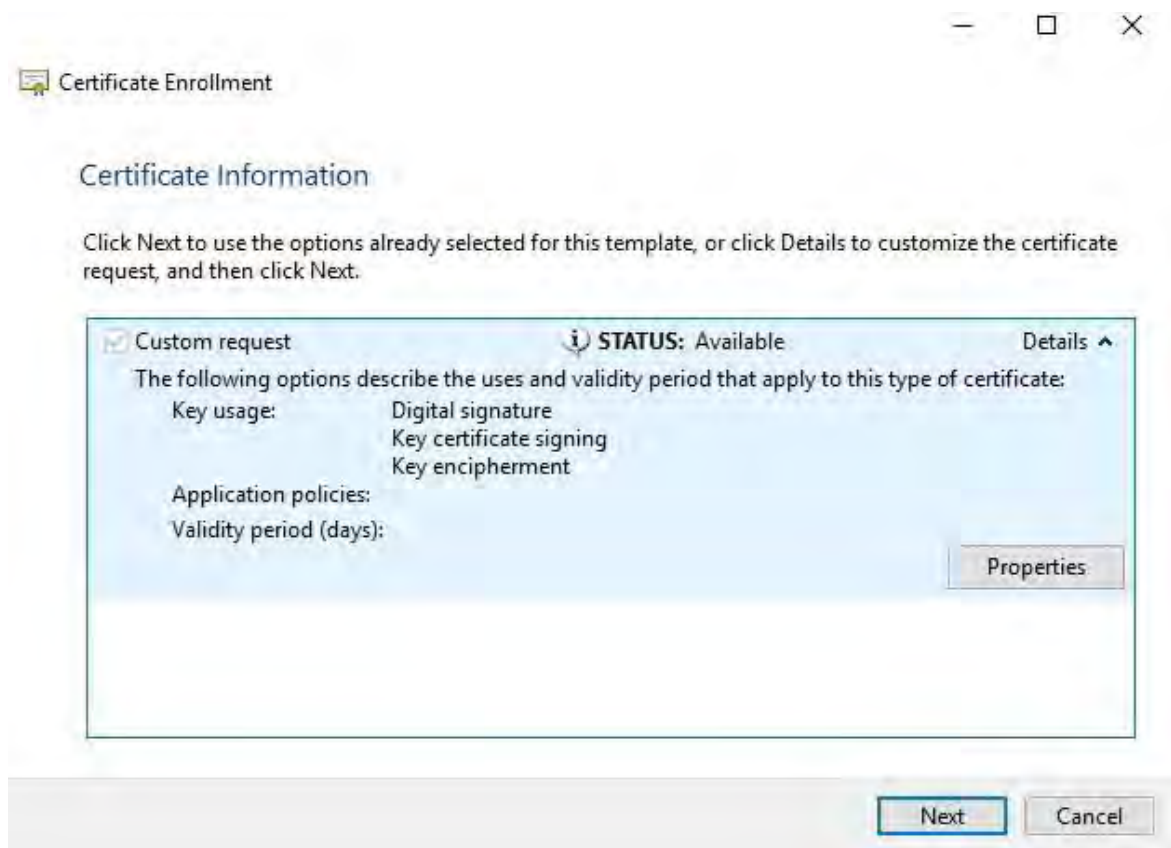
Fare clic su **Avanti**.



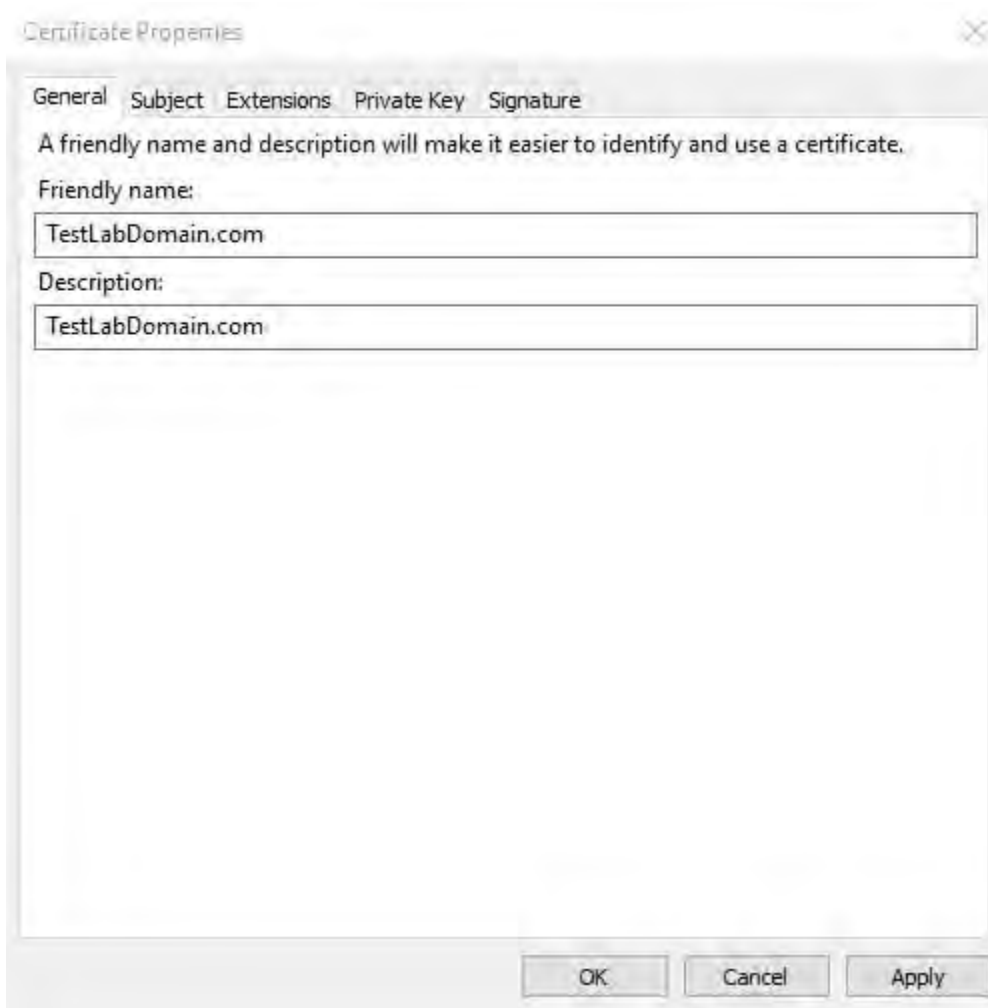
8. Selezionare il modello **di chiave CNG (Nessun modello)** e il formato di richiesta **CMC**, quindi fare clic su **Avanti**.



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



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

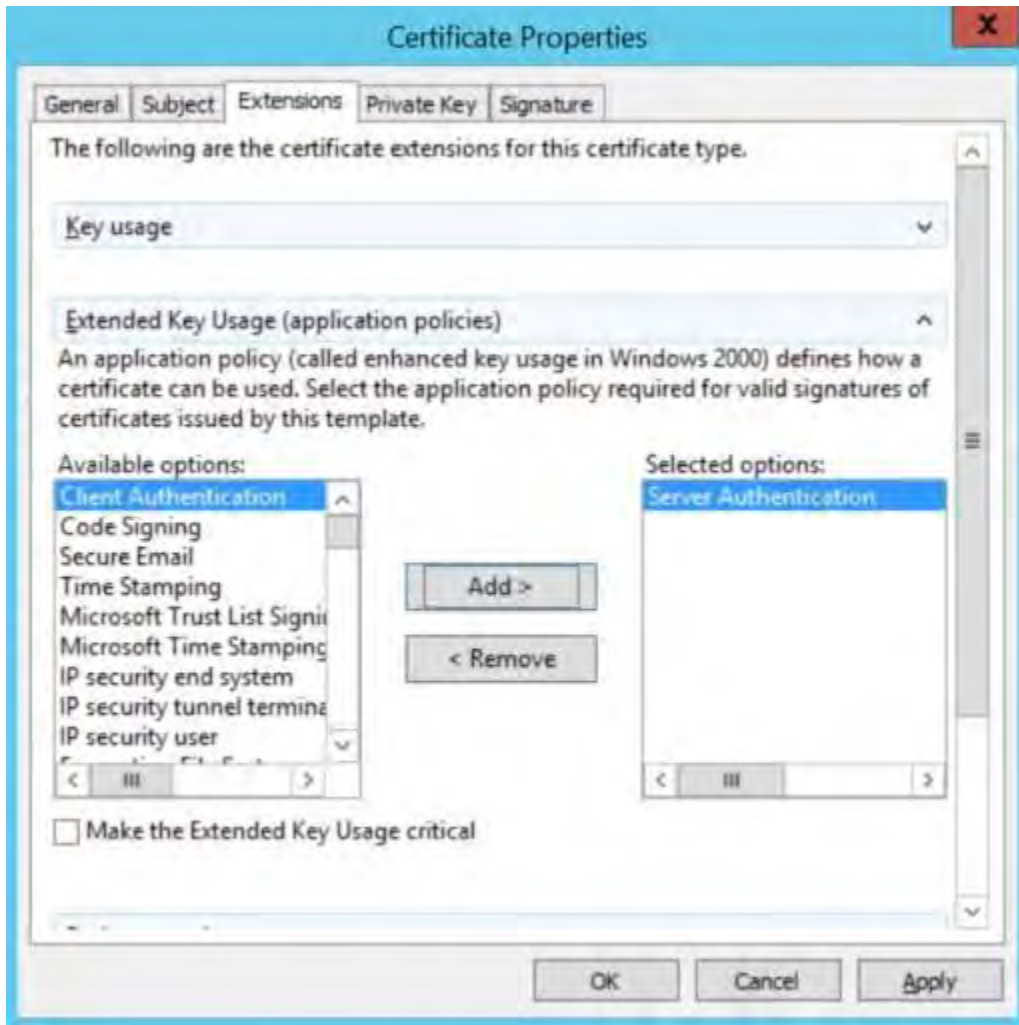


11. Nella scheda **Oggetto**, immettere i parametri necessari per il nome del soggetto.

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

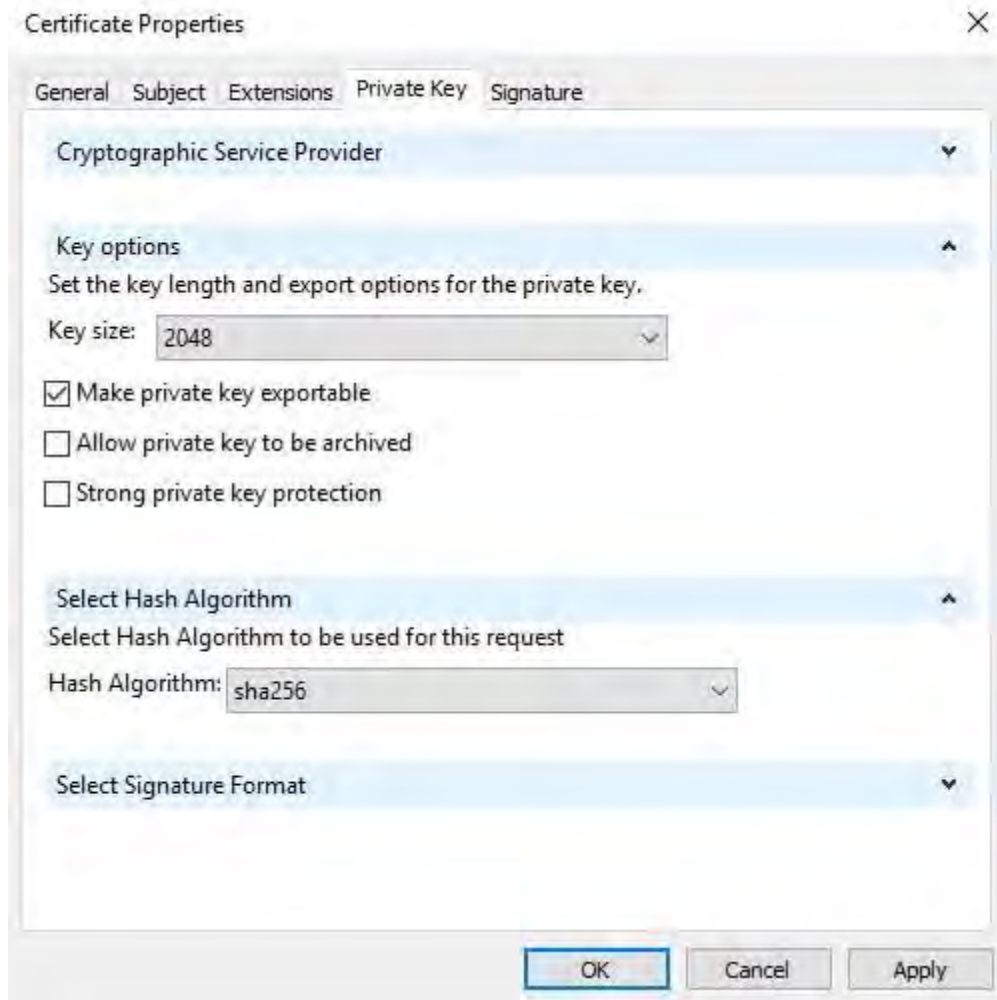


12. Nella scheda **Estensioni** espandere il menu **Utilizzo chiavi esteso (criteri dell'applicazione)**. Aggiungere **l'autenticazione server** dall'elenco delle opzioni disponibili.



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

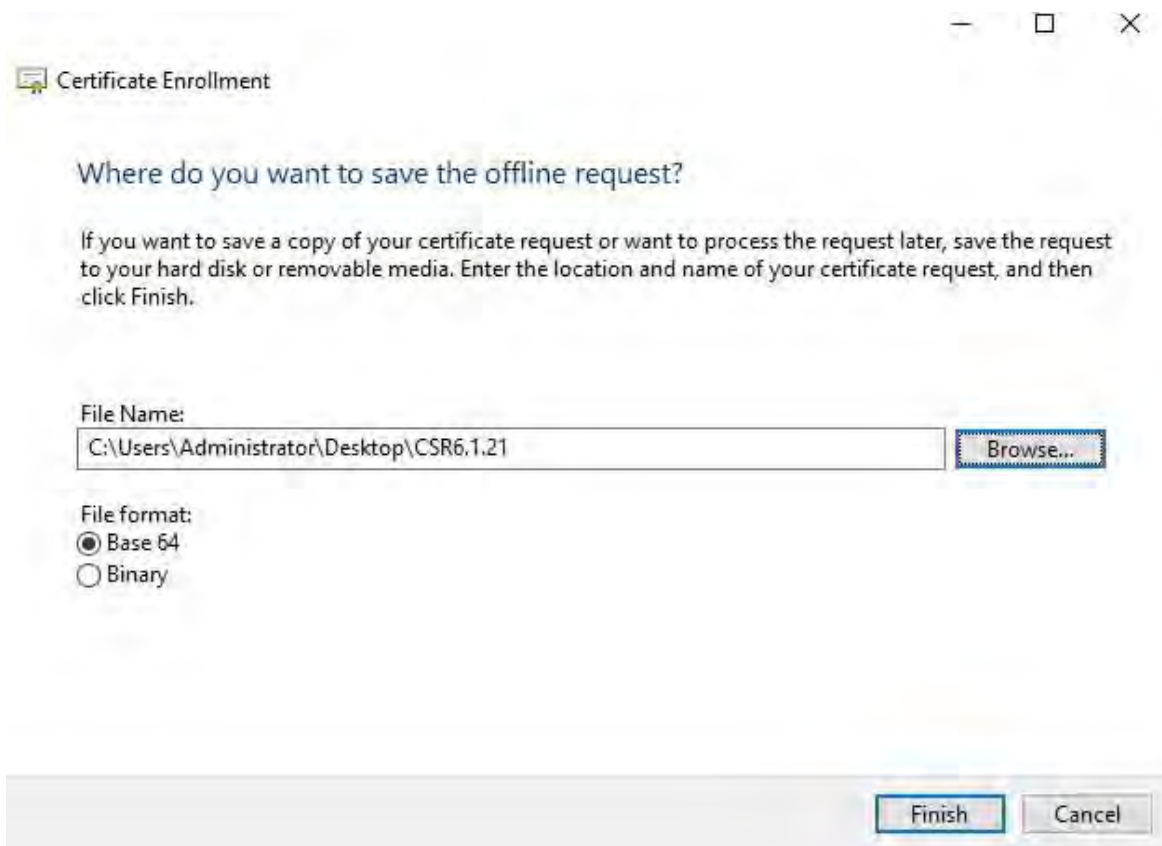
Imposta la dimensione della chiave su 2048 e seleziona l'opzione per rendere esportabile la chiave privata. Fare clic su **OK**.



14. Una volta definite tutte le proprietà del certificato, fare clic su **Avanti** nella **procedura guidata** Registrazione certificati.

15. 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.

16. Fare clic su **Fine**.



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

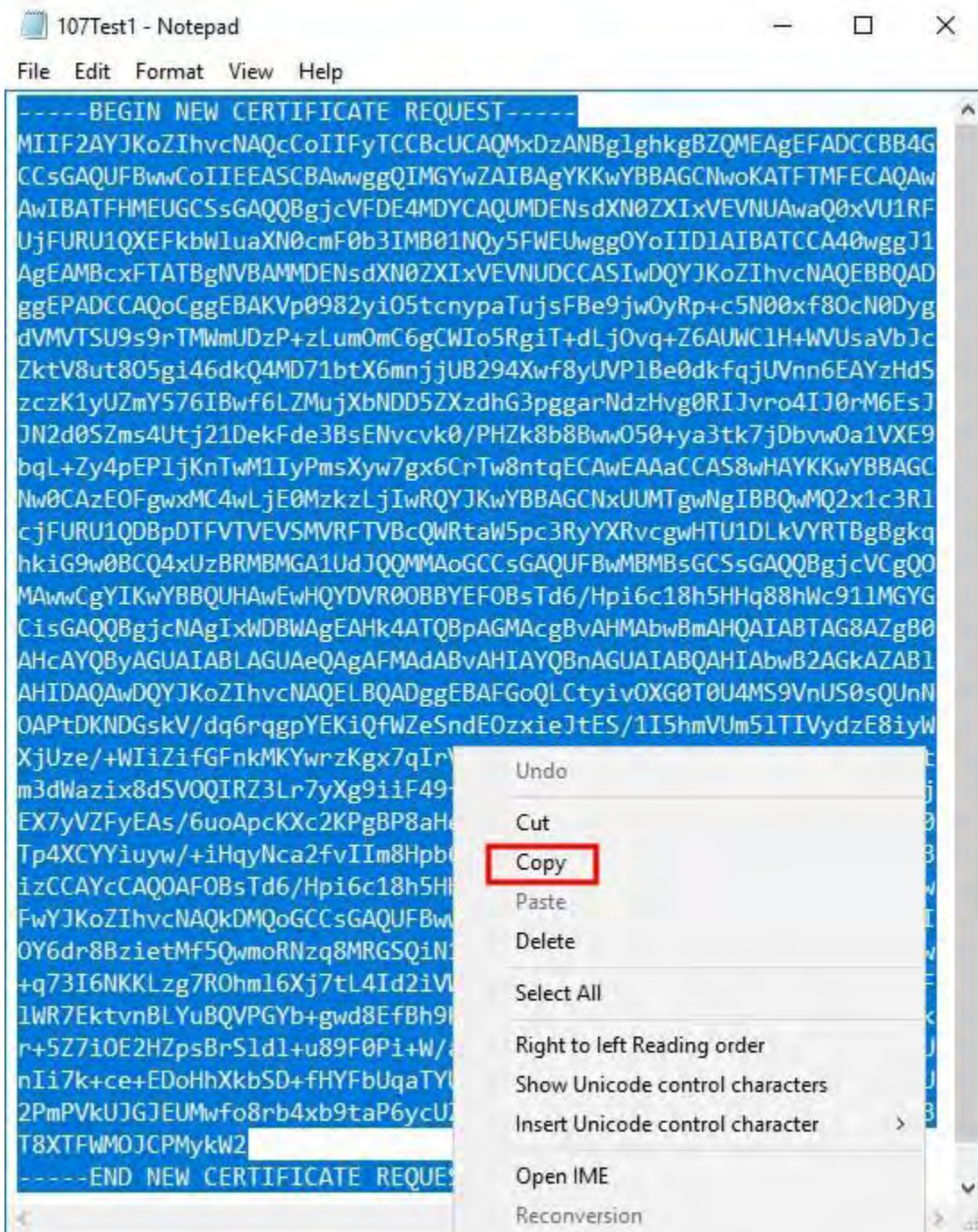
Carica il file .req per ricevere in cambio un certificato firmato

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](#).



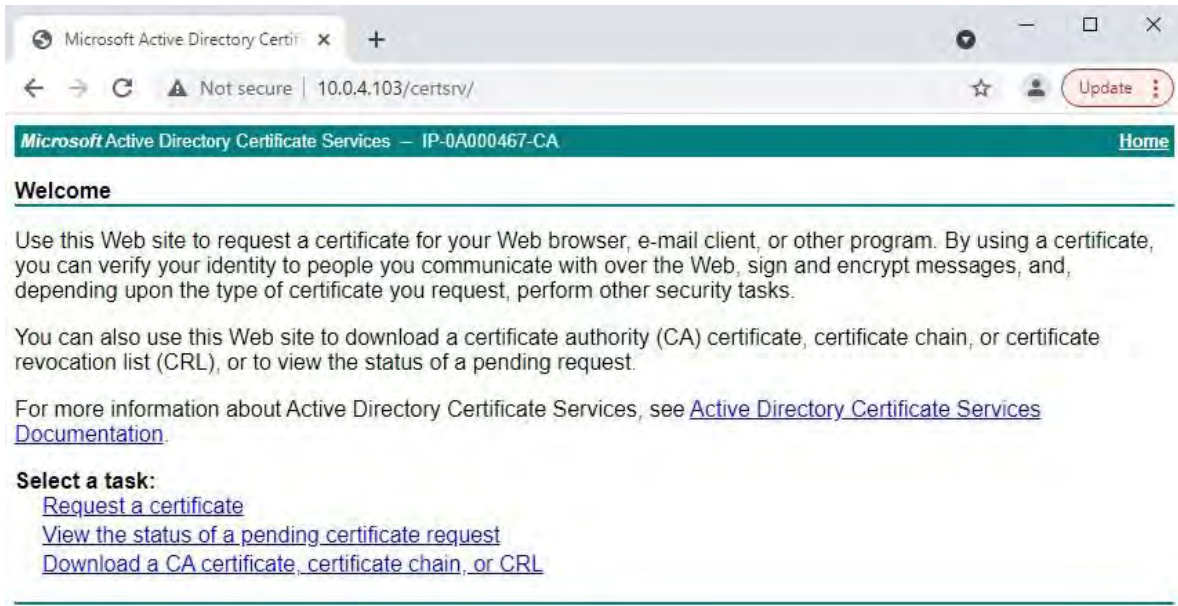
A meno che il dominio non abbia installato Servizi certificati Active Directory solo di recente o non sia stato installato solo per questo scopo, sarà necessario inviare questa richiesta seguendo una procedura separata configurata dal team di amministrazione del dominio. Si prega di confermare questo processo con loro prima di procedere.

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

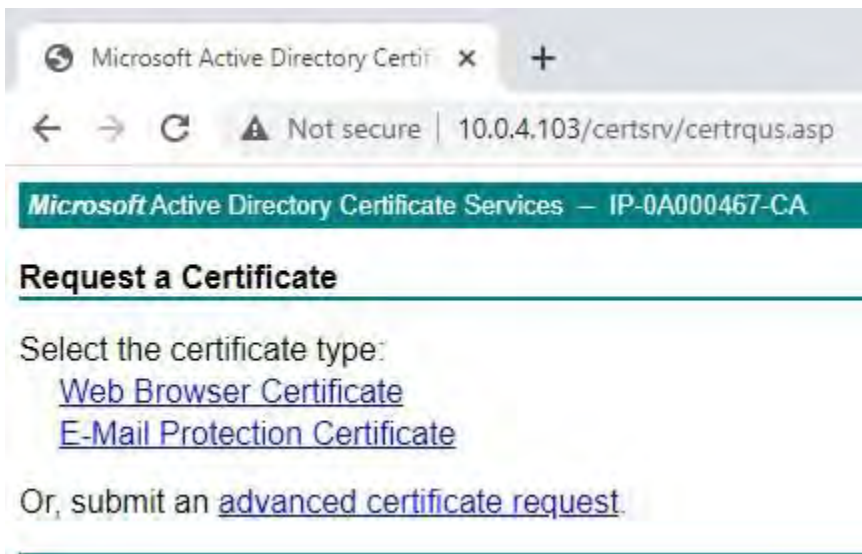


2. Copia l'intero contenuto del file. Sono incluse le linee tratteggiate che segnano l'inizio e la fine della richiesta di certificato.

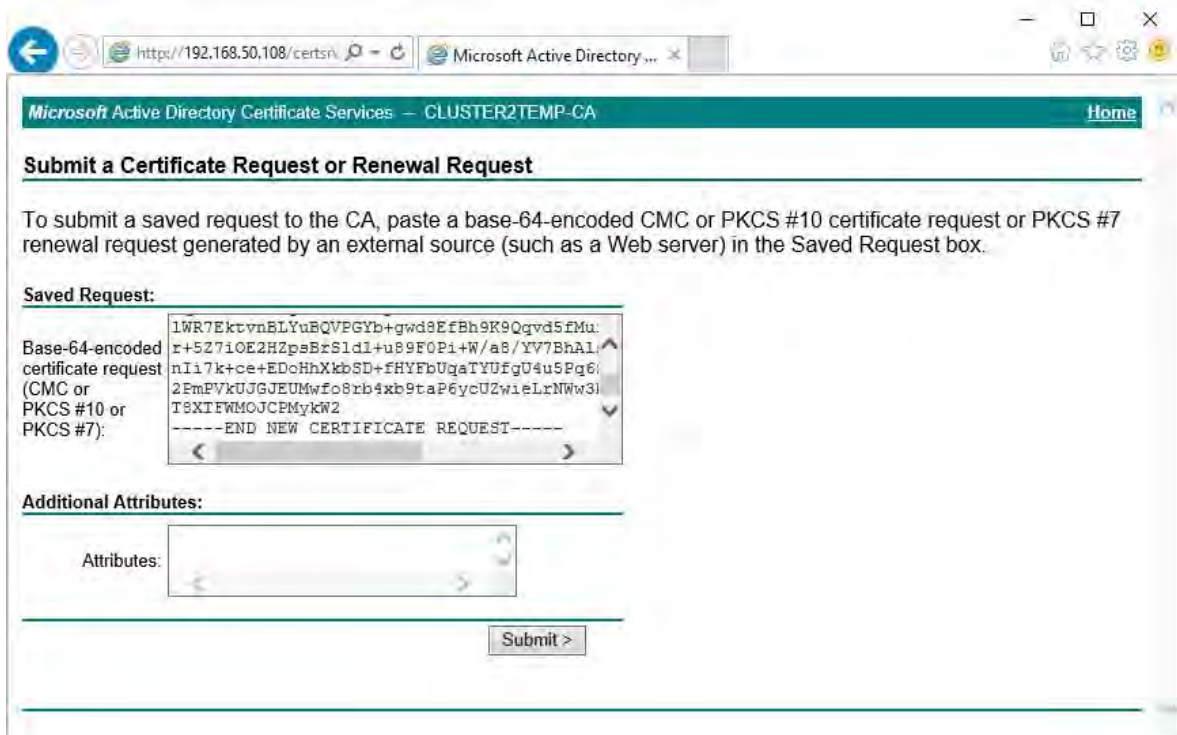
3. Apri un browser web e inserisci l'indirizzo della CA del dominio.



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



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.



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.

Installare il certificato manualmente

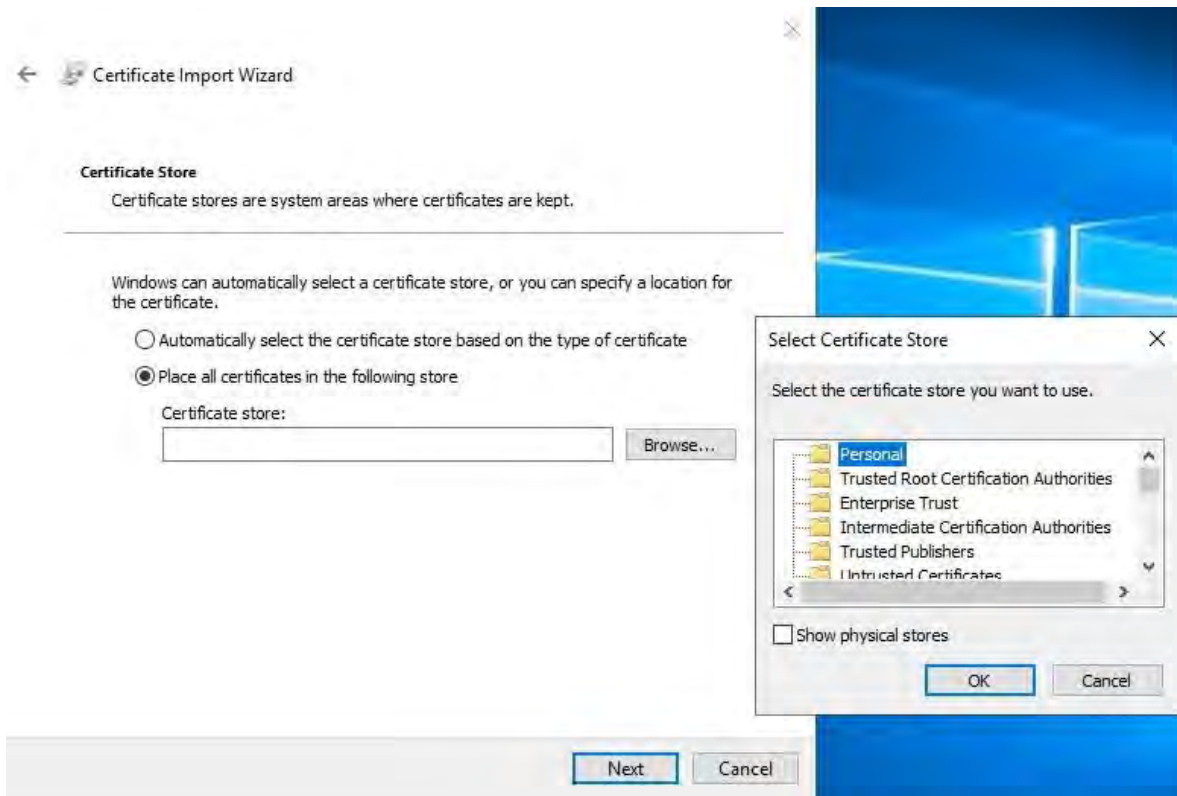
Se il certificato ti viene consegnato, puoi installarlo manualmente.

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.

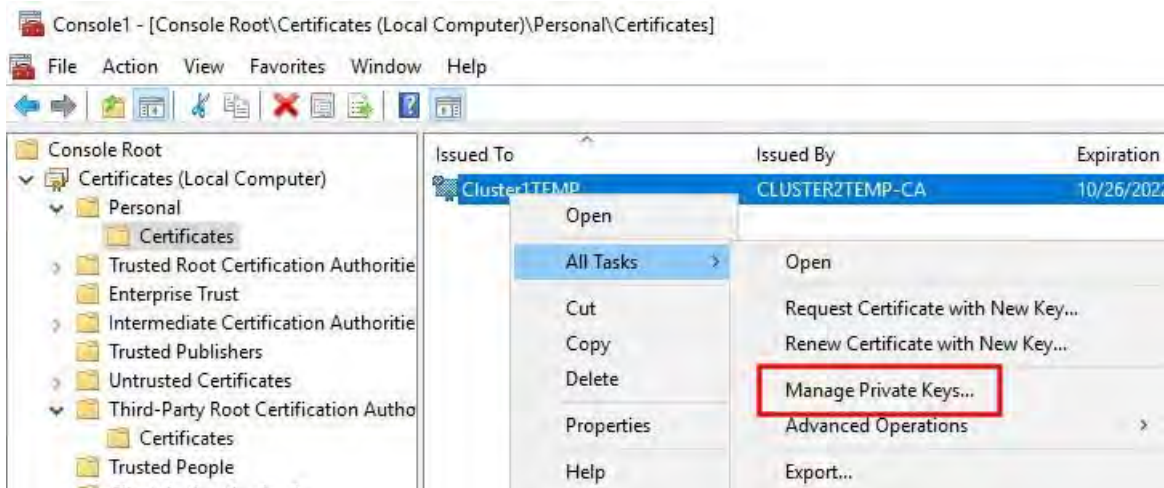
Selezionare questa opzione per installare il certificato per l'utente corrente e fare clic su **Avanti**.



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



- Completare la **procedura guidata** Installa certificato.
- Passare allo snap-in Certificati di Microsoft Management Console (MMC).
- 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**.



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.

Assicuratevi 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 prima di procedere.

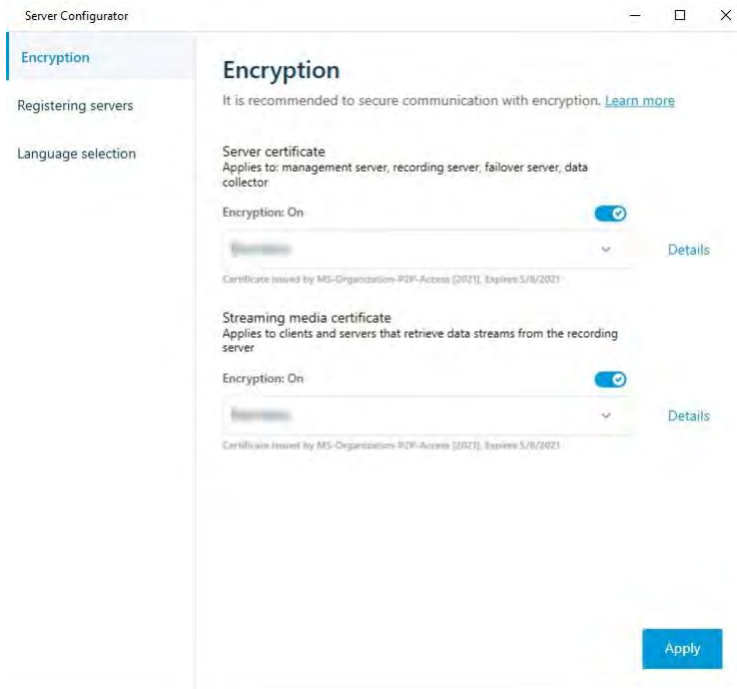
Abilitare la crittografia del server per i server di gestione e i server di registrazione

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 del server**
Da:
 - Il menu Start di Windowso
 - 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.

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.



5. 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 registrazione.

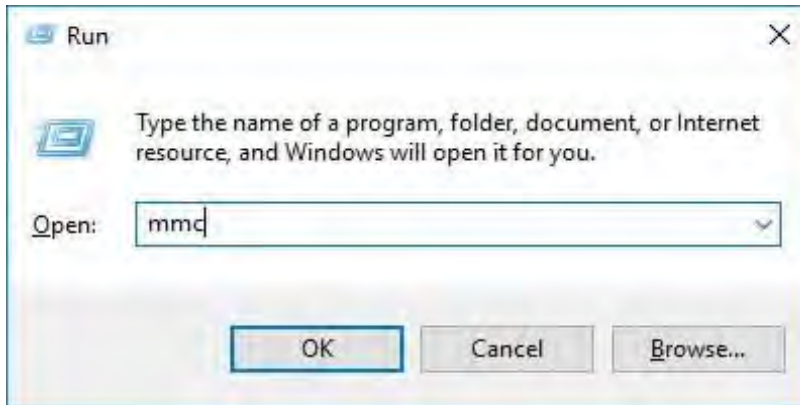
Installare i certificati in un ambiente di gruppo di lavoro per la comunicazione con il server di gestione o il server di registrazione

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 sia allo scenario di dominio che a quello di CA commerciale.

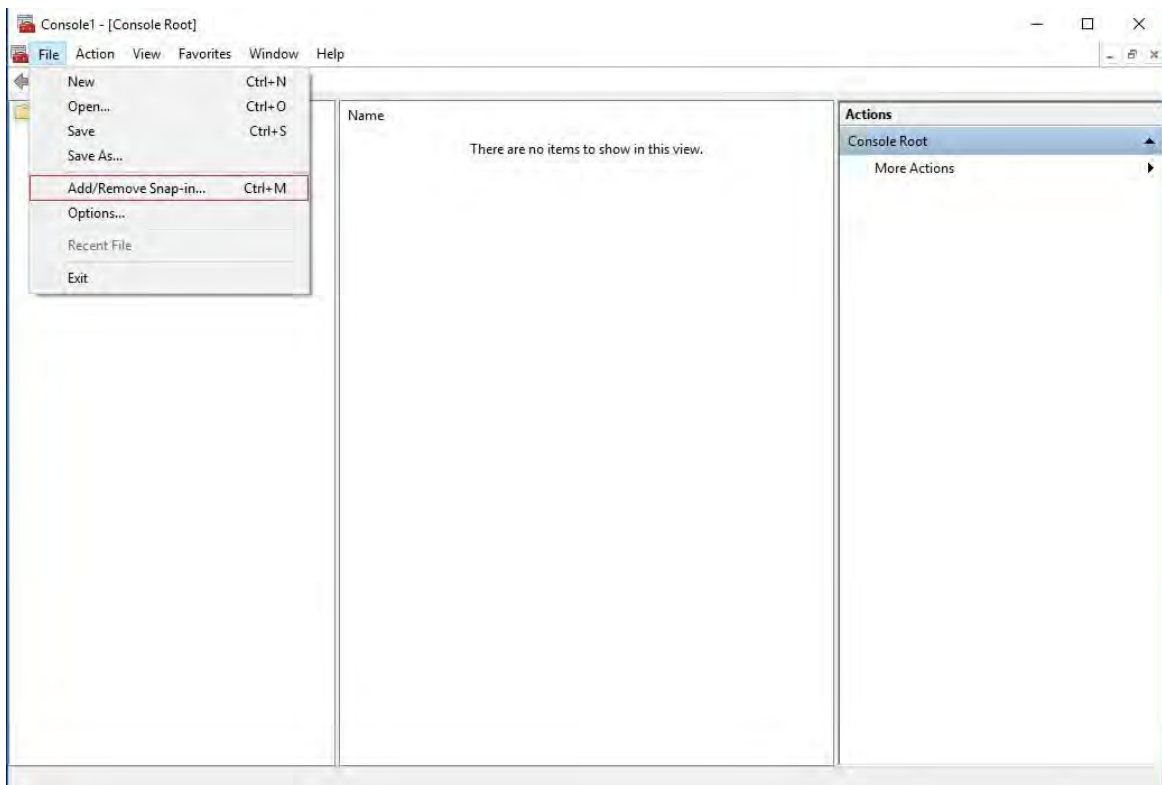
Aggiungere un certificato CA al server

Aggiungere il certificato CA al server effettuando le seguenti operazioni.

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

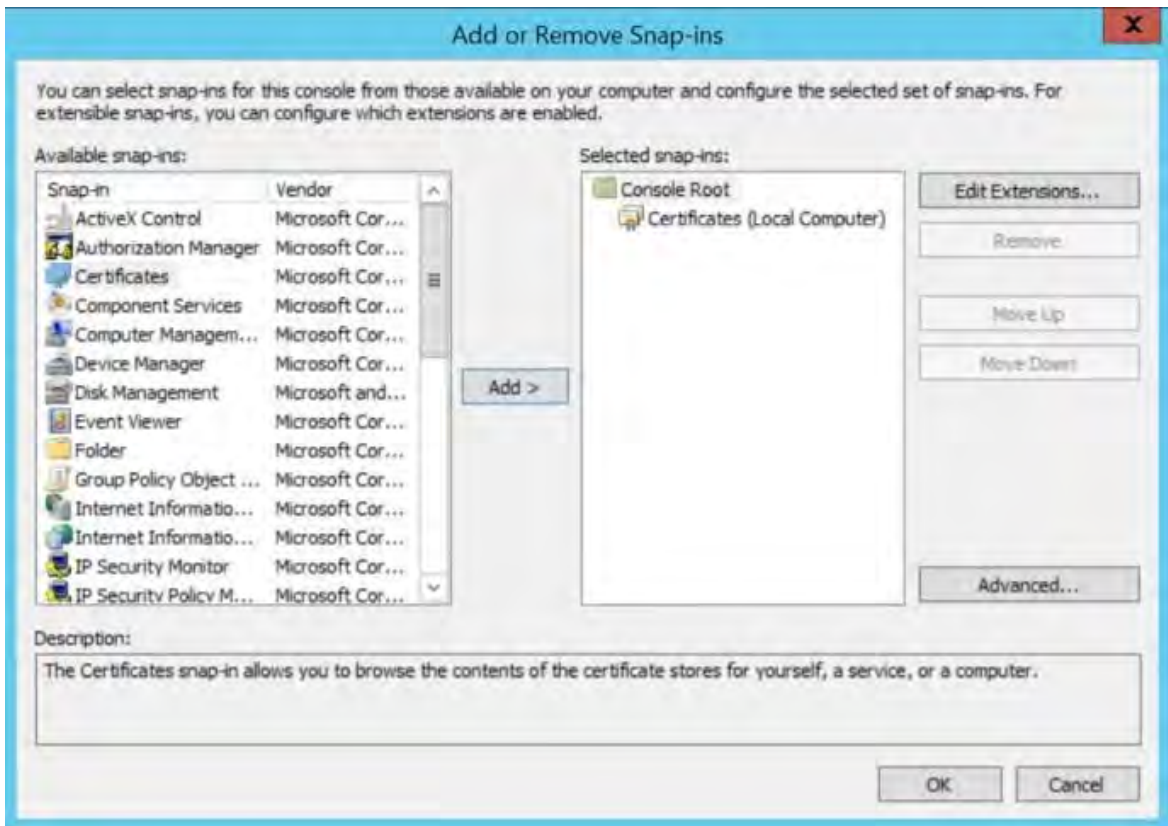


2. In Microsoft Management Console, dal menu **File** selezionare **Aggiungi/Rimuovi snap-in....**

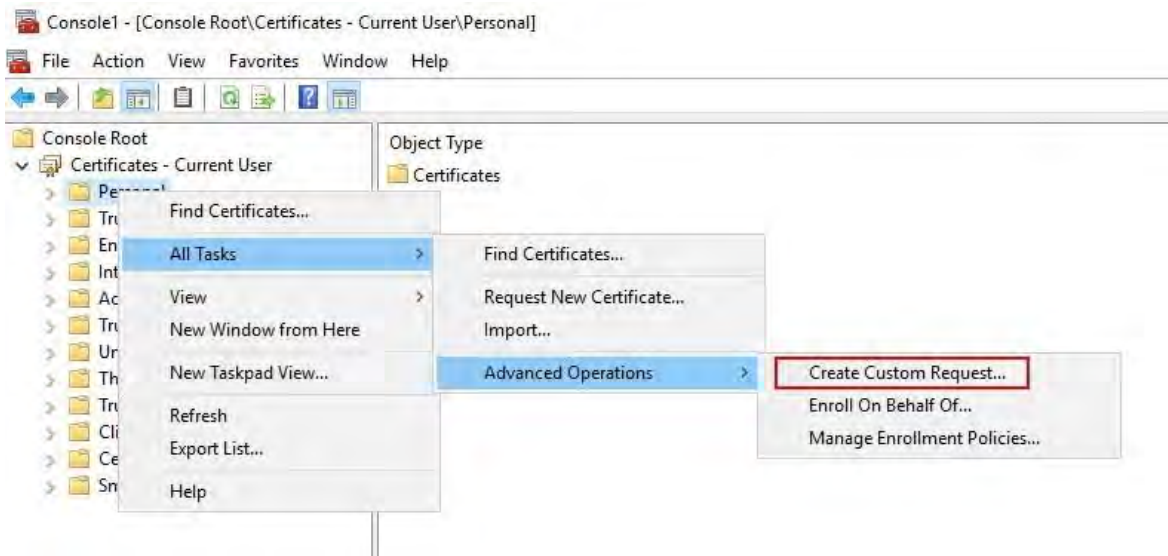


3. Selezionare lo snap-in Certificati e fare clic su **Aggiungi**.

Fare clic su **OK**.

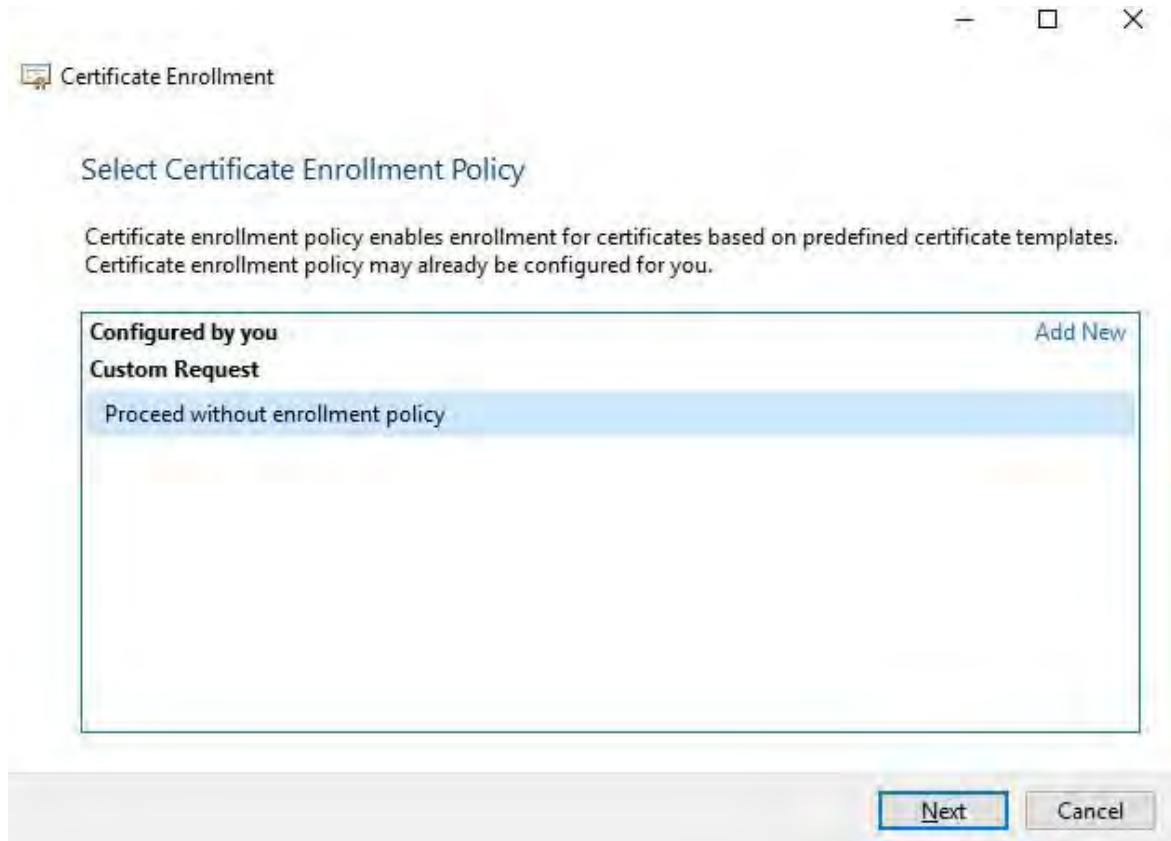


4. Espandere l'oggetto Certificati. Fare clic con il pulsante destro del mouse sulla **cartella Personale** e selezionare **Tutte le attività > Operazioni avanzate > Crea richiesta personalizzata**.

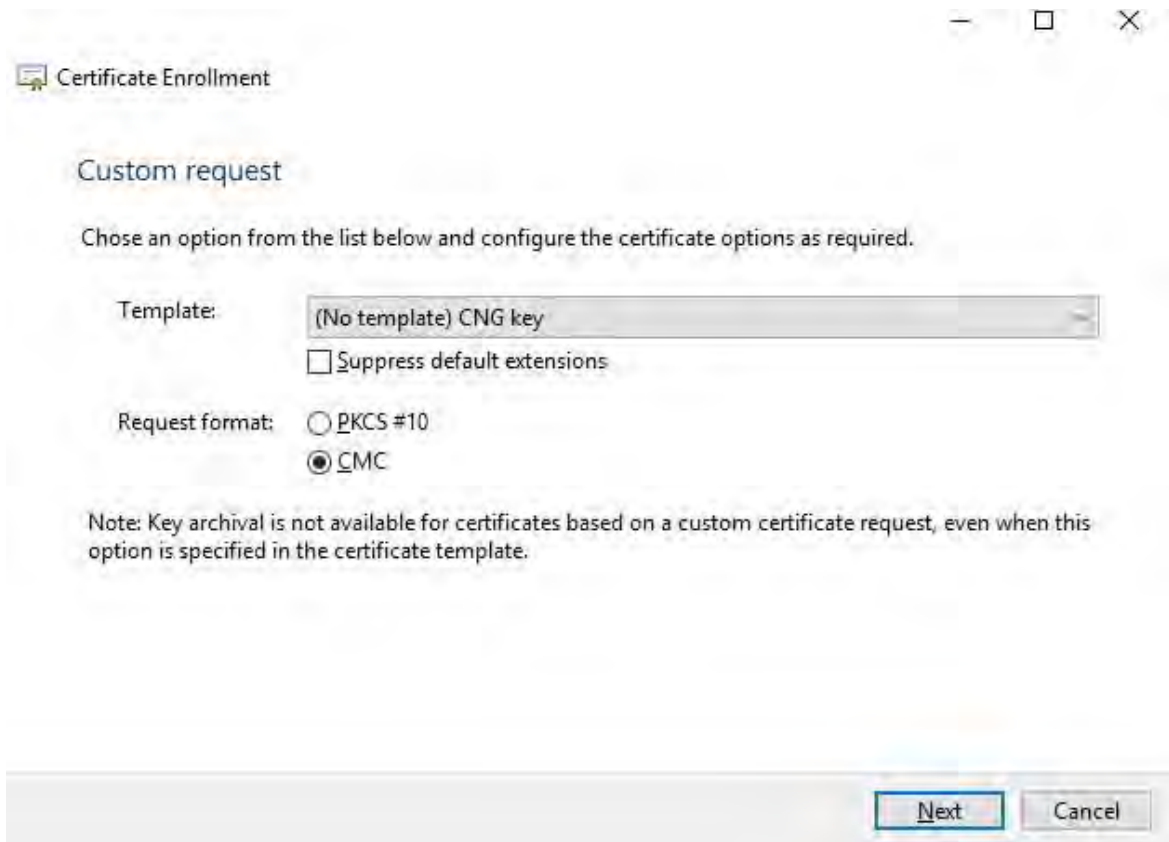


5. Fare clic su **Avanti** nella procedura guidata **Registrazione certificati** e selezionare **Procedi senza criteri di registrazione**.

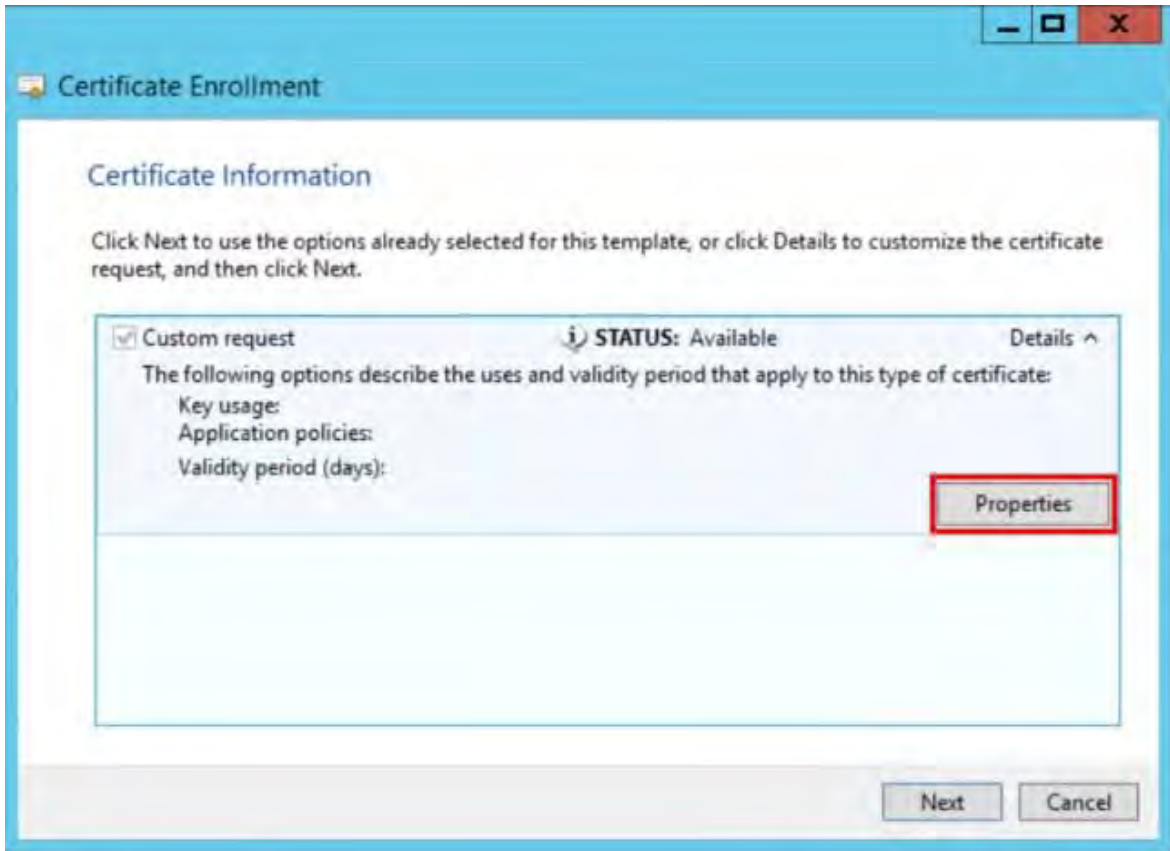
Fare clic su **Avanti**.



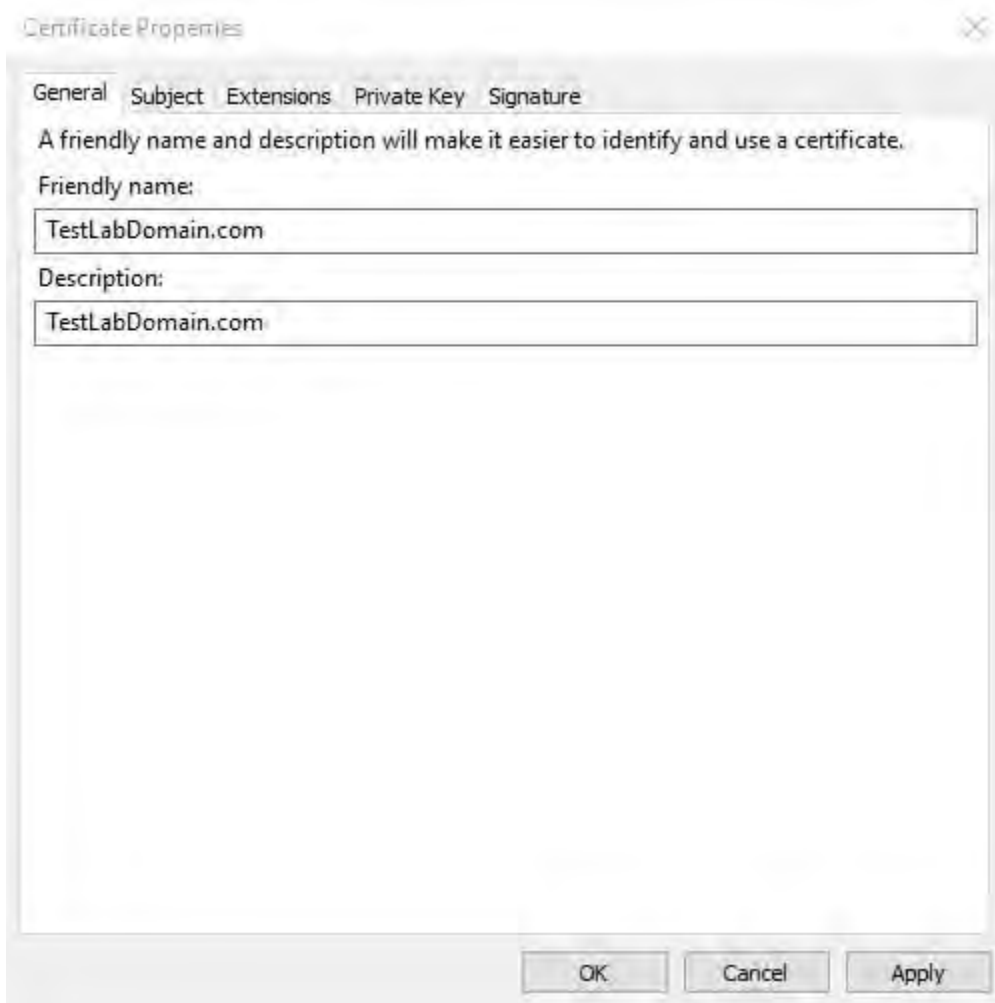
6. Selezionare il modello **di chiave CNG (Nessun modello)** e il formato di richiesta **CMC**, quindi fare clic su **Avanti**.



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



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

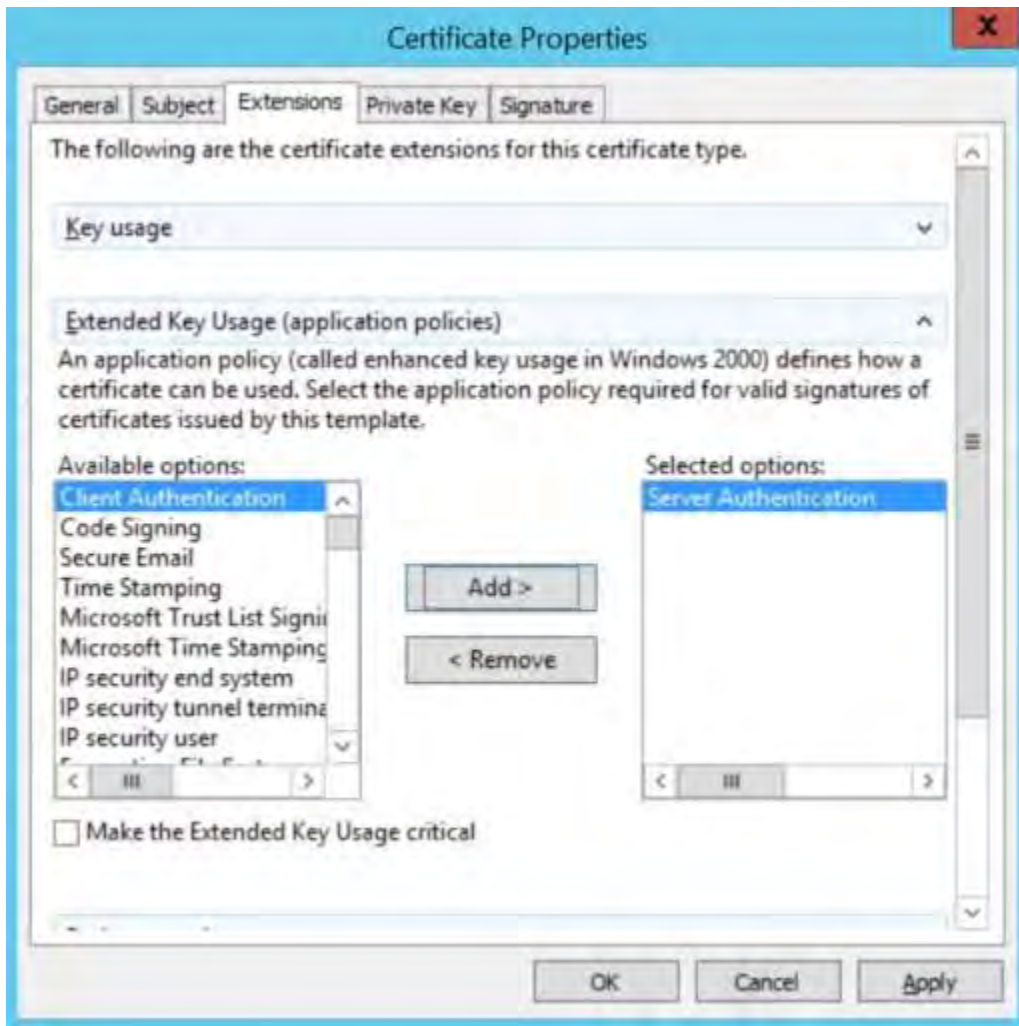


9. Nella scheda **Oggetto**, immettere i parametri necessari per il nome del soggetto.

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

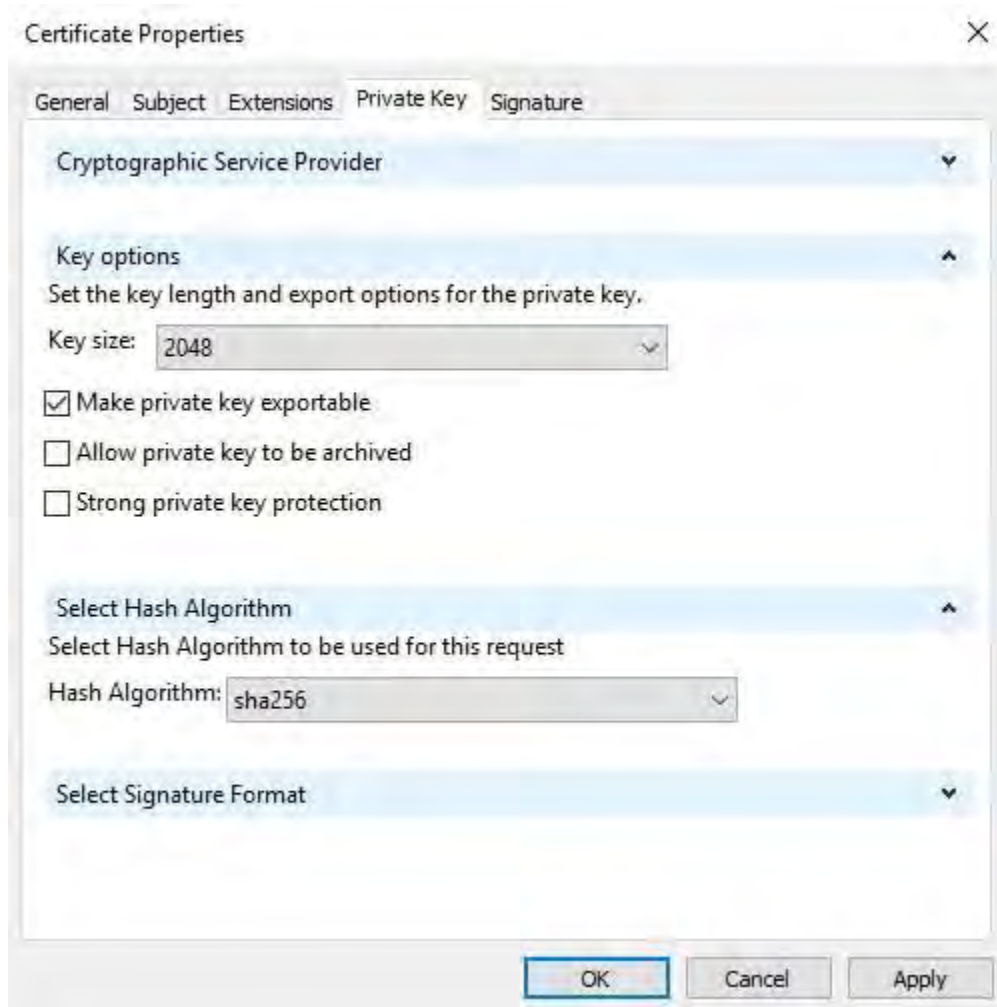


10. Nella scheda **Estensioni** espandere il menu **Utilizzo chiavi esteso (criteri dell'applicazione)**. Aggiungere **l'autenticazione** server dall'elenco delle opzioni disponibili.



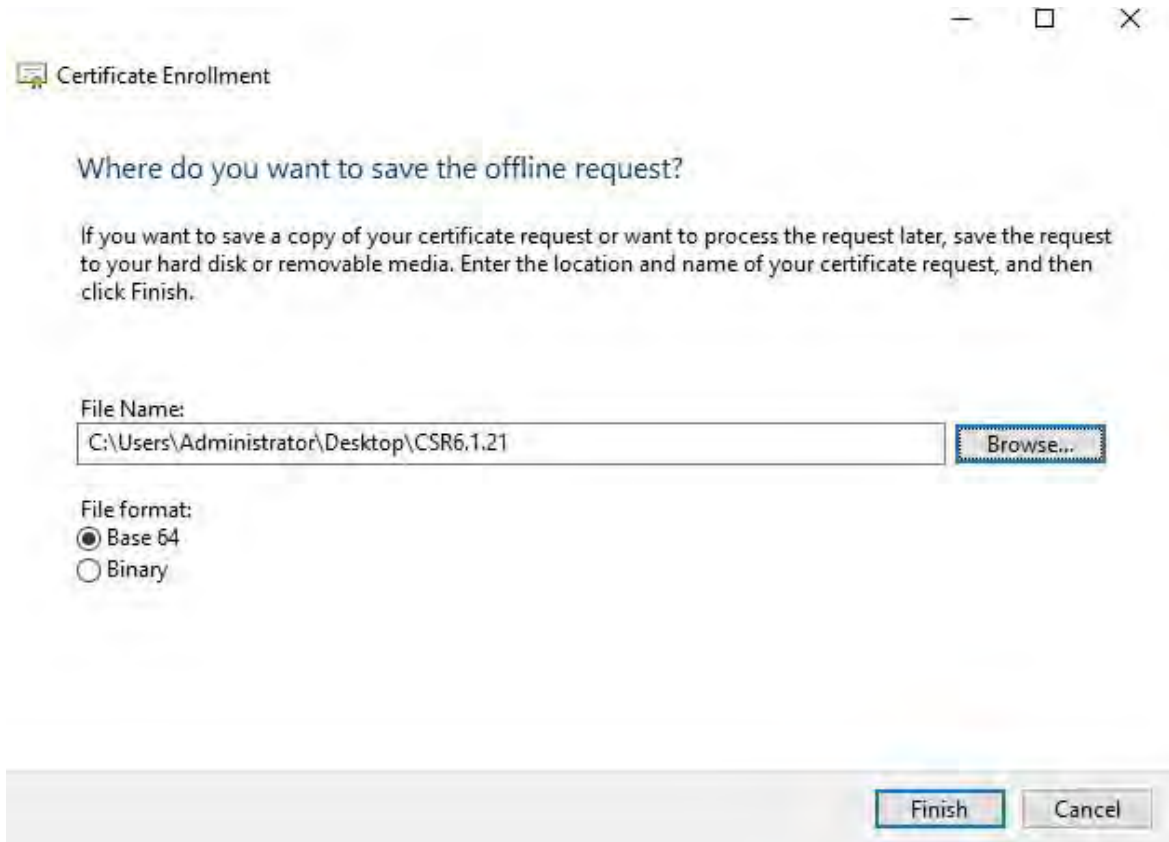
11. Nella scheda **Chiave privata** espandere il menu **Opzioni chiave**.

Imposta la dimensione della chiave su 2048 e seleziona l'opzione per rendere esportabile la chiave privata. Fare clic su **OK**.



12. Quando tutte le proprietà del certificato sono state definite, fare clic su **Avanti** nella finestra di dialogo **Registrazione certificati** mago.
13. 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.

14. Fare clic su **Fine**.



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

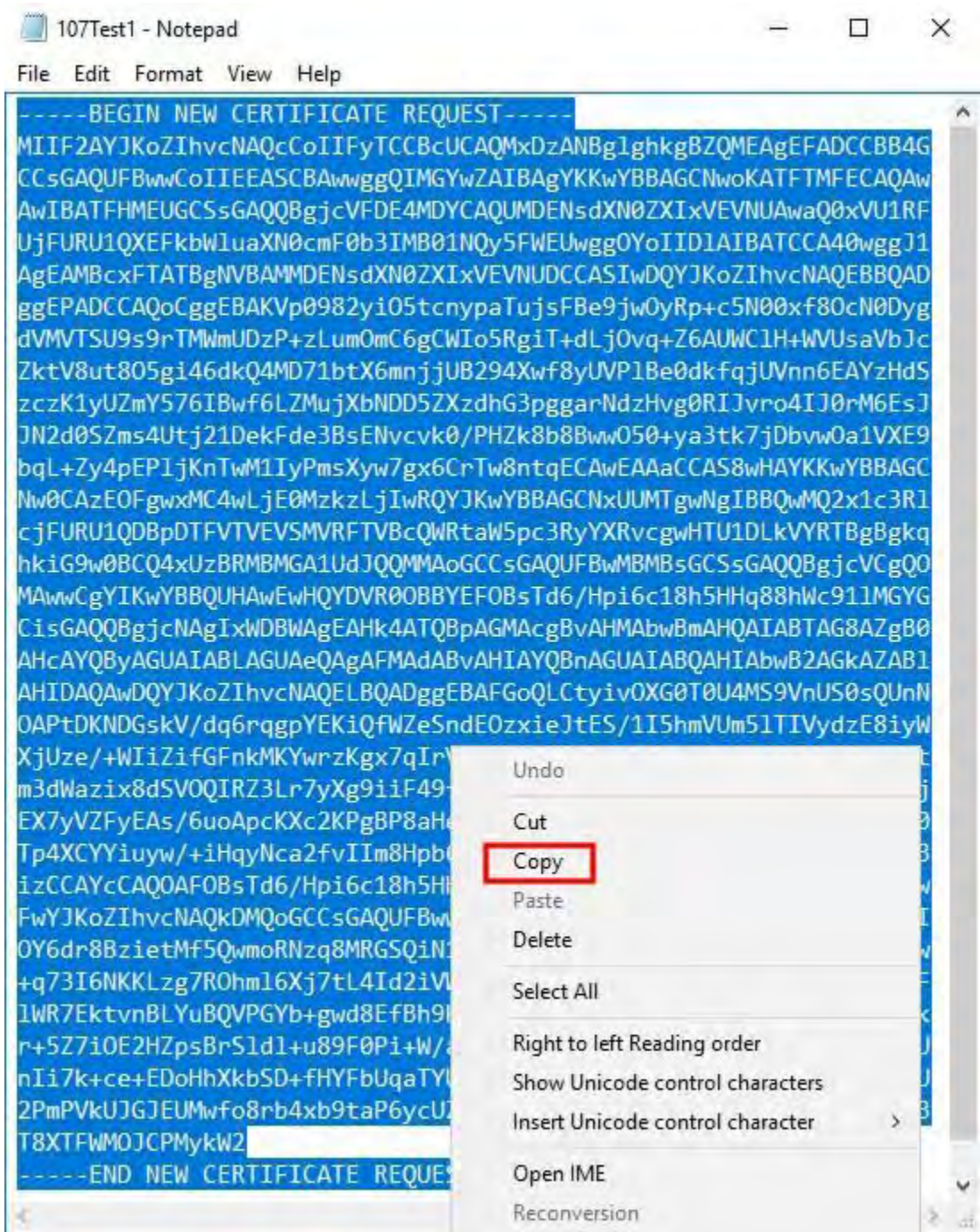
Carica il file .req per ricevere in cambio un certificato firmato

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.

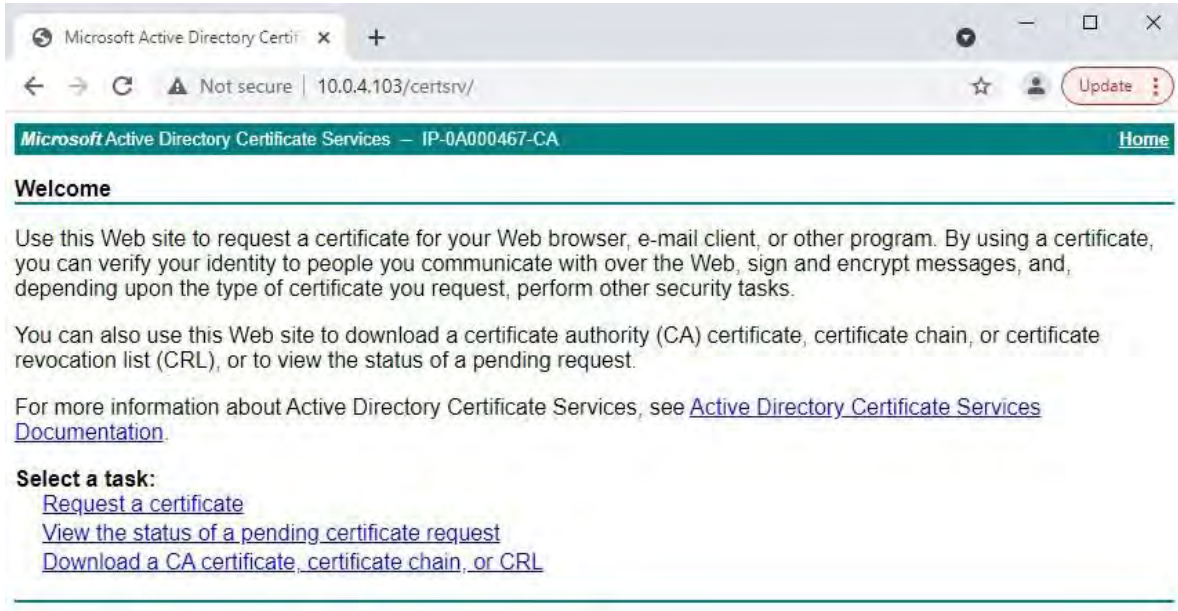
1. Individua la posizione del file .req e aprilo in Blocco note.



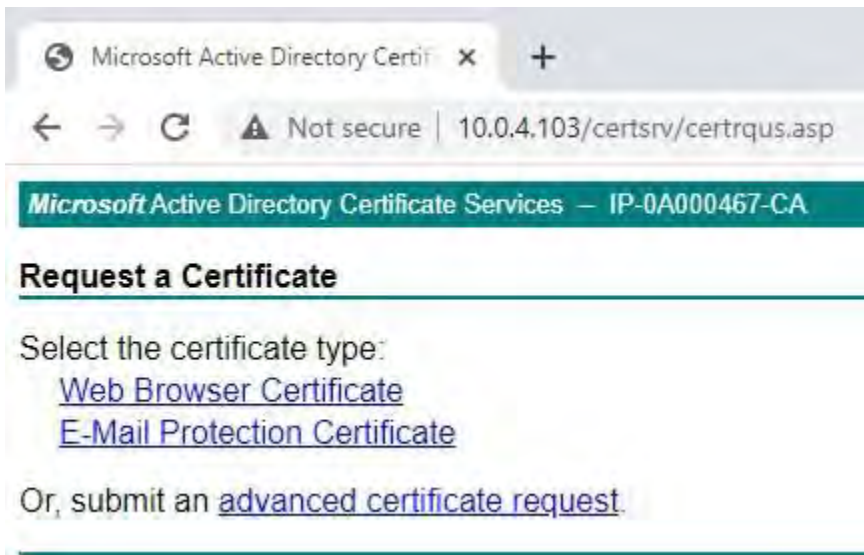
2. Copia l'intero contenuto del file. Sono incluse le linee tratteggiate che segnano l'inizio e la fine della richiesta di certificato.

3. Apri un browser web e inserisci l'indirizzo della CA interna, che dovrebbe trovarsi in: [ip.ad.dr.ess/certsrv].

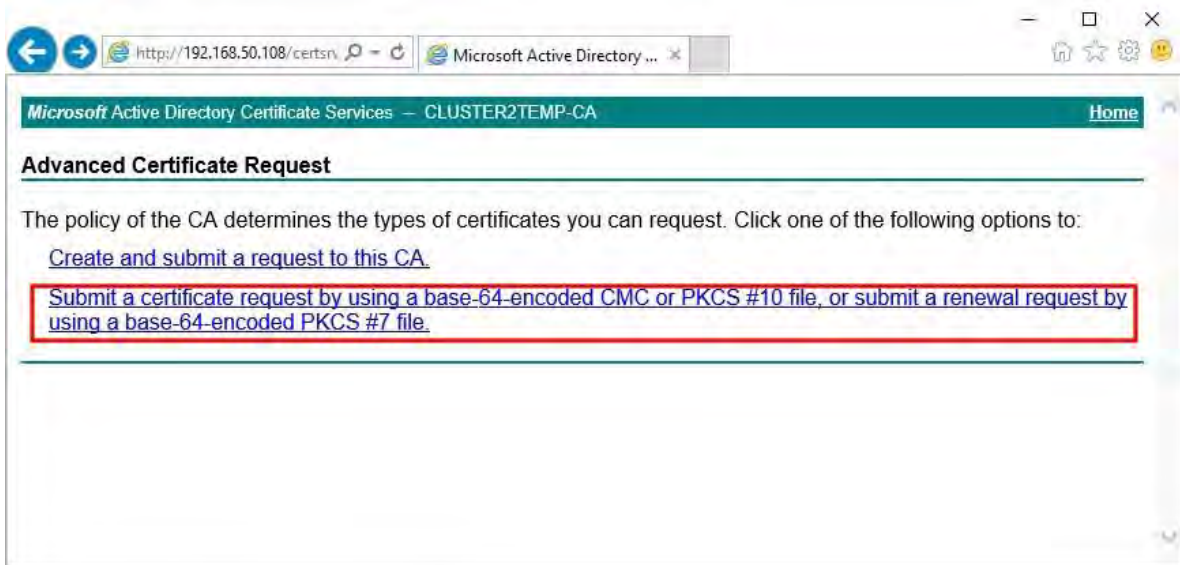
Dove, ip.ad.dr.ess è l'indirizzo IP o il nome DNS del server host di Servizi certificati Active Directory della rete interna.



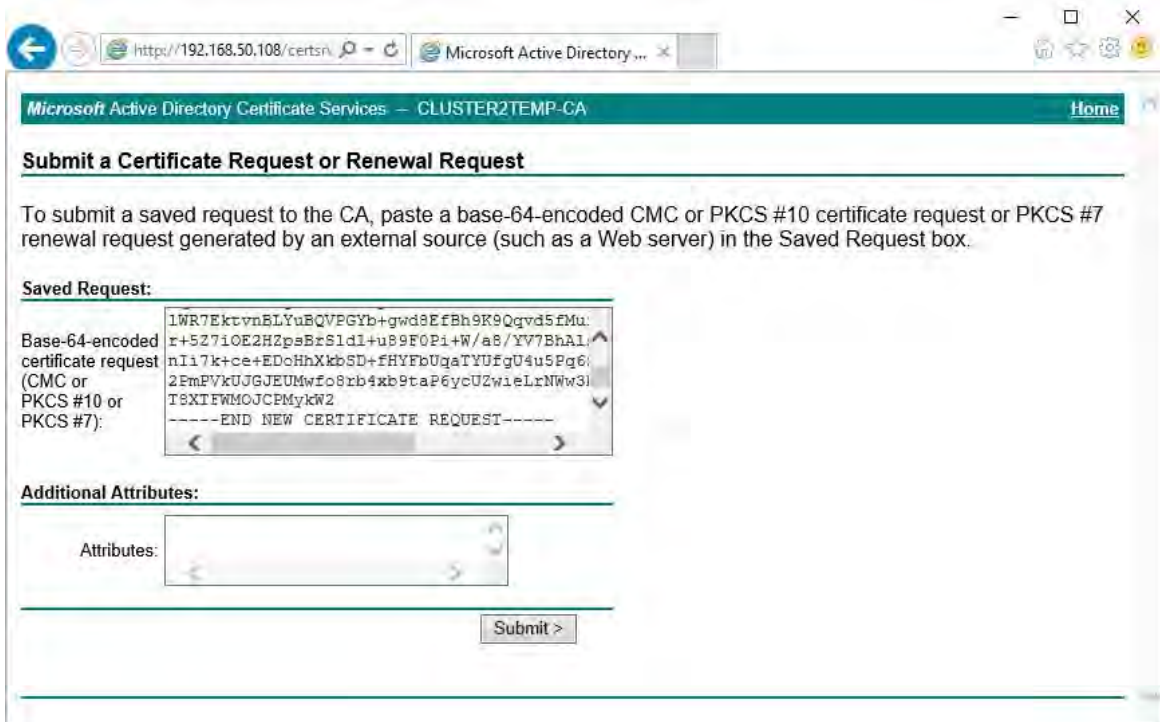
4. Fai clic sul **link Richiedi un certificato**.
5. Fare clic sul collegamento di **richiesta avanzata del certificato**.



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



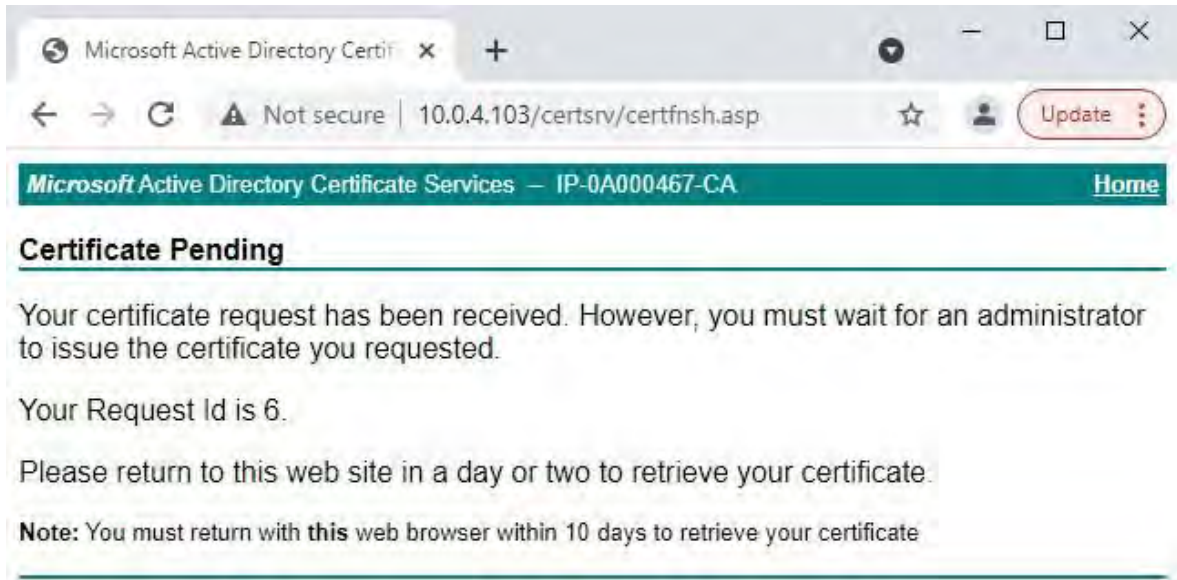
- 7. Incolla il contenuto del file .req nel modulo. Se è necessario selezionare un modello di certificato, selezionare **Server Web** dall'elenco Modello di certificato.



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

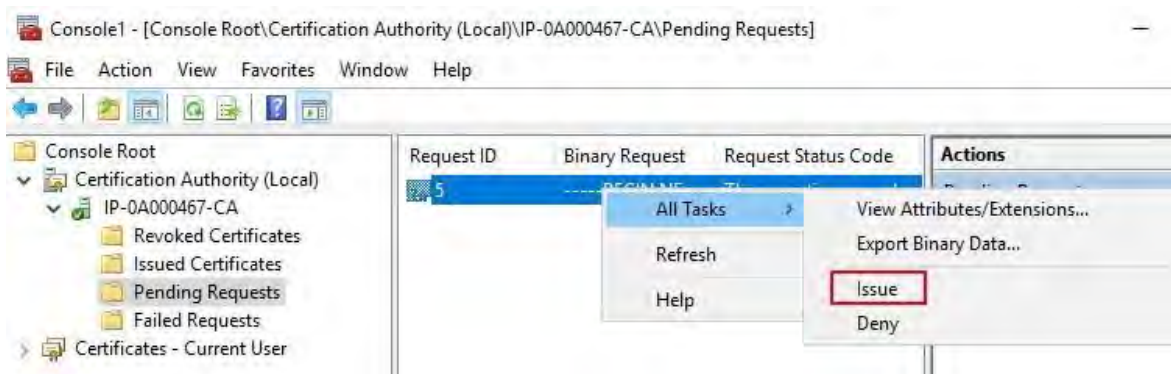


Emettere i certificati manualmente

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

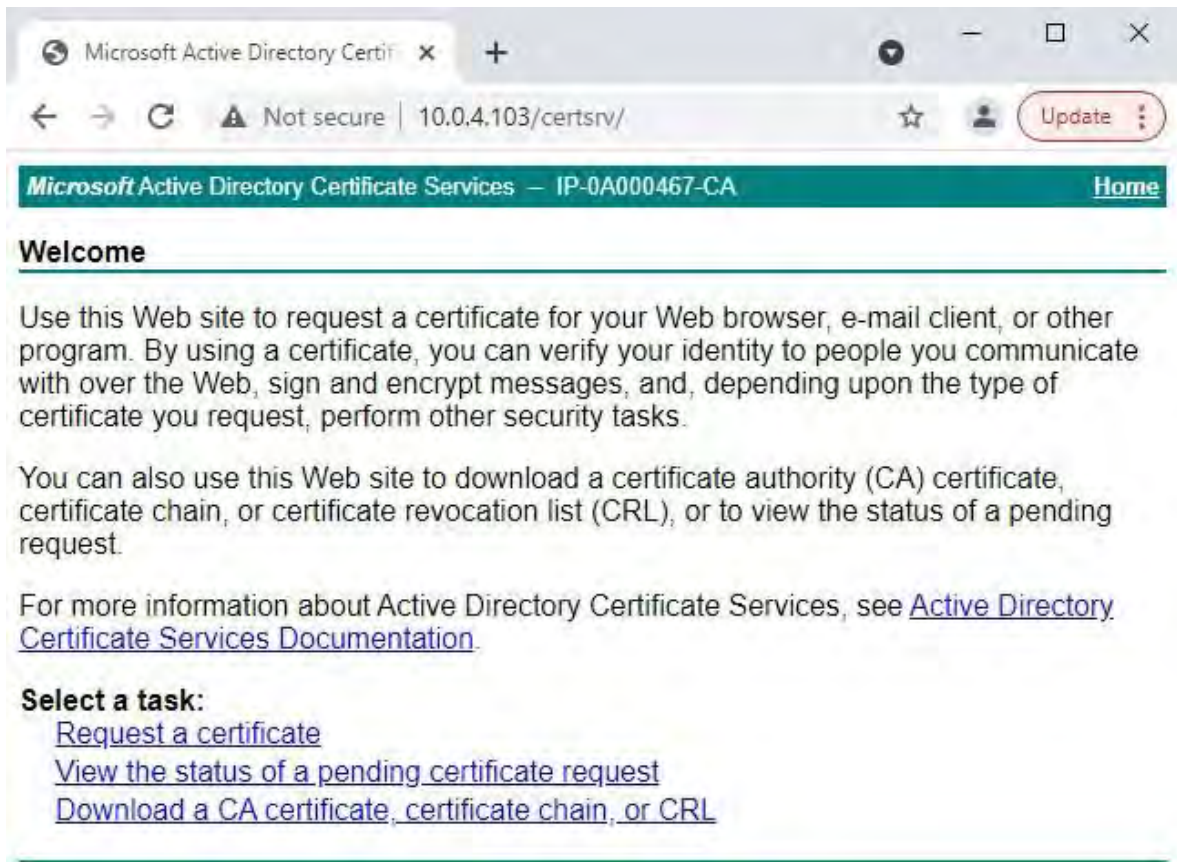
1. Aprire Microsoft Management Console (MMC).
2. Passare allo **snap-in** Autorità di certificazione.
3. Espandere l' oggetto **Autorità di certificazione**.

Nella cartella **Richieste in sospenso** fare clic con il pulsante destro del mouse sull'ID richiesta corrispondente e, nell' **elenco Tutte le attività**, selezionare **Problema**.

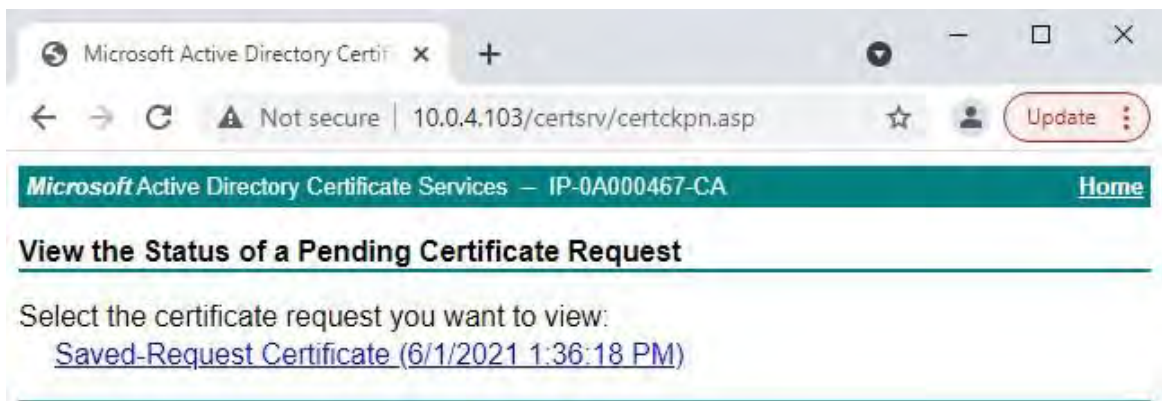


4. Aprire un browser e accedere al sito interno di CA IIS all'indirizzo [ip.ad.dr.ess/certsrv].

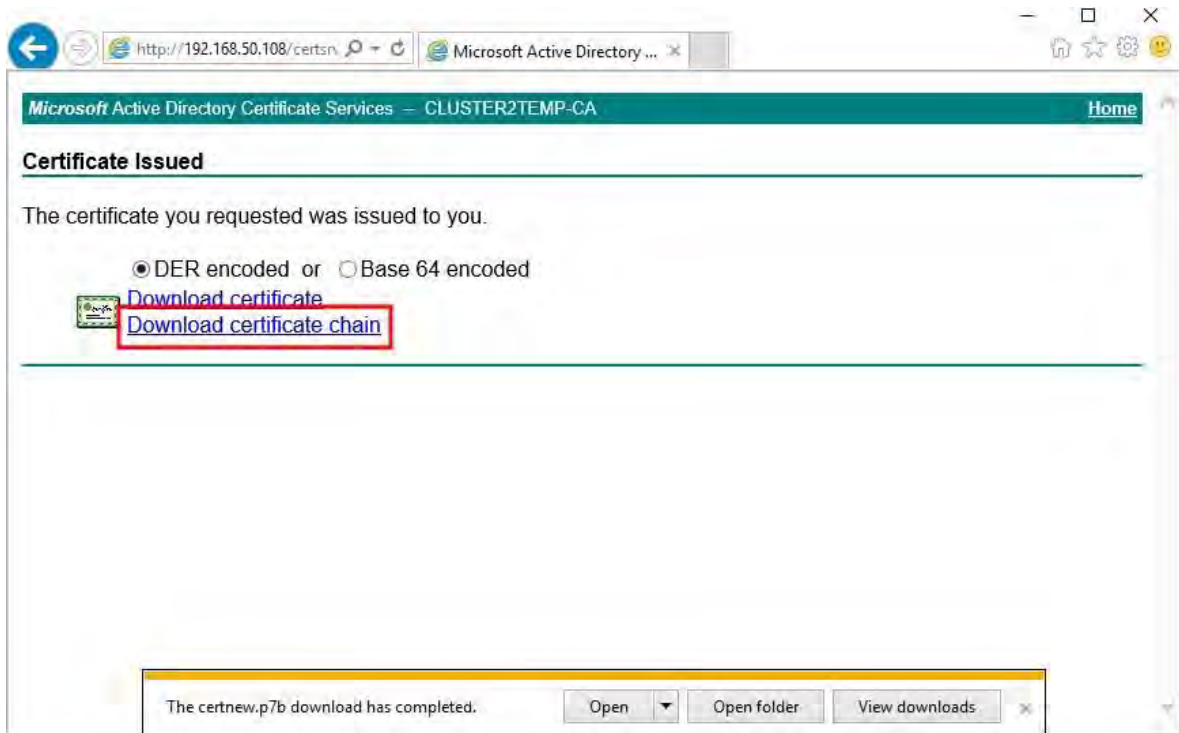
Fare clic sul collegamento **Visualizza lo stato di una richiesta di certificato in sospeso**.



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



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

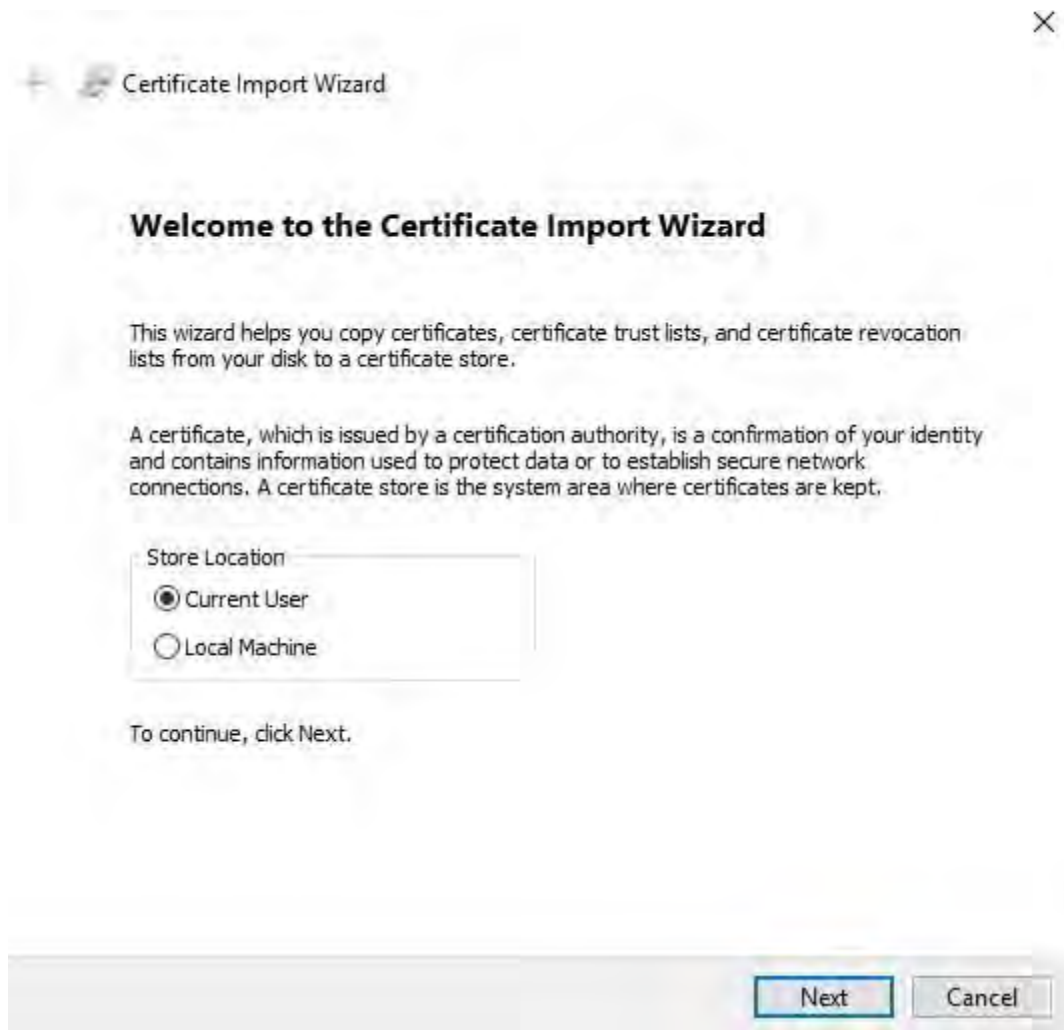


7. Passare alla cartella dei download, fare clic con il pulsante destro del mouse sul certificato e selezionare **Installa certificato** dal menu di scelta rapida.



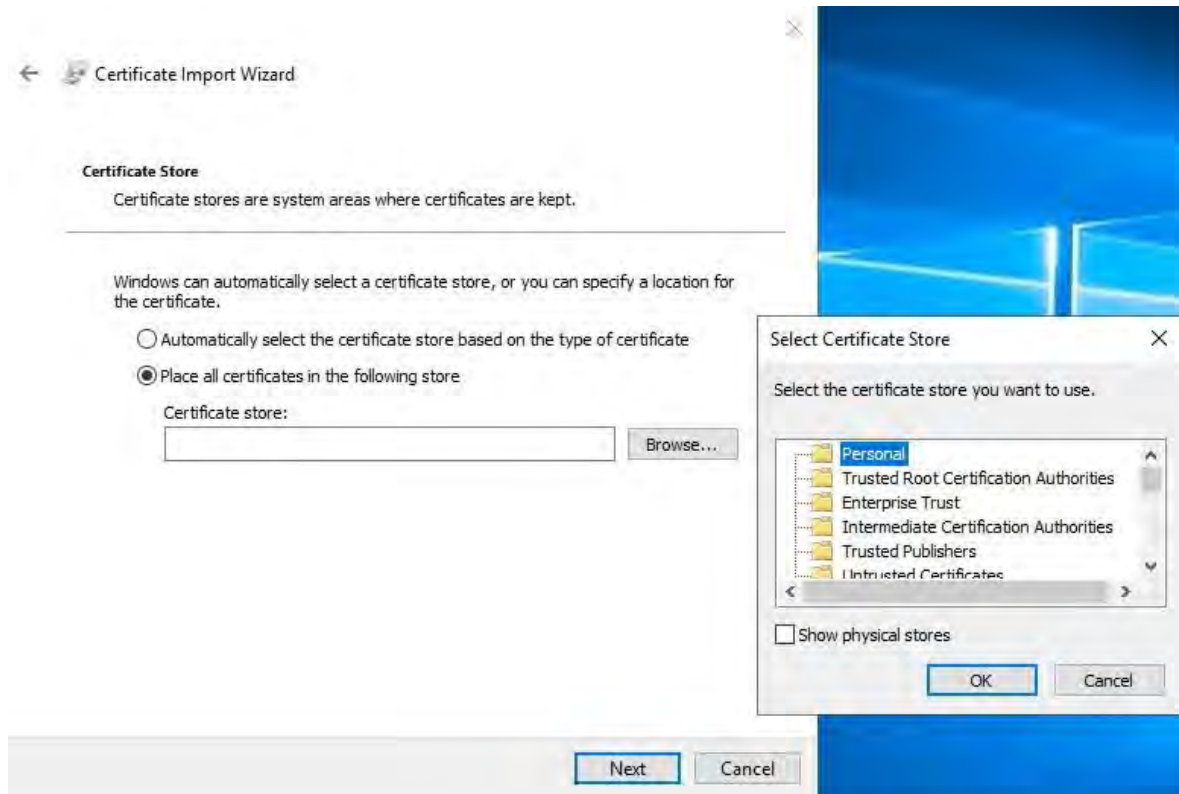
8. Accetta l'avviso di sicurezza, se visualizzato.

Selezionare questa opzione per installare il certificato per l'utente corrente e fare clic su **Avanti**.



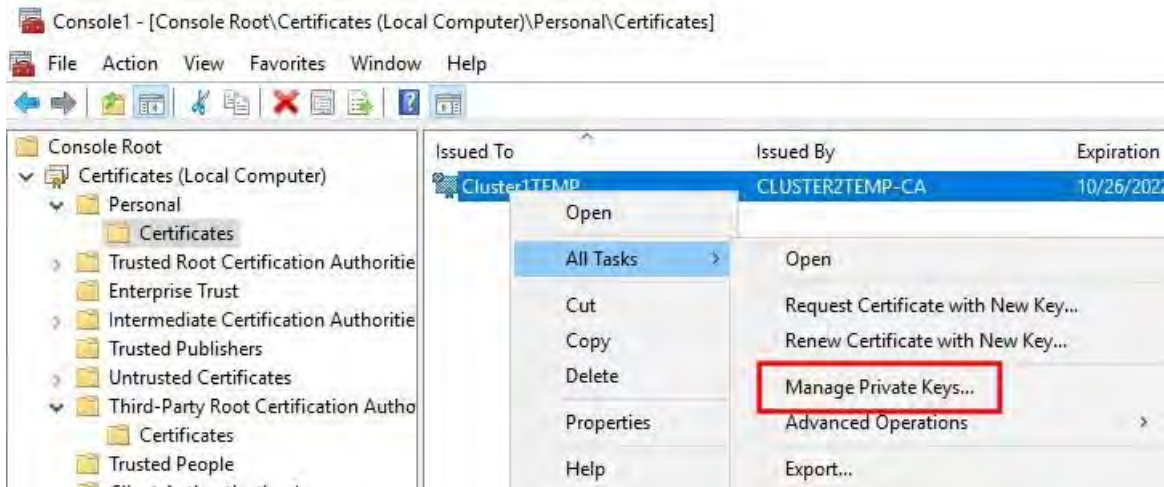
- Scegli una posizione del negozio. Selezionare Posizione **tutti i certificati nell'archivio seguente** e fare clic sul pulsante **Sfoglia** per aprire la finestra **Selezione archivio certificati**. Passare all'archivio **certificati personali** e fare clic su **OK**.

Fare clic su **Avanti**.



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

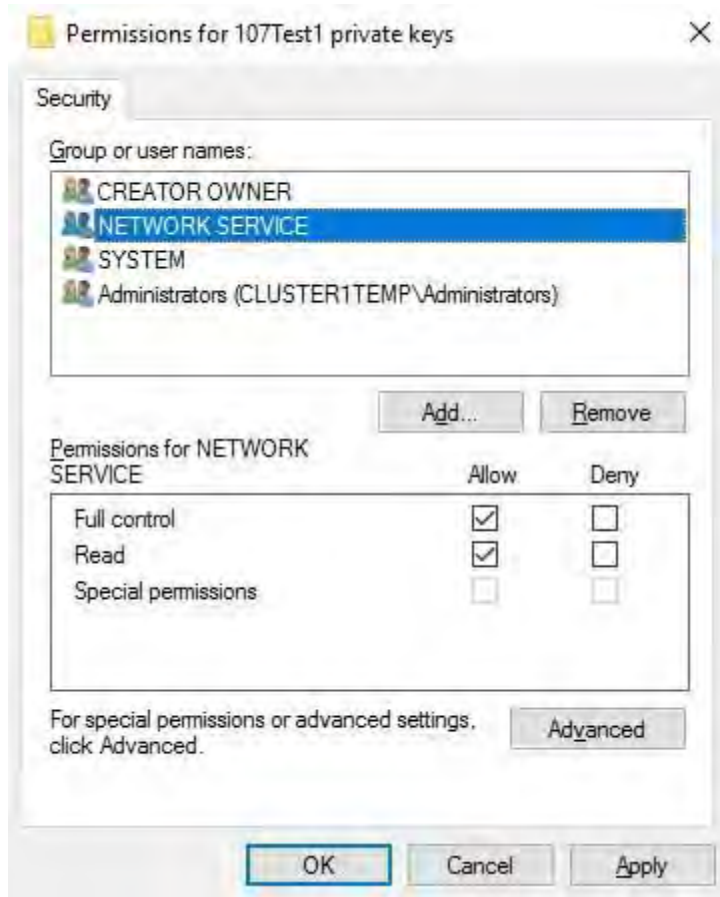
12. Nella console passare all'archivio personale in cui è installato il certificato. Fare clic con il pulsante destro del mouse sul certificato e selezionare **Tutte le attività > Gestisci chiavi private**.



13. 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.

Assicuratevi 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.



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

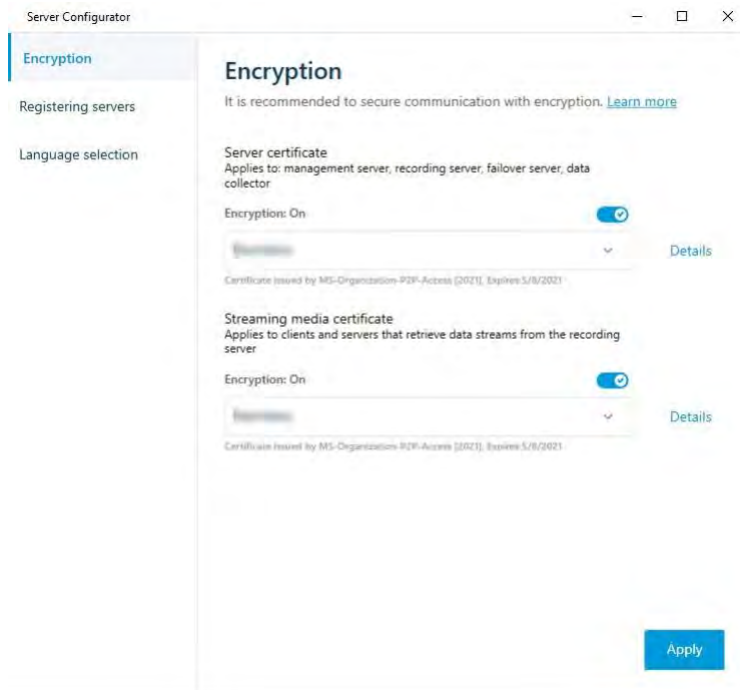
Una volta installato il certificato con le proprietà e le autorizzazioni corrette, eseguire le operazioni seguenti.

1. Su un computer in cui è installato un server di gestione o un server di registrazione, aprire il **configuratore del server**
 Da:
 - Il menu Start di Windows
 - o
 - 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.

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.



5. 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 registrazione.

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.



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](#)

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.

Prerequisiti:

- Un certificato di autenticazione server è considerato attendibile nel computer che ospita il

server eventi Innanzitutto, abilitare la crittografia nel server eventi.

Passi:

1. Su un computer in cui è installato un server di eventi, aprire il **configuratore del server** da:
 - Il menu Start di Windows
 - o
 - Il server di eventi facendo clic con il pulsante destro del mouse sull'icona del server di eventi sulla barra delle applicazioni del computer
2. In **Server Configurator**, in **Server eventi e componenti aggiuntivi**, attivare **Crittografia**.
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 eventi e i componenti aggiuntivi correlati.

Selezionare **Dettagli** per visualizzare le informazioni dell'archivio certificati di Windows sul certificato selezionato.



5. 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.

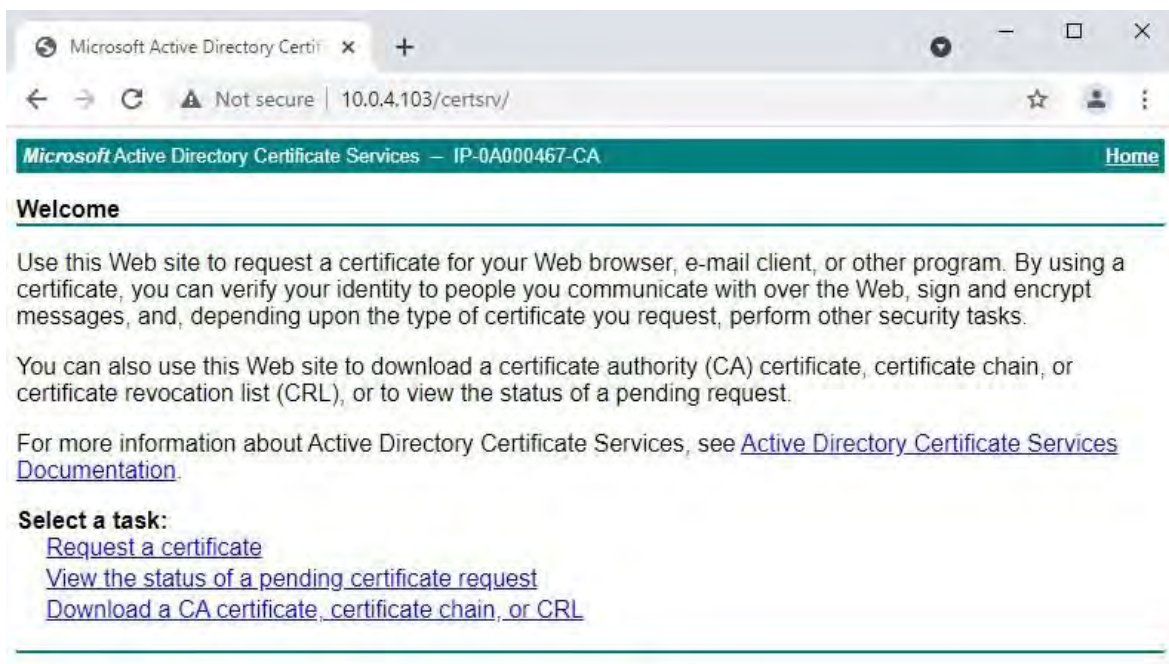
Importare i certificati client

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/>

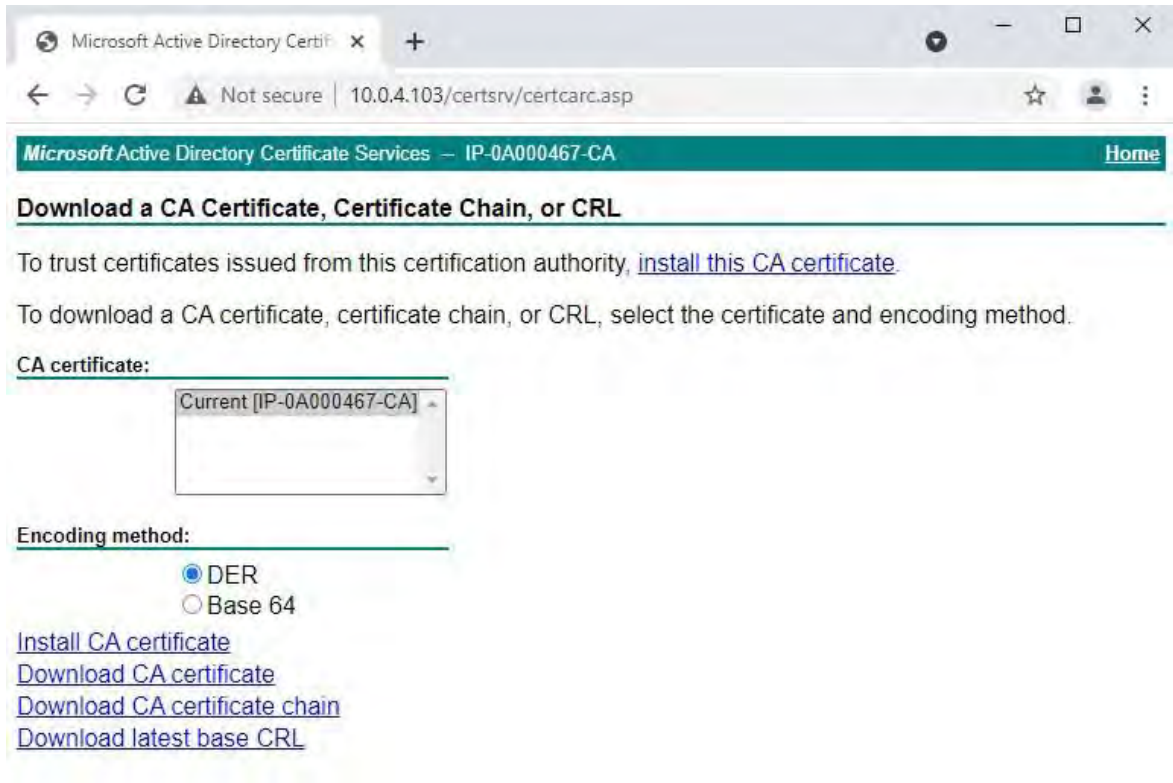
Tuttavia, l'indirizzo del server che detiene il certificato (chiave privata) prenderà il posto di "localhost". Per esempio:



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

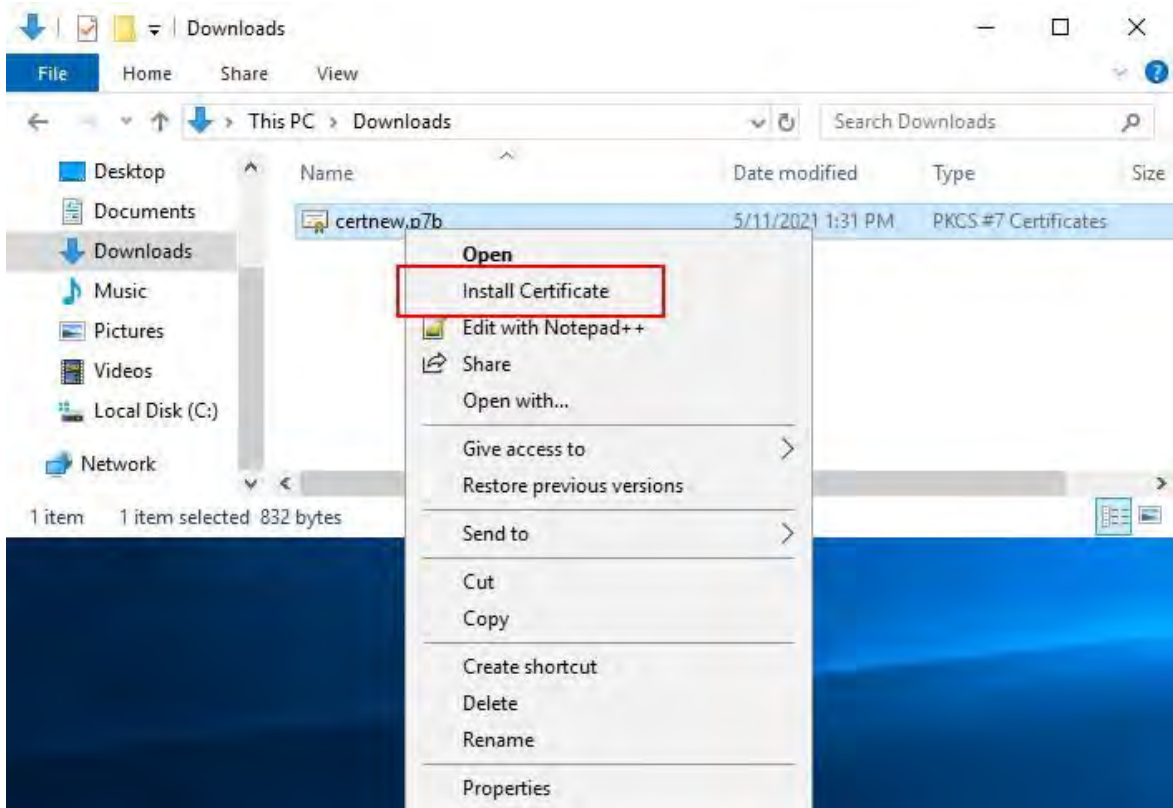
2. Fare clic su **Scarica un certificato CA, una catena di certificati o un CRL.**

3. Nel campo **Certificato CA**, selezionare il certificato CA da utilizzare con il sistema MOBOTIX HUB e fare clic su **Scarica la catena di certificati CA**.



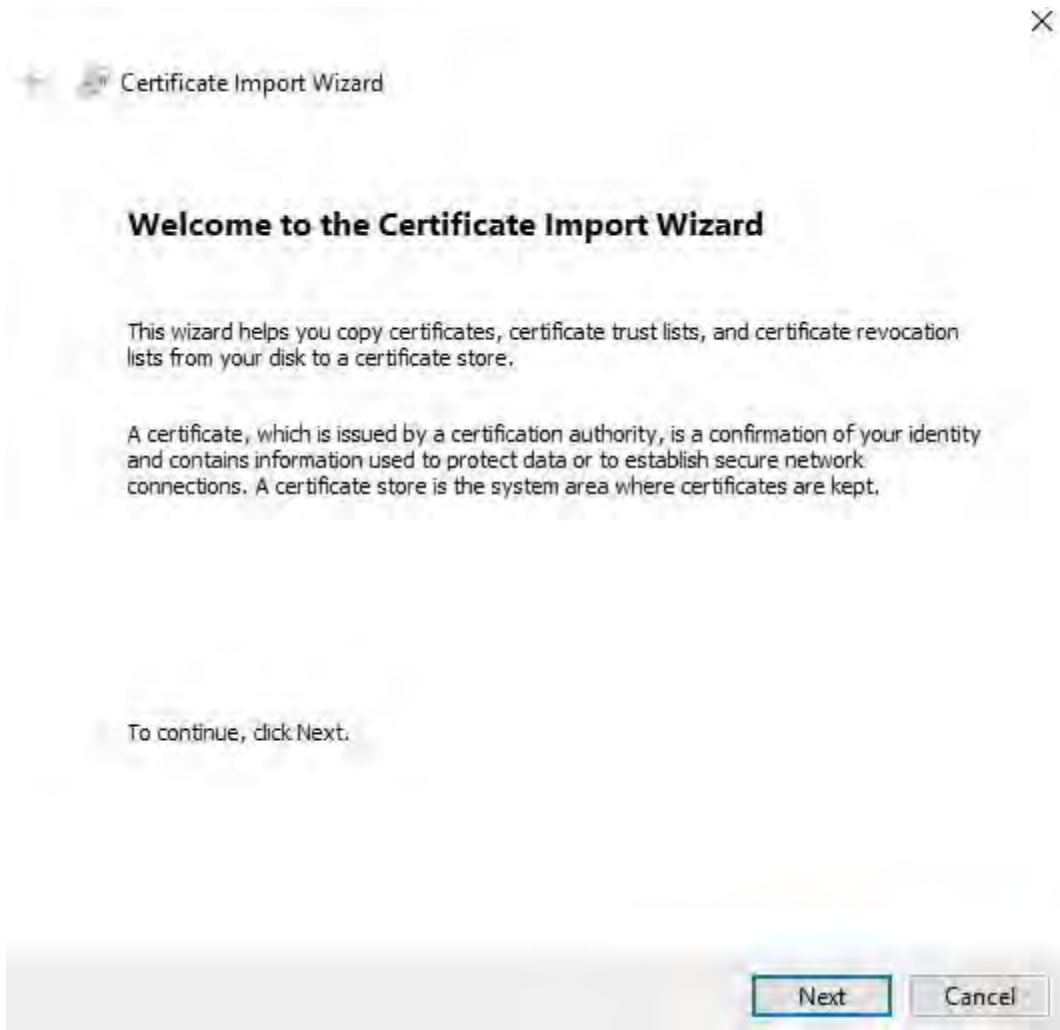
4. Selezionare **Codifica DER** e scaricare la catena di certificati.

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.

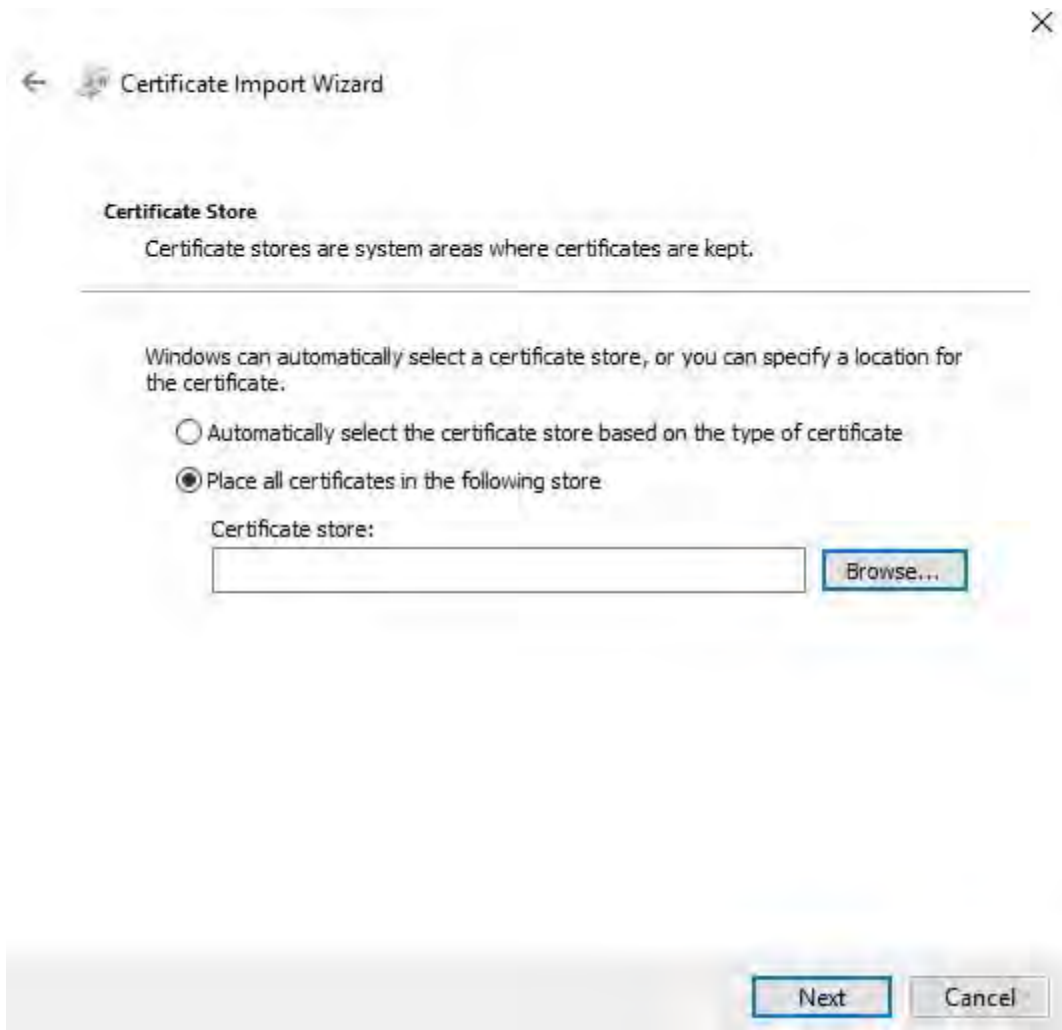


6. Viene avviata l' **Importazione guidata certificati**.

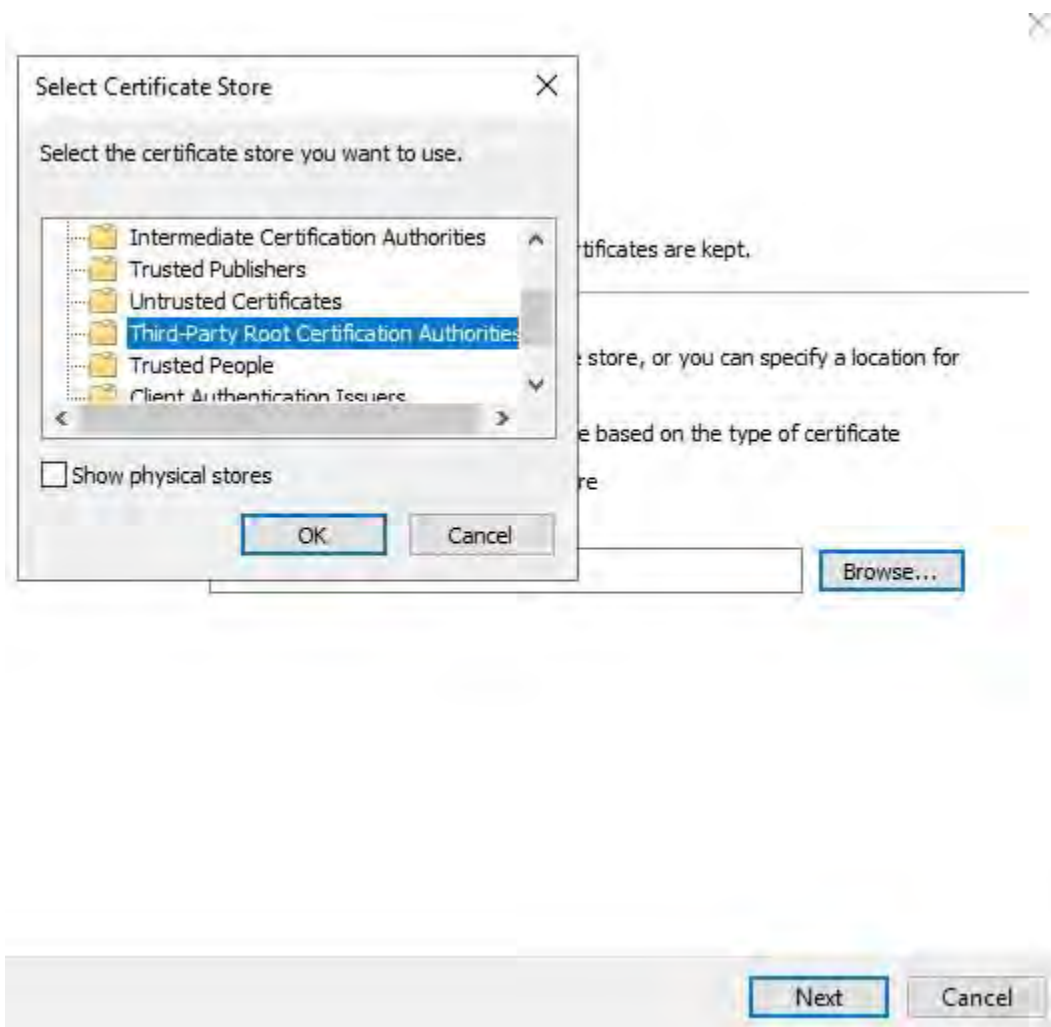
Fare clic su **Avanti**.



7. Scegli una posizione del negozio. Selezionare Posizione **tutti i certificati nell'archivio seguente** e fare clic sul pulsante **Sfoglia** per aprire la finestra **Seleziona archivio certificati**.



8. Passare all' archivio certificati delle **autorità di certificazione radice di terze parti** e fare clic su **OK**. Fare clic su **Avanti**.



9. 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.

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.



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.



The image shows a 'Properties' dialog box for a failover server. The title bar reads 'Properties'. The main content area is titled 'Failover server information' and contains the following fields:

- Name:** Failover recording server 1
- Description:** Failover for Recording server 1
- Host name:** [redacted].local
- Local web server address:** https://[redacted].local:7563/
- Web server address:** https://www.failoverrecordingserver1:89/
- UDP port:** 8844
- Database location:** C:\MediaDatabase

At the bottom of the dialog, there is a checkbox labeled 'Enable this failover server' which is checked. Below the checkbox are three icons: 'Info', 'Network', and 'Multicast'.

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)

```
$ca_certificate = New-SelfSignedCertificate -CertStoreLocation cert:\CurrentUser\My -DnsName 'Autorità di certificazione VMS' -KeyusageProperty All '
    -KeyUsage CertSign, CRLSign, DigitalSignature -FriendlyName 'Certificato CA VMS' '
    -TextExtension @"(2.5.29.19={critico}{testo}ca=VERO)"
```

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"
```

```

# 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

```

```

# 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'

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

# 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

```

MOBOTIX

BeyondHumanVision

IT_02/25

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 2023