



## **MOBOTIX HUB – Guía de certificados**

V2.03

## Contenido

<b>Derechos de autor, marcas comerciales y exención de responsabilidad</b>	<b>3</b>
<b>Acerca de esta guía</b>	<b>4</b>
<b>Introducción a los certificados</b>	<b>5</b>
<b>Información general sobre los escenarios y procedimientos utilizados con los certificados</b>	<b>8</b>
¿Qué clientes necesitan certificados?	11
<b>Configurador de servidores (explicado)</b>	<b>13</b>
<b>Scripts de PowerShell</b>	<b>16</b>
<b>Creación y distribución manual de certificados</b>	<b>17</b>
Creación de un certificado de CA	17
Instalar certificados en los clientes	19
Crear certificado SSL	27
Importar certificado SSL	29
<b>Creación de un certificado SSL para el servidor de administración de conmutación por error</b>	<b>38</b>
<b>Instalar certificados para la comunicación con el servidor móvil</b>	<b>40</b>
<b>Instale certificados de CA comerciales o de terceros para la comunicación con el servidor de administración, o Servidor de grabación</b>	<b>57</b>
<b>Instalación de Servicios de certificados de Active Directory</b>	<b>74</b>
<b>Instalación de certificados en un dominio para la comunicación con el servidor de gestión o el servidor de grabación</b>	<b>86</b>
<b>Instalación de certificados en un entorno de grupo de trabajo para la comunicación con el servidor de gestión o Servidor de Grabación</b>	<b>104</b>
<b>Instalar certificados para la comunicación con el servidor de eventos</b>	<b>126</b>
<b>Importar certificados de cliente</b>	<b>129</b>
<b>Ver el estado de cifrado de los clientes</b>	<b>135</b>
<b>Visualización del estado de cifrado en un servidor de grabación de conmutación por error</b>	<b>136</b>
<b>Apéndice A: Creación de un script de certificado de CA</b>	<b>137</b>
<b>Apéndice B: Crear script de certificado SSL de servidor</b>	<b>138</b>
<b>Apéndice C Creación de un script de certificado de servidor de administración de conmutación por error</b>	<b>139</b>

# Derechos de autor, marcas comerciales y exención de responsabilidad

Derechos de autor © 2023 MOBOTIX AG

## **Marcas**

MOBOTIX HUB es una marca registrada de MOBOTIX AG.

Microsoft y Windows son marcas comerciales registradas de Microsoft Corporation. App Store es una marca de servicio de Apple Inc. Android es una marca comercial de Google Inc.

Todas las demás marcas comerciales mencionadas en este documento son marcas comerciales de sus respectivos propietarios.

## **Renuncia**

Este texto está destinado únicamente a fines de información general y se ha tenido el debido cuidado en su preparación.

Cualquier riesgo que surja del uso de esta información recae en el destinatario, y nada de lo aquí contenido debe interpretarse como constitutivo de ningún tipo de garantía.

MOBOTIX AG se reserva el derecho de realizar ajustes sin previo aviso.

Todos los nombres de personas y organizaciones utilizados en los ejemplos de este texto son ficticios. Cualquier parecido con cualquier organización o persona real, viva o muerta, es pura coincidencia y no intencionada.

Este producto puede hacer uso de software de terceros para el que se pueden aplicar términos y condiciones específicos. Cuando ese sea el caso, puede encontrar más información en el `3rd_party_software_terms_and_conditions.txt` de archivos que se encuentra en la carpeta de instalación del sistema MOBOTIX.

## Acerca de esta guía

Esta guía ofrece una introducción al cifrado y los certificados, junto con procedimientos paso a paso sobre cómo instalar certificados en un entorno de Windows Workgroup.

MOBOTIX recomienda establecer una infraestructura de clave pública (PKI) para crear y distribuir certificados. Una PKI es un conjunto de roles, políticas, hardware, software y procedimientos necesarios para crear, administrar, distribuir, usar, almacenar y revocar certificados digitales y administrar el cifrado de clave pública. En un dominio de Windows, se recomienda establecer una PKI mediante los Servicios de certificados de Active Directory (AD CS).



Si no puede crear una PKI, ya sea porque hay diferentes dominios sin confianza entre ellos o porque no se usan dominios en absoluto, es posible crear y distribuir certificados manualmente.

**ADVERTENCIA:** No se recomienda crear y distribuir certificados manualmente como una forma segura de distribuir certificados. Si elige la distribución manual, es responsable de mantener siempre seguros los certificados privados. Cuando se mantienen seguros los certificados privados, los equipos cliente que confían en los certificados son menos vulnerables a los ataques.

### ¿Cuándo es necesario instalar los certificados?

Primero, decida si su sistema necesita comunicación cifrada.

No utilices certificados con cifrado de servidor de grabación si utilizas una o varias integraciones que no admiten la comunicación HTTPS. Se trata, por ejemplo, de integraciones de SDK de MIP de terceros que no son compatibles con HTTPS.

A menos que la instalación se realice en una red físicamente aislada, se recomienda proteger la comunicación mediante certificados.

En este documento se describe cuándo utilizar los certificados:

- Si su sistema VMS HUB de MOBOTIX está configurado en un entorno de grupo de trabajo de Windows
- Antes de instalar o actualizar a MOBOTIX HUB VMS 2019 R1 o posterior, si desea habilitar el cifrado durante la instalación.
- Antes de activar el cifrado, si ha instalado MOBOTIX HUB VMS 2019 R1 o una versión posterior sin cifrado
- Al renovar o reemplazar certificados debido a la caducidad

## Introducción a los certificados

El Protocolo de Transferencia de Hipertexto Seguro (HTTPS) es una extensión del Protocolo de Transferencia de Hipertexto (HTTP) para la comunicación segura a través de una red informática. En HTTPS, el protocolo de comunicación se cifra mediante Transport Layer Security (TLS) o su predecesor, Secure Sockets Layer (SSL).

En MOBOTIX HUB VMS, la comunicación segura se obtiene mediante el uso de TLS/SSL con cifrado asimétrico (RSA). TLS/SSL utiliza un par de claves, una privada y otra pública, para autenticar, proteger y administrar conexiones seguras.

Una autoridad de certificación (CA) es cualquier persona que pueda emitir certificados raíz. Puede ser un servicio de Internet que emite certificados raíz o cualquier persona que genere y distribuya un certificado manualmente. Una CA puede emitir certificados a los servicios web, es decir, a cualquier software que utilice la comunicación https. Este certificado contiene dos claves, una clave privada y una clave pública. La clave pública se instala en los clientes de un servicio web (clientes de servicio) mediante la instalación de un certificado público. La clave privada se utiliza para firmar certificados de servidor que deben instalarse en el servidor.

Cada vez que un cliente de servicio llama al servicio web, el servicio web envía el certificado del servidor, incluida la clave pública, al cliente. El cliente de servicio puede validar el certificado de servidor mediante el certificado de CA pública ya instalado. El cliente y el servidor ahora pueden usar los certificados de servidor público y privado para intercambiar una clave secreta y, por lo tanto, establecer una conexión TLS/SSL segura.

En el caso de los certificados distribuidos manualmente, los certificados deben instalarse antes de que el cliente pueda realizar dicha comprobación.

Consulte [Seguridad de la capa de transporte](#) para obtener más información sobre TLS.

En MOBOTIX HUB VMS, se pueden habilitar las siguientes ubicaciones en las que se puede activar el cifrado TLS/SSL:

- En la comunicación entre el servidor de administración y los servidores de grabación, servidores de eventos y servidores móviles
- En el servidor de grabación en la comunicación con clientes, servidores e integraciones que recuperan flujos de datos del servidor de grabación.
- En la comunicación entre los clientes y el servidor móvil En esta

guía, se hace referencia a los siguientes como clientes:

- Cliente de escritorio MOBOTIX HUB
- Cliente de gestión
- Servidor de administración (para el Monitor del sistema y para imágenes y clips de vídeo AVI en notificaciones por correo electrónico)
- Servidor móvil MOBOTIX HUB
- Servidor de eventos MOBOTIX HUB
- BUJE MOBOTIX LPR
- Puente de red abierto de MOBOTIX

- Servidor DLNA HUB de MOBOTIX
- Sitios que recuperan flujos de datos del servidor de grabación a través de Milestone Interconnect
- Integraciones de SDK de MIP de terceros compatibles con HTTPS

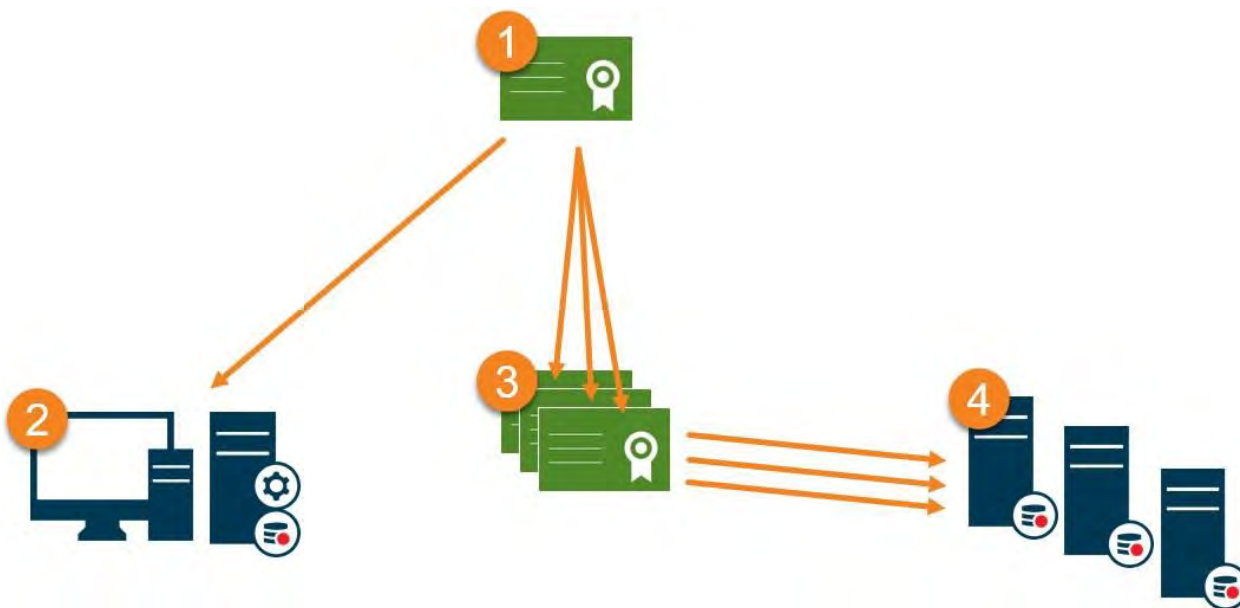
En el caso de las soluciones creadas con el SDK de MIP 2018 R3 o versiones



- Si las integraciones se realizan mediante bibliotecas del SDK de MIP, deben reconstruirse con
- Si las integraciones se comunican directamente con las API del servidor de grabación sin
- En caso de duda, pregunte a su proveedor quién

### Distribución de certificados

El gráfico ilustra el concepto básico de cómo se firman, confían y distribuyen los certificados en MOBOTIX HUB VMS.



- 1** Una autoridad de certificación (CA) es cualquier persona que pueda emitir certificados raíz. Un certificado de CA actúa como un tercero de confianza, en el que confían tanto el sujeto/propietario (servidor) como la parte que verifica el certificado (clientes) (consulte [Crear certificado de CA en la página 17](#)).
- 2** El certificado público debe ser de confianza en todos los equipos cliente. De esta manera, los clientes pueden verificar la validez de los certificados emitidos por la CA (consulte [Instalar certificados en los clientes en la página 19](#)).
- 3** El certificado de CA se utiliza para emitir certificados de autenticación de servidor privado a los servidores (consulte [Crear certificado SSL en la página 27](#)).

4 Los certificados SSL privados creados deben importarse al almacén de certificados de Windows en todos los servidores (consulte [Importar certificado SSL en la página 29](#)).

Requisitos para el certificado SSL privado:

- Se emite al servidor para que el nombre de host del servidor se incluya en el certificado, ya sea como sujeto (propietario) o en la lista de nombres DNS a los que se emite el certificado
- De confianza en todos los equipos que ejecutan servicios o aplicaciones que se comunican con el servicio en los servidores, mediante la confianza en el certificado de CA que se usó para emitir el certificado SSL
- La cuenta de servicio que ejecuta el servidor debe tener acceso a la clave privada del certificado en el servidor.



Los certificados tienen una fecha de caducidad. No recibirá una advertencia cuando un certificado esté a punto de caducar. Si un certificado caduca, los clientes ya no confiarán en el servidor con el certificado caducado y, por lo tanto, no podrán comunicarse con él.

Para renovar los certificados, siga los pasos de esta guía como lo hizo al crear certificados .

## Información general sobre los escenarios y procedimientos utilizados con los certificados

Los procedimientos para configurar la comunicación segura en un entorno MOBOTIX HUB VMS son diferentes en función del tipo de servidores que requieran una comunicación segura.

Los procedimientos también son diferentes en una red WORKGROUP en comparación con una red DOMAIN.

Los tipos de aplicaciones cliente MOBOTIX HUB VMS que se utilizan en el sistema también determinan algunos de los procedimientos necesarios para las comunicaciones seguras.



Normalmente, el uso de certificados para la comunicación del servidor se puede omitir en una sola instalación de servidor, excepto para servir como protección adicional al comunicarse con el servidor de administración.

Esta lista muestra los diferentes escenarios:

- Servidor móvil MOBOTIX HUB

En MOBOTIX HUB VMS, el cifrado se habilita o deshabilita por servidor móvil. El cifrado se activa o deshabilita durante la instalación del producto MOBOTIX HUB VMS o mediante Server Configurator. Cuando se habilita el cifrado en un servidor móvil, se utiliza la comunicación cifrada con todos los clientes, servicios e integraciones que recuperan flujos de datos.

El servidor móvil se conecta al cliente móvil de MOBOTIX HUB y al cliente web de MOBOTIX HUB. Los navegadores, sistemas operativos y dispositivos móviles que alojan estos clientes mantienen una lista de certificados raíz de CA de confianza. Solo la autoridad conoce su clave privada, pero todos conocen su clave pública, que es similar a cualquier certificado en particular .

Estos clientes, por lo tanto, ya tienen claves de certificado instaladas y funcionan con la mayoría de los certificados de terceros que están disponibles para instalar en el propio servidor móvil.

Dado que cada CA de terceros tiene sus propios requisitos para solicitar un certificado, es mejor investigar los requisitos individuales directamente con la CA.

Este documento describe cómo crear una solicitud de certificado en el servidor móvil e instalar el certificado una vez que se ha emitido desde la CA.

Ver:

[Instale los certificados para la comunicación con el servidor móvil en la página 40](#)



- Servidor de gestión y servidor de grabación de MOBOTIX HUB

Puede cifrar la conexión bidireccional entre el servidor de administración y el servidor de grabación. Cuando se habilita el cifrado en el servidor de administración, se aplica a las conexiones de todos los servidores de grabación que se conectan al servidor de administración. Si habilita el cifrado en el servidor de administración, también debe habilitar el cifrado en todos los servidores de grabación. Antes de habilitar el cifrado, debe instalar certificados de seguridad en el servidor de administración y en todos los servidores de grabación, incluidos los servidores de grabación de conmutación por error.

- Certificado de CA comercial o de terceros

El proceso para solicitar certificados de CA de terceros para su uso con servidores de administración y servidores de grabación es el mismo que con el servidor móvil. La única diferencia es la configuración con el Configurador de Servidores.

Ver:

[Instale certificados de CA comerciales o de terceros para la comunicación con el servidor de administración o el servidor de grabación en la página 57](#)

- Dominio

Cuando los puntos de conexión de cliente y servidor funcionan dentro de un entorno de dominio con su propia infraestructura de autoridad de certificación, no es necesario distribuir certificados de CA a las estaciones de trabajo cliente. Siempre que tenga una directiva de grupo dentro del dominio, se encargará de la distribución automática de todos los certificados de CA de confianza a todos los usuarios y equipos del dominio.

El proceso para solicitar un certificado e instalar un certificado de servidor es el mismo que en un grupo de trabajo.

Ver:

[Instale certificados en un dominio para la comunicación con el servidor de administración o el servidor de grabación en la página 86](#)

- Grupo de trabajo

Cuando se opera en un entorno de grupo de trabajo, se supone que no hay infraestructura de autoridad de certificación. Para distribuir certificados, es necesario crear una infraestructura de autoridad de certificación. También es necesario distribuir las claves de certificado a las estaciones de trabajo cliente. A excepción de estos requisitos, el proceso de solicitud e instalación de un certificado en un servidor es similar a los escenarios de dominio y de terceros.

Ver:

[Instale certificados en un entorno de grupo de trabajo para la comunicación con el servidor de gestión o el servidor de grabación en la página 104](#)

- Servidor de eventos MOBOTIX HUB

Puede cifrar la conexión bidireccional entre el servidor de eventos y los componentes que se comunican con el servidor de eventos, incluido el servidor LPR. Cuando se habilita el cifrado en el servidor de eventos, se aplica a las conexiones de todos los componentes que se conectan al servidor de eventos. Antes de habilitar el cifrado, debe instalar certificados de seguridad en el servidor de eventos y en todos los componentes de conexión.

Ver:

[Instale certificados para la comunicación con el servidor de eventos en la página 126](#)

- Cliente

En los escenarios de Terceros/Comercial y Dominio, los clientes no necesitan tener instaladas claves de certificado. Solo necesita instalar claves de certificado de cliente en un entorno de grupo de trabajo.

Cuando se habilita el cifrado en un servidor de grabación, se cifra la comunicación con todos los clientes, servidores e integraciones que recuperan flujos de datos del servidor de grabación.

En este documento se hace referencia a ellos como "clientes" para el Servidor de Registro:

- Cliente de escritorio MOBOTIX HUB
- Cliente de gestión
- Servidor de administración (para el Monitor del sistema y para imágenes y clips de vídeo AVI en notificaciones por correo electrónico )
- Servidor móvil MOBOTIX HUB
- Servidor de eventos MOBOTIX HUB
- BUJE MOBOTIX LPR
- Puente de red MOBOTIX
- Servidor DLNA HUB de MOBOTIX
- Sitios que recuperan flujos de datos del servidor de grabación a través de MOBOTIX Interconnect
- Algunas integraciones de SDK de MIP de terceros



En el caso de las soluciones creadas con MIP SDK 2018 R3 o versiones anteriores que acceden a servidores de grabación: si las integraciones se realizan con bibliotecas del SDK de MIP, deben reconstruirse con MIP SDK 2019 R1; si las integraciones se comunican directamente con las API del servidor de grabación sin utilizar las bibliotecas del SDK de MIP, los integradores deben aadear compatibilidad con HTTPS ellos mismos.

Ver:

[¿Qué clientes necesitan certificados? en la página 11](#)

[Importar certificados de cliente en la página 129](#)



## ¿Qué clientes necesitan certificados?

¿Qué clientes necesitan certificados instalados? ¿Cómo planificamos esto? ¿Qué podemos hacer para prepararnos?

Los clientes basados en navegador web y los clientes que se distribuyen a través de un servicio o almacén público de distribución de aplicaciones de terceros, por ejemplo, Google Play o Apple AppStore, no deben requerir la instalación de un certificado. MOBOTIX HUB Mobile no utilizará certificados instalados. MOBOTIX HUB Mobile solo puede utilizar certificados de terceros de confianza.

Si los servidores MOBOTIX HUB (Servidor de Gestión y Servidor de Grabación) están instalados en ordenadores que están unidos al Dominio, y los usuarios que inician sesión en el Desk Client son todos usuarios del Dominio, el Dominio se encargará de toda la distribución de clave pública y la autenticación necesarias para establecer comunicaciones seguras.



-  No Public Key Distribution Needed
-  Public Key Distribution Needed

Solo en un escenario en el que los Servicios de certificados de Active Directory (AD CS) se usan para crear certificados autofirmados y los recursos (usuarios y equipos) funcionan en un entorno que no es de dominio, sería necesario distribuir claves públicas a las estaciones de trabajo cliente.

Consulte también [Instalar certificados en los clientes en la página 19](#) e [Importar certificados de cliente en la página 129](#).

## Configurador de servidores (explicado)

Utilice el Configurador de servidores para seleccionar certificados en servidores locales para la comunicación cifrada y registrar servicios de servidor para que estén cualificados para comunicarse con los servidores.

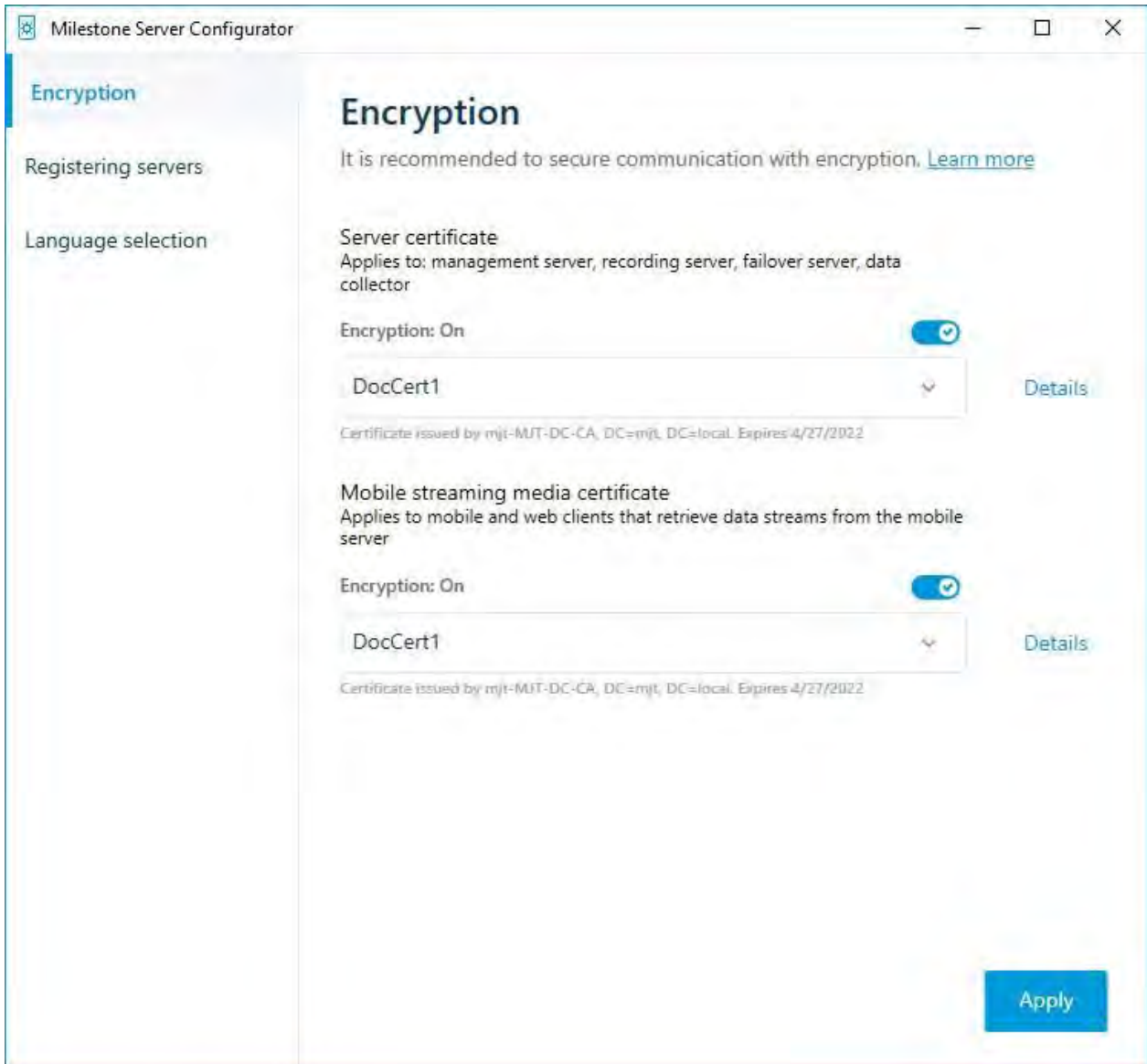
Los siguientes tipos de servidores en MOBOTIX HUB VMS necesitan certificados para una comunicación segura:

- Servidores de administración
- Servidores de grabación
- Servidores de eventos
- Servidores Móviles

Estos servidores trabajan con el Configurador de servidores para gestionar comunicaciones seguras. Utilice el configurador de servidores para determinar si los servidores MOBOTIX HUB utilizan o no comunicaciones cifradas seguras y para gestionar los certificados que utilizan los servidores MOBOTIX HUB.

El configurador de servidores se instala de forma predeterminada en cualquier ordenador que aloje un servidor MOBOTIX HUB. Abra el Configurador de servidores desde:

- El menú Inicio de Windows
- o
- El gestor de servidores MOBOTIX HUB haciendo clic con el botón derecho del ratón en el icono del gestor de servidores en la barra de tareas del ordenador y seleccionando Server Configurator



Utilice el configurador de servidores para elegir los certificados que utilizan los servidores MOBOTIX HUB para proteger las comunicaciones con sus aplicaciones cliente y para verificar que los ajustes de cifrado están configurados correctamente.

En la **sección Cifrado** del Configurador de servidores, establezca el cifrado de los siguientes tipos:

- **Certificado de servidor**

Seleccione el certificado que se utilizará para cifrar la conexión bidireccional entre el servidor de administración y los siguientes servidores:

- Servidor de grabación
- Servidor de eventos
- Servidor de registro
- Servidor LPR
- Servidor móvil

- **Servidor de eventos y complementos**

Seleccione el certificado que se usará para cifrar la conexión bidireccional entre el servidor de eventos y los componentes que se comunican con el servidor de eventos, incluido el servidor LPR.

- **Certificado de transmisión de medios**

Seleccione el certificado que se utilizará para cifrar la comunicación entre los servidores de grabación y todos los clientes, servidores e integraciones que recuperan flujos de datos de los servidores de grabación.

- **Certificado de medios de transmisión móvil**

Seleccione el certificado que se utilizará para cifrar la comunicación entre el servidor móvil y los clientes móviles y web que recuperan flujos de datos del servidor móvil.

En la sección **Registro de servidores** del Configurador de servidores, registre los servidores que se están ejecutando en el equipo con el servidor de administración designado.

Para registrar los servidores, compruebe la dirección del servidor de administración y seleccione **Registrar**.

## Scripts de PowerShell

Puede utilizar PowerShell y el módulo PSTools de Milestone para instalar, integrar, simplificar, supervisar y automatizar el mantenimiento continuo y los procesos de configuración necesarios de sistemas MOBOTIX HUB VMS grandes, complejos y técnicamente avanzados.

No obstante, MOBOTIX recomienda que los administradores, instaladores y técnicos sepan cómo configurar manualmente el entorno MOBOTIX HUB VMS de sus clientes. Aprenderá con experiencia cuándo usar scripts de PowerShell en lugar de configuraciones manuales. Puede encontrar scripts de PowerShell en estas ubicaciones:

- Proceso/video de PowerShell para [servidor móvil y permite cifrar](#)
- [Repositorio de Github](#) para información, documentación y scripts de PSTools de Milestone.



## Creación y distribución manual de certificados

### Es importante saber:



No se recomienda crear y distribuir certificados manualmente como una forma segura de distribuir certificados. Si elige la distribución manual, es responsable de mantener los certificados privados seguros en todo momento. Cuando se mantienen seguros los certificados privados, los equipos cliente que confían en los certificados son menos vulnerables a los ataques.

En algunas situaciones, Windows Update puede quitar periódicamente certificados que no son de una "entidad de certificación de terceros de confianza".

Para asegurarse de que Windows Update no quite los certificados, debe habilitar la **opción Desactivar la actualización automática de certificados raíz**. Antes de realizar este cambio, debe asegurarse de que el cambio sigue la política de seguridad de su empresa.

1. Habilite esto abriendo el Editor de **políticas de grupo local** en la computadora (haga clic en la barra de inicio de Windows y escriba **gpedit.msc**).
2. En el Editor de **directivas de grupo local** de Windows, vaya a **Configuración del equipo > Plantillas administrativas > Administración de comunicaciones por Internet** del sistema > > **Configuración de comunicaciones por Internet**.
3. Haga doble clic en **Desactivar la actualización automática de certificados raíz** y seleccione **Habilitado**.
4. Haga clic en **Aceptar**.

Tenga en cuenta que esta configuración puede estar controlada por una política de dominio. En cuyo caso, debe estar deshabilitado en ese nivel.

Su certificado ahora permanecerá en el equipo a pesar de que no sea de una "autoridad de certificación de terceros de confianza", ya que Windows Update no se pondrá en contacto con el sitio web de Windows Update para ver si Microsoft ha agregado la CA a su lista de autoridades de confianza.

## Creación de un certificado de CA

En un ordenador con acceso restringido y que no esté conectado a su sistema MOBOTIX HUB, ejecute este script una vez para crear un certificado de CA.



El equipo que use para crear certificados debe ejecutar Windows 10 o Windows Server OS 2016 o posterior.




Tenga en cuenta que cuando crea certificados de esta manera, los certificados están relacionados con el equipo en el que están instalados. Si cambia el nombre del equipo, el VMS no podrá iniciarse hasta que los certificados se vuelvan a crear y se vuelvan a instalar en el equipo.

Este script crea dos certificados:

- Un certificado privado: solo existe en el almacén de certificados personales para el usuario actual después de ejecutar el script . Se recomienda crear una copia de seguridad guardada en un medio (USB) en un lugar seguro, y preferiblemente dos copias de seguridad guardadas en ubicaciones físicamente diferentes. Con la excepción de las copias de seguridad, este certificado nunca debe salir del equipo en el que creó el certificado
- Un certificado público: se importará como certificado de confianza en todos los equipos cliente

1. En el Apéndice A, en la parte posterior de esta guía, encontrará un script para crear el certificado de CA. Copia el contenido.
2. Abra el Bloc de notas y pegue el contenido.



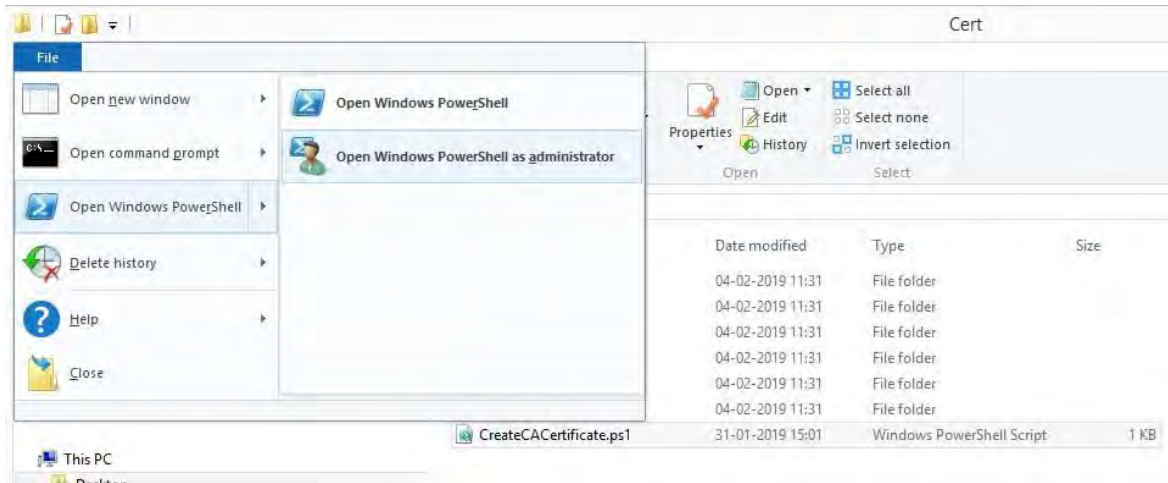
Es muy importante que las líneas se rompan en los mismos lugares que en el Apéndice A. Puede agregar los saltos de línea en el Bloc de notas o, alternativamente, volver a abrir este PDF con Google Chrome, copiar el contenido nuevamente y pegarlo en el Bloc de notas.



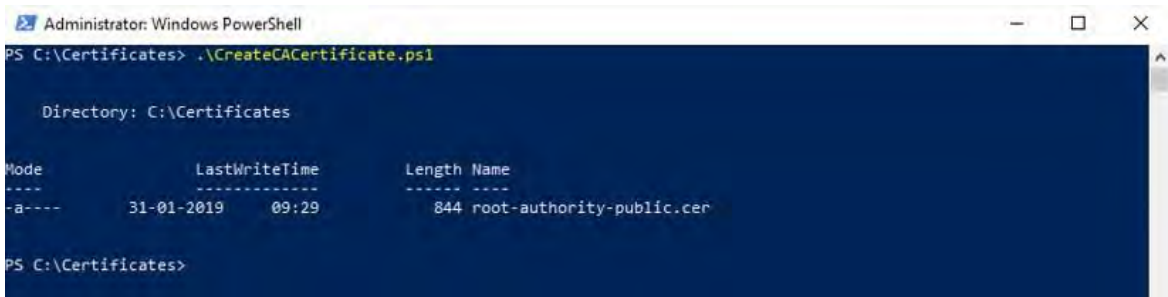
```

# 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"
    
```


3. En el Bloc de notas, haga clic en **Archivo -> Guardar como**, asigne al archivo el nombre **CreateCACertificate.ps1** y guárdelo localmente, así:  
C:\Certificates\CreateCACertificate.ps1.
4. En el Explorador de archivos, vaya a C:\Certificates y seleccione el **archivo CreateCACertificate.ps1**.
5. En el menú **Archivo**, seleccione **Abrir Windows PowerShell** y, a continuación, **Abrir Windows PowerShell como administrador**.



6. En PowerShell, en el símbolo del sistema, escriba `.\CreateCACertificate.ps1` y presione **Entrar**.




7. Compruebe que el **archivo root-authority-public.cer** aparece en la carpeta donde ejecutó el script.

 Es posible que el equipo requiera que cambie la directiva de ejecución de PowerShell. En caso afirmativo, escriba **Set-ExecutionPolicy RemoteSigned**. Pulse **Intro** v seleccione **A**.

## Instalar certificados en los clientes

Después de crear el certificado de CA, confíe en el certificado de CA pública instalándolo en todos los equipos que actúen como clientes del servicio de acuerdo con las descripciones de Introducción [a los certificados en la página 5](#).

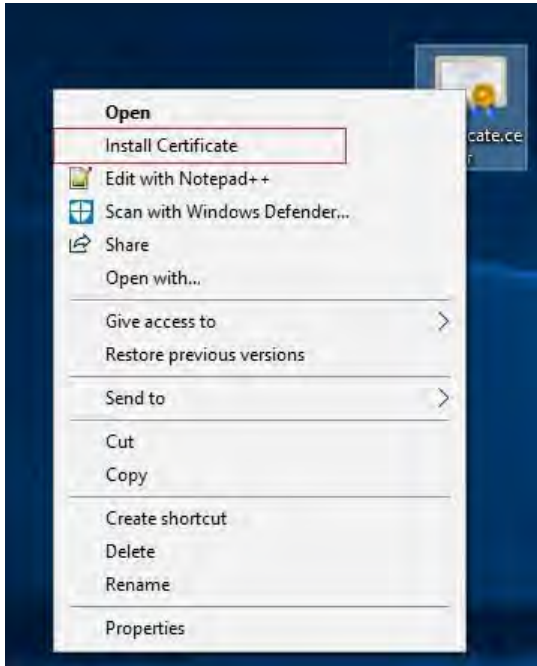
 Consulte [Importar certificados de cliente en la página 129](#) para obtener un procedimiento alternativo a la instalación manual de certificados en los clientes.

1. Copie el archivo root-authority-public.cer del ordenador en el que creó el certificado de CA (C:\Certificates\root-authority-public.cer) en el ordenador en el que está instalado el cliente MOBOTIX HUB.



Para obtener información sobre los servicios de cliente y servidor, y las integraciones que requieren el certificado, consulte [Introducción a los certificados en la página 5](#).

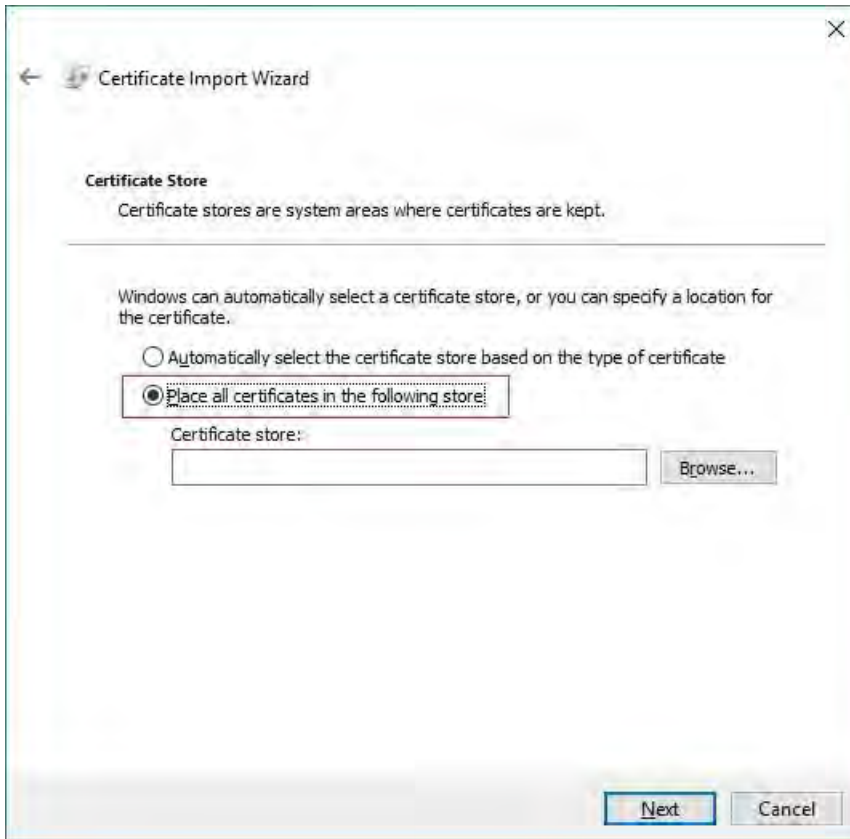
2. Haga clic con el botón derecho en el certificado y seleccione **Instalar certificado**.



3. En el **Asistente para importación** de certificados, seleccione instalar el certificado en el almacén del **equipo local** y haga clic en **Siguiente**.



4. Seleccione esta opción para localizar manualmente el almacén en el que se instalará el certificado.



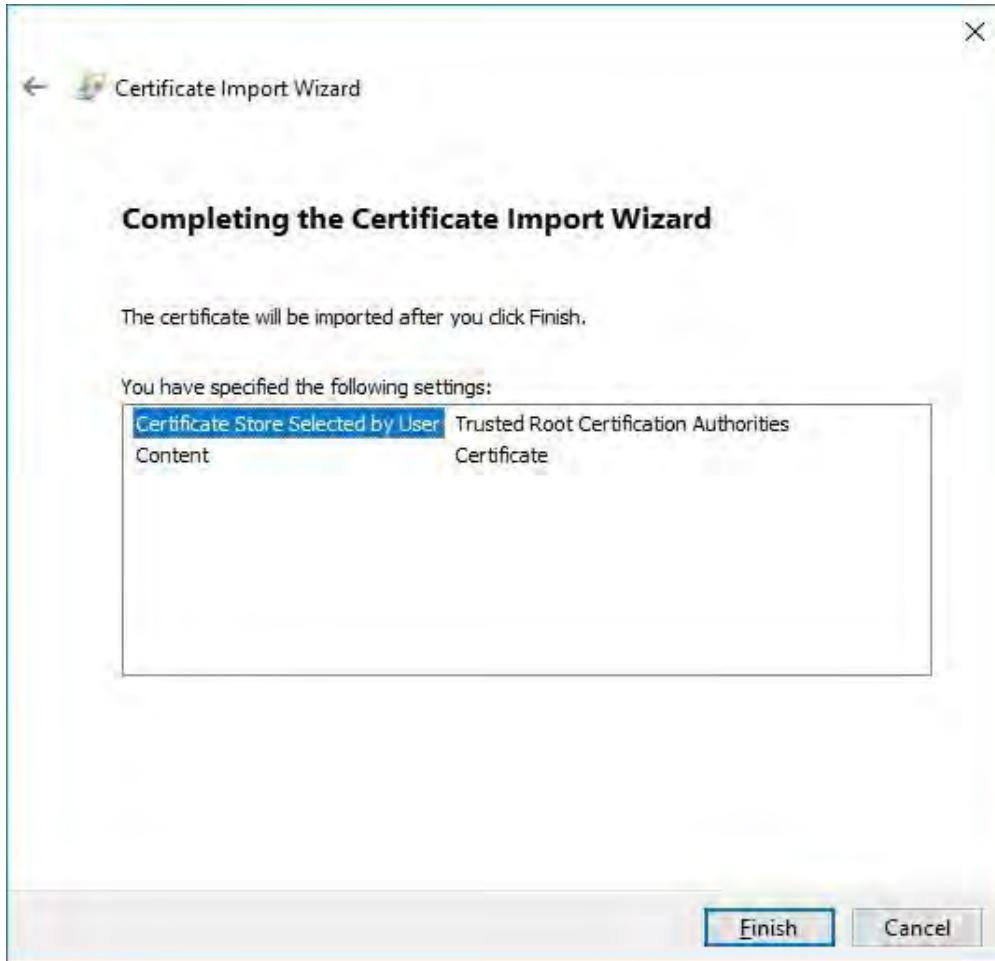
5. Haga clic en **Examinar**, seleccione **Entidades de certificación raíz de confianza** y haga clic en **Aceptar**. A continuación, haga clic en **Siguiente**.



6. En el cuadro de diálogo **Finalización del Asistente para la importación de certificados**, haga clic en **Finalizar**.



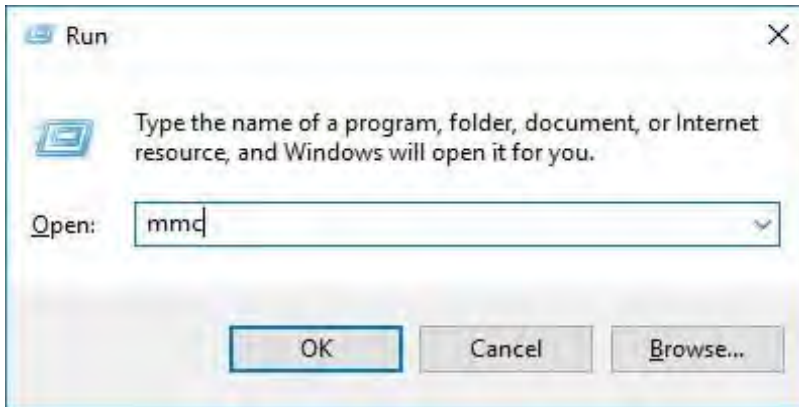
Si recibe una advertencia de seguridad que indica que está a punto de instalar un certificado raíz, haga clic en **Sí** para continuar.



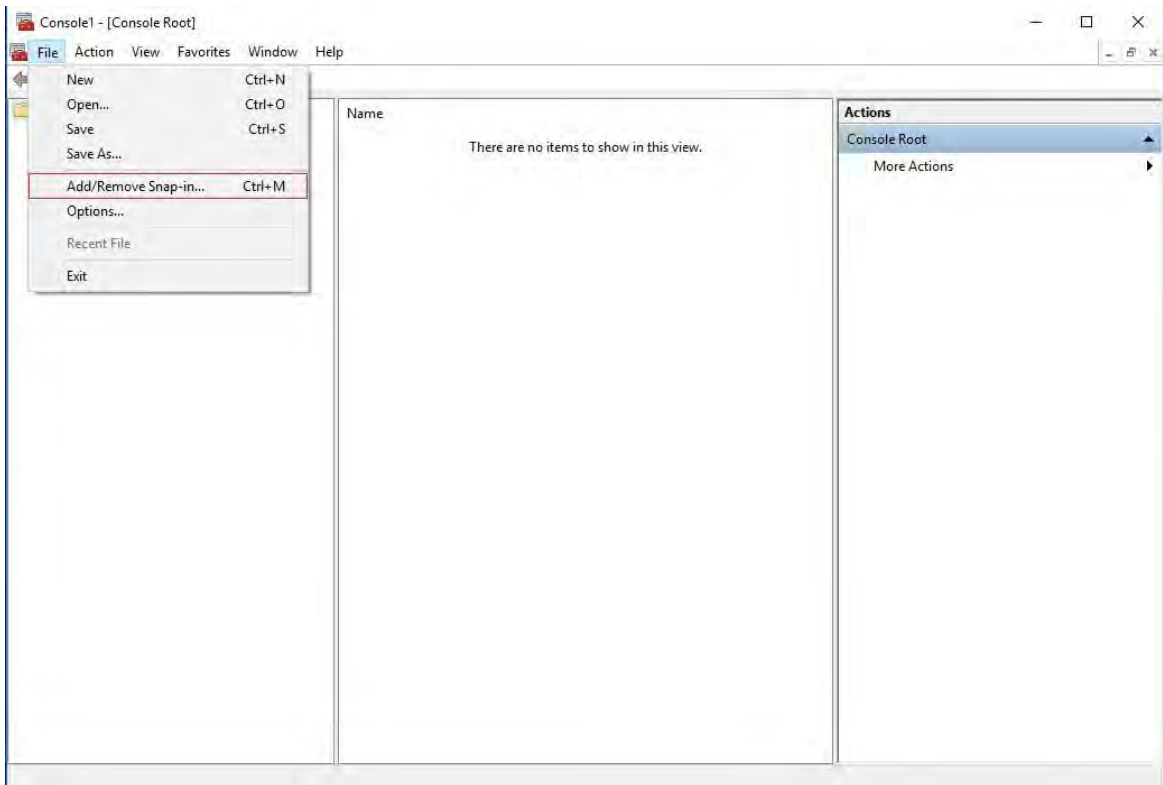
7. Recibirá un cuadro de diálogo de confirmación de que la importación se ha realizado correctamente.



- Para comprobar que el certificado está importado, inicie Microsoft Management Console.

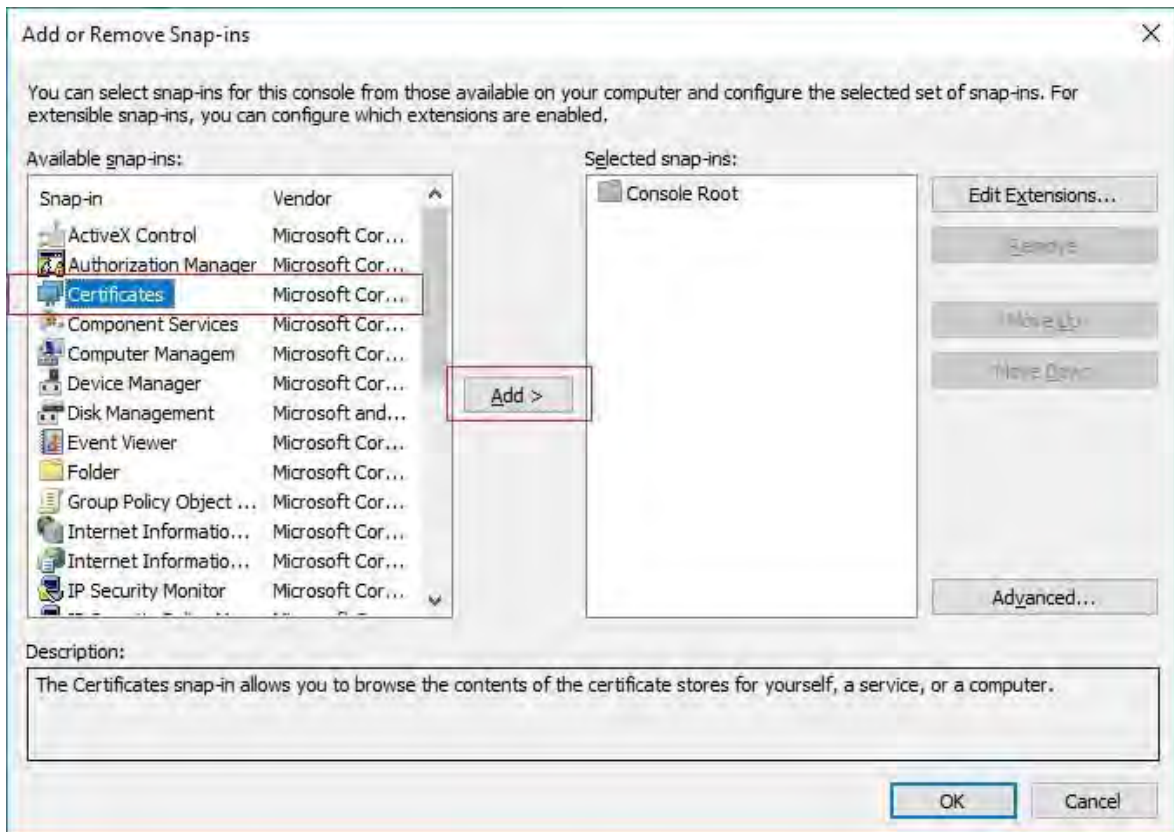


- En Microsoft Management Console, en el menú **Archivo**, seleccione **Agregar o quitar complemento....**

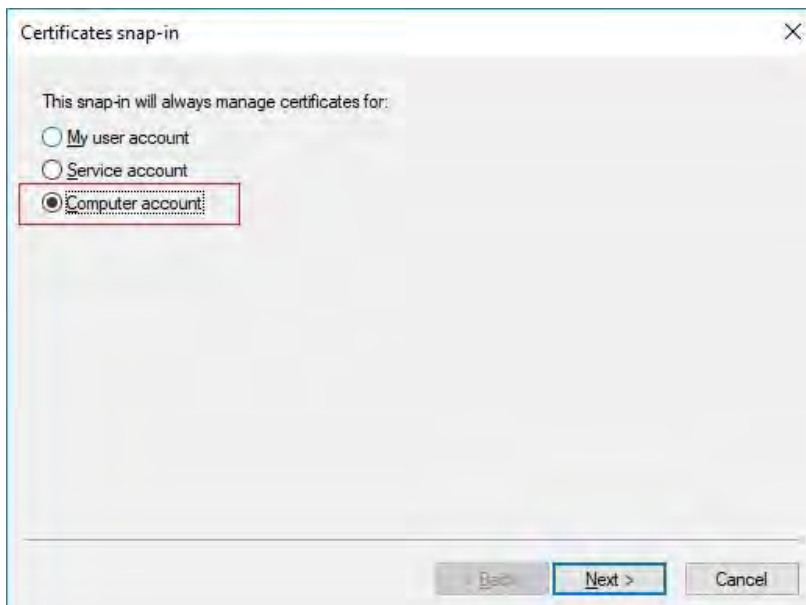




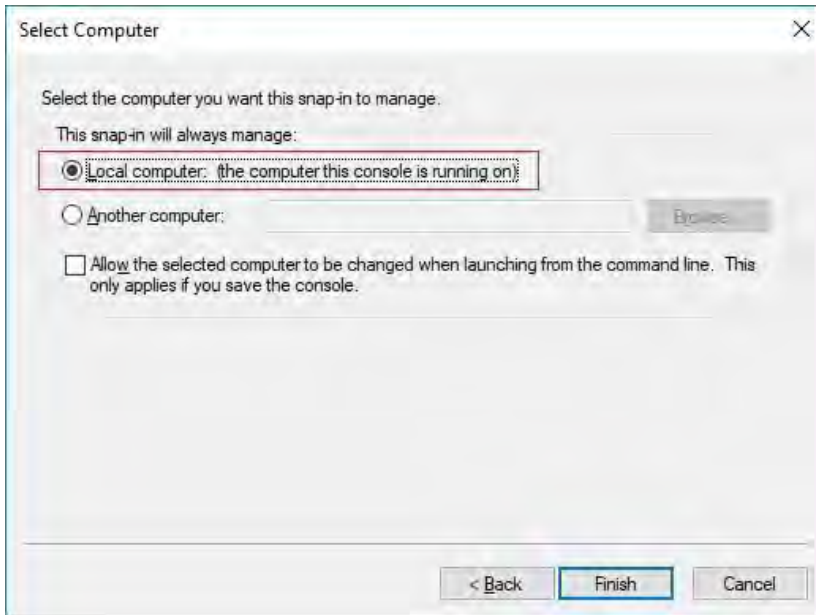
10. Seleccione el **complemento Certificados** y haga clic en **Agregar**.



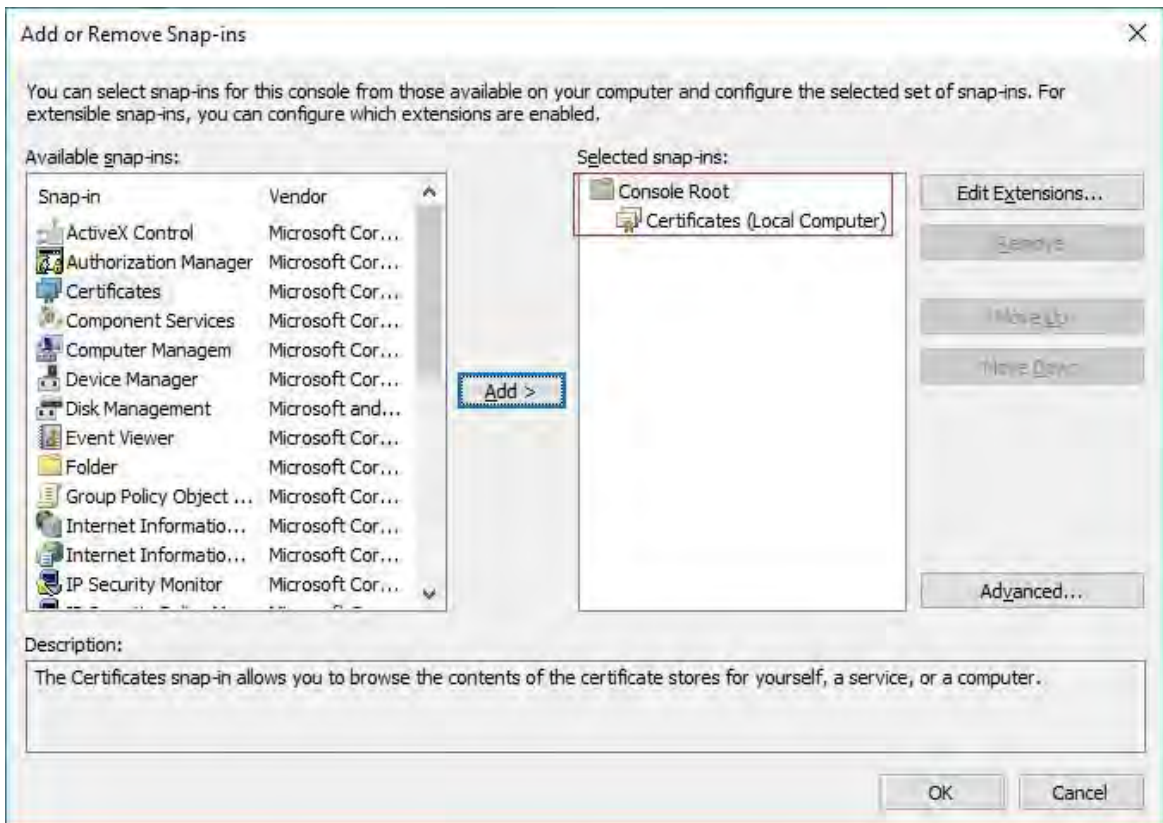
11. Seleccione que el complemento debe administrar certificados para la cuenta de equipo.



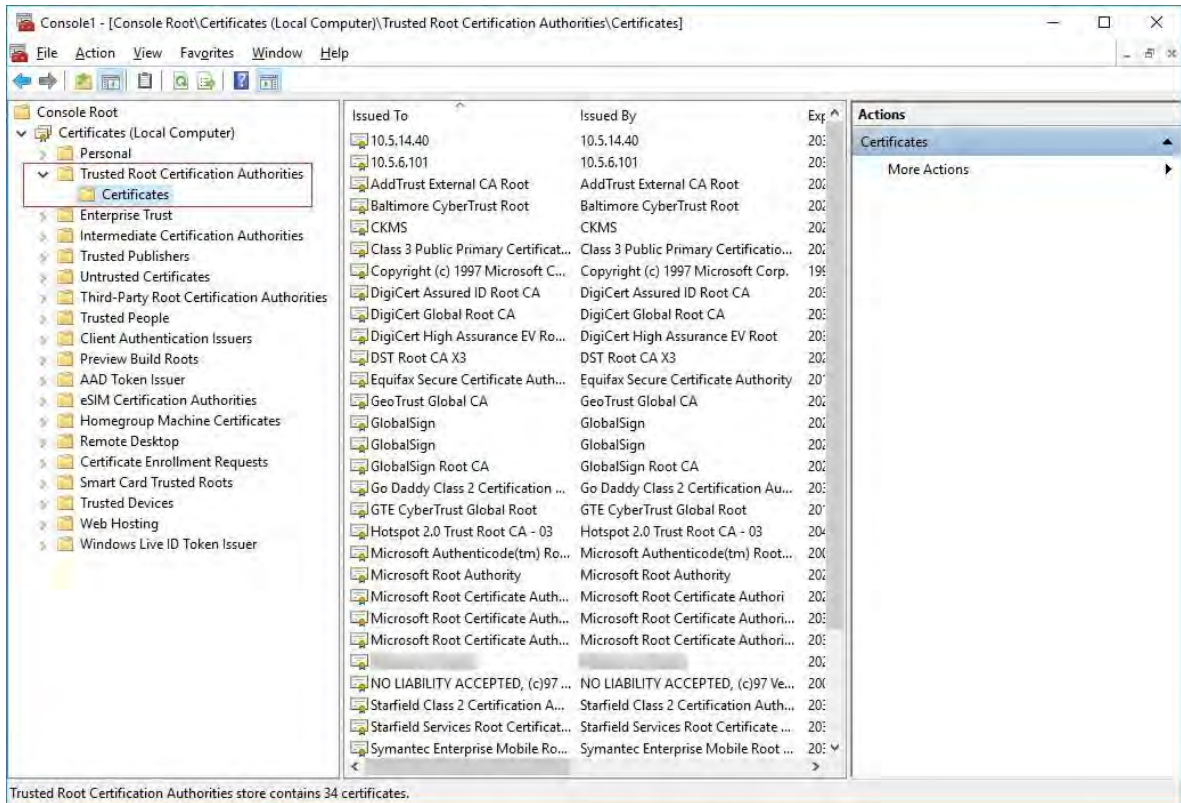
- 12. Seleccione **Equipo local** como el equipo que desea que administre el complemento y haga clic en **Finalizar**.



- 13. Haga clic en **Aceptar** después de agregar el complemento.



14. Verifique que el certificado aparezca en la vista central de las **entidades de certificación raíz de confianza** subárbol.



15. Repita los pasos en el siguiente equipo que se ejecute como cliente del servicio en el que se habilite el cifrado , hasta que haya instalado el certificado en todos los equipos pertinentes.

## Crear certificado SSL

Una vez que haya instalado el certificado de CA en todos los clientes, está listo para crear certificados que se instalarán en todos los equipos que ejecutan servidores (servidores de grabación, servidores de administración, servidores móviles o servidores de conmutación por error).




Si desea configurar un servidor de administración de conmutación por error, debe crear un certificado SSL diferente. Para obtener más información, consulte [Creación de un certificado SSL para el servidor de administración de conmutación por error en la página 38](#).

En el equipo donde creó el certificado de CA, desde la carpeta donde colocó el certificado de CA, ejecute el script de **certificado de servidor** para crear certificados SSL para todos los servidores.

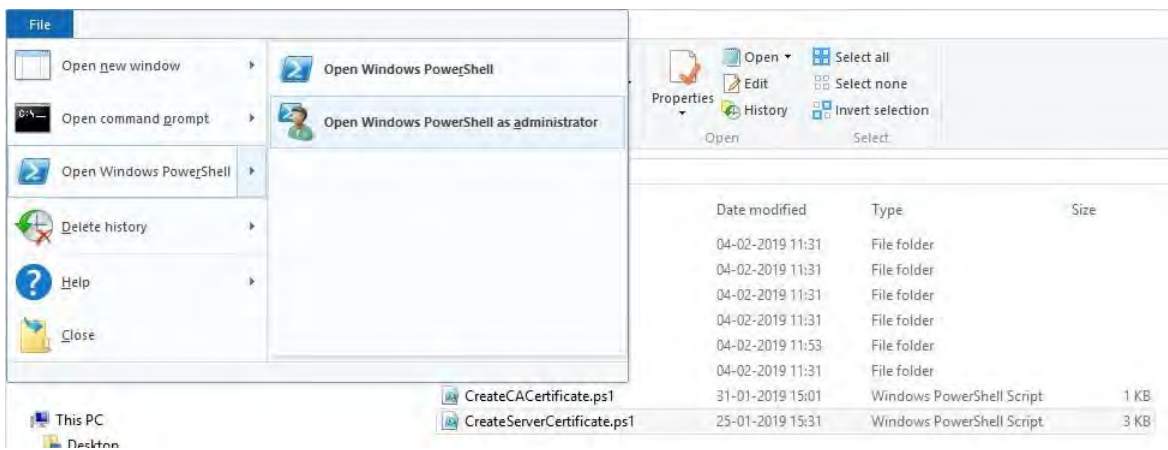


El equipo que use para crear certificados debe ejecutar Windows 10 o Windows Server 2016 o posterior.


1. En el Apéndice B, en la parte posterior de esta guía, encontrará un script para crear certificados de servidor.
2. Abra el Bloc de notas y pegue el contenido.

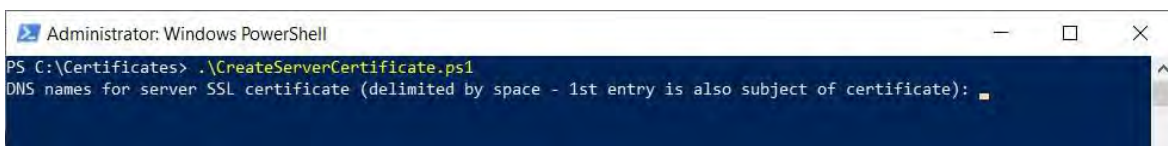
 Es muy importante que las líneas se rompan en los mismos lugares que en el Apéndice B. Puede agregar los saltos de línea en el Bloc de notas o, alternativamente, volver a abrir este PDF con Google Chrome, copiar el contenido nuevamente y pegarlo en el Bloc de notas.

3. En el Bloc de notas, haga clic en **Archivo -> Guardar como**, asigne al archivo el nombre **CreateServerCertificate.ps1** y guárdelo localmente en la misma carpeta que el certificado de CA, de la siguiente manera:  
C:\Certificates\CreateServerCertificate.ps1.
4. En el Explorador de archivos, vaya a C:\Certificates y seleccione el **archivo CreateServerCertificate.ps1**.
5. En el menú **Archivo**, seleccione **Abrir Windows PowerShell** y, a continuación, **Abrir Windows PowerShell como administrador**.



6. En PowerShell, en el símbolo del sistema, escriba `.\CreateServerCertificate.ps1` y presione **Entrar**.
7. Introduzca el nombre DNS del servidor. Si el servidor tiene varios nombres, por ejemplo, para uso interno y externo, agréguelos aquí, separados por un espacio. Presione **Entrar**.

 Para encontrar el nombre DNS, abra el Explorador de archivos en el equipo que ejecuta el servicio Servidor de grabación. Haga clic con el botón derecho en **Este equipo** y seleccione **Propiedades**. Utilice el **nombre completo del equipo**.



- Introduzca la dirección IP del servidor. Si el servidor tiene varias direcciones IP, por ejemplo, para uso interno y externo, agréguelas aquí, separadas por un espacio. Presione **Entrar**.



Para encontrar la dirección IP, puede abrir el símbolo del sistema en la computadora que ejecuta el servicio de servidor de grabación. Escriba **ipconfig /all**. Si ha instalado el sistema MOBOTIX HUB, puede abrir el cliente de gestión, navegar hasta el servidor y encontrar la dirección IP en la pestaña **Información**.

- Especifique una contraseña para el certificado y pulse **Intro** para finalizar la creación.



Esta contraseña se utiliza cuando se importa el certificado en el servidor.

Aparece un archivo Subjectname.pfx en la carpeta donde se ejecutó el script.

- Ejecute el script hasta que tenga certificados para todos los servidores.

## Importar certificado SSL

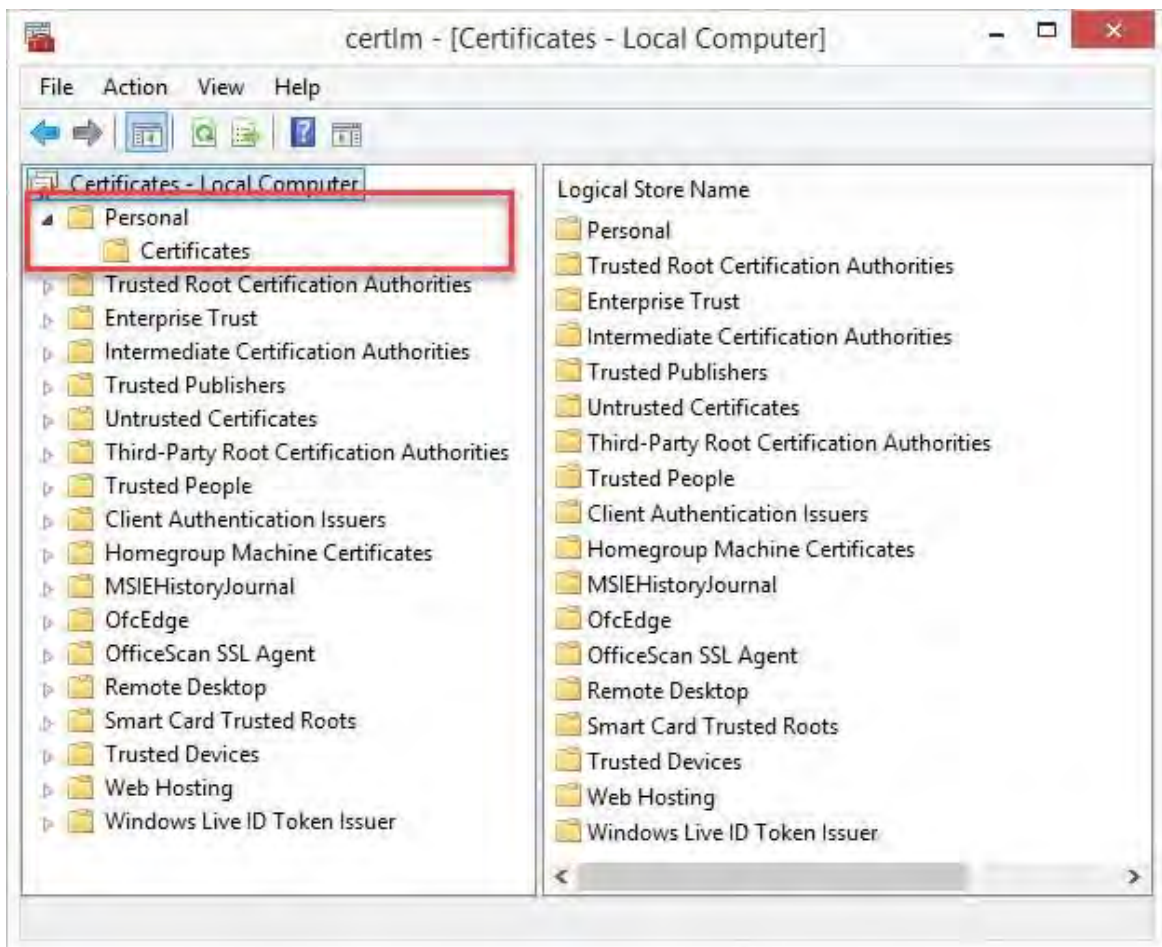
Después de crear los certificados SSL, instálelos en los equipos que ejecutan el servicio de servidor.

- Copie el archivo Subjectname.pfx correspondiente del equipo en el que creó el certificado en el equipo de servicio de servidor correspondiente.



Recuerde que cada certificado se crea en un servidor específico.

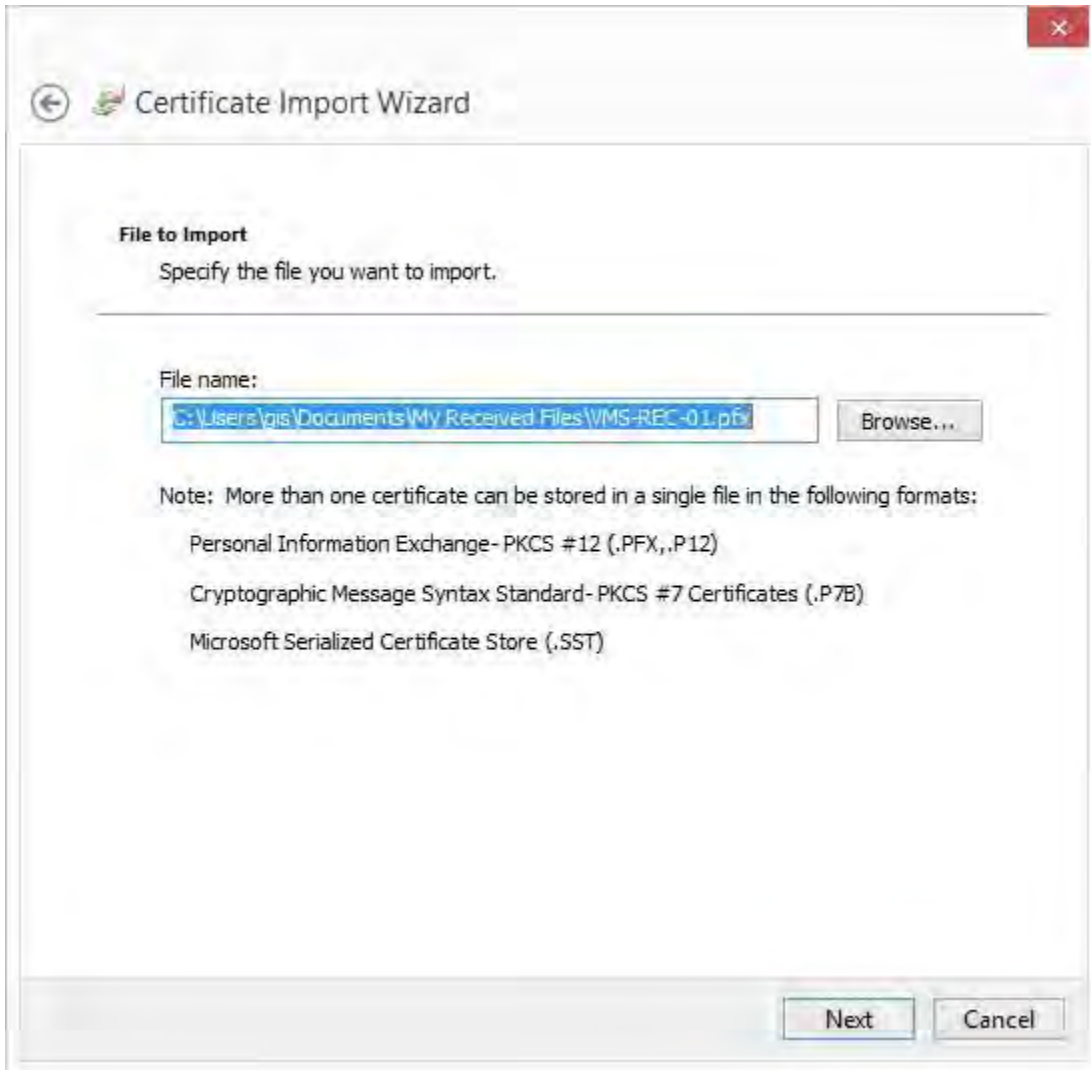
2. En el equipo de servicio del servidor, inicie **Administrar certificados de equipo**.
3. Haga clic en **Personal**, haga clic con el botón derecho en **Certificados** y seleccione **Todas las tareas > importar**.



4. Seleccione esta opción para importar el certificado en el almacén del **equipo local** y haga clic en **Siguiente**.

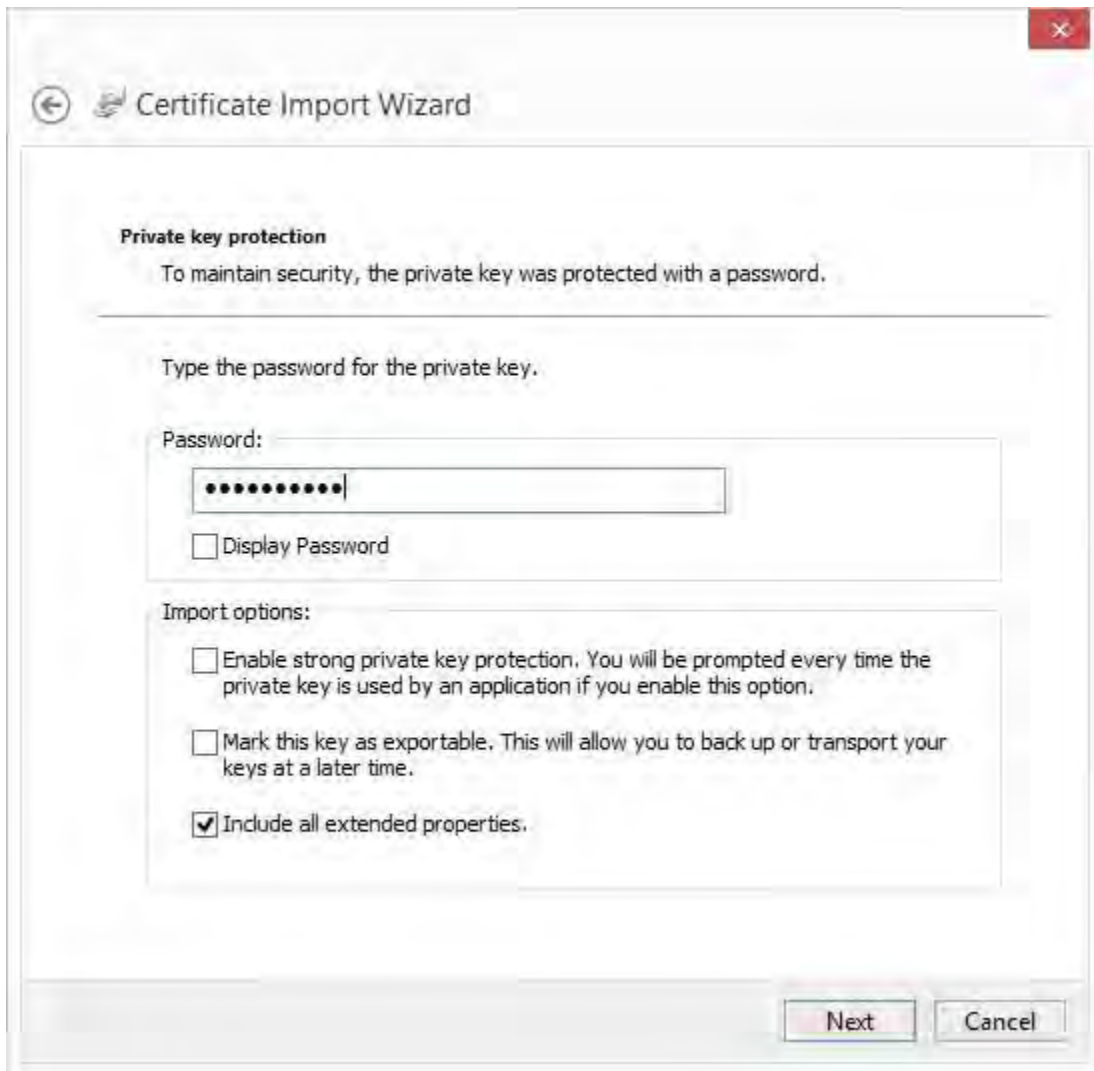


5. Vaya al archivo de certificado y haga clic en **Siguiente**.





6. Introduzca la contraseña de la clave privada que especificó al crear el certificado de servidor y, a continuación, haga clic en **Siguiente**.



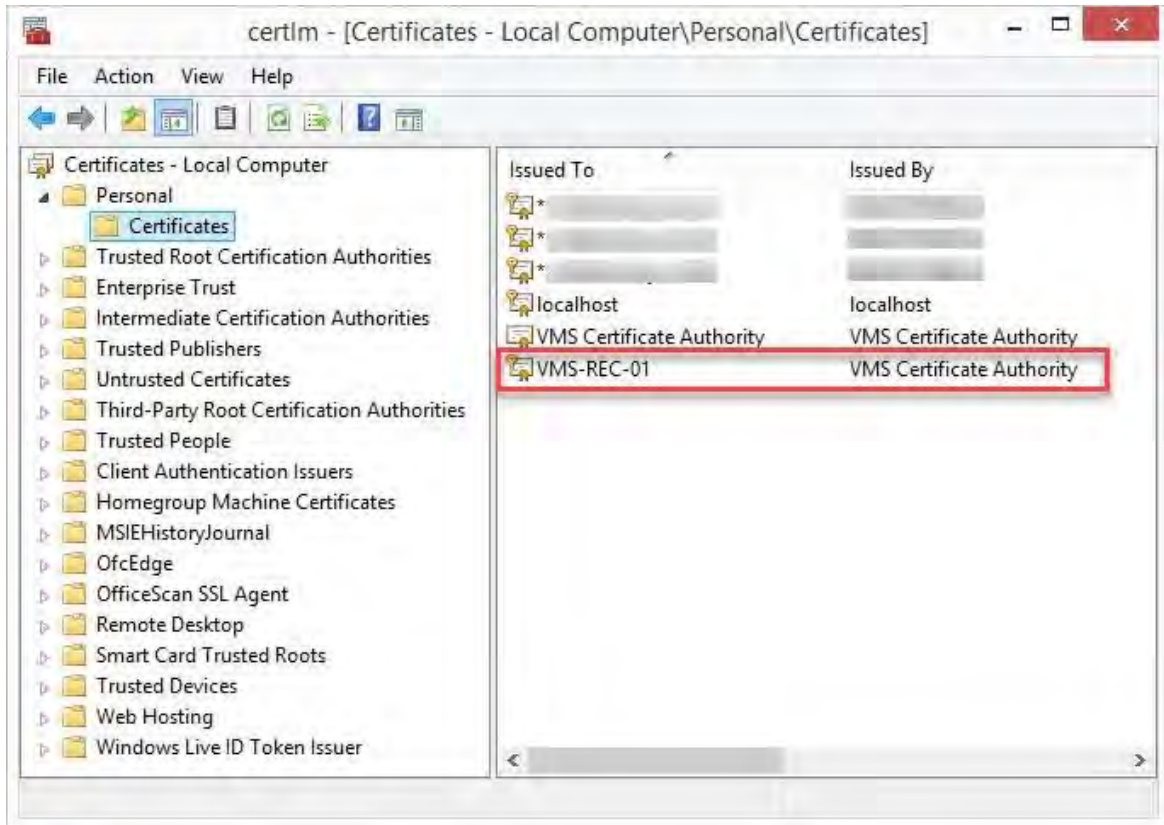
7. Coloque el archivo en el **Almacén de certificados: Personal** y, a continuación, haga clic en **Siguiente**.



8. Verifique la información y haga clic en **Finalizar** para importar el certificado.

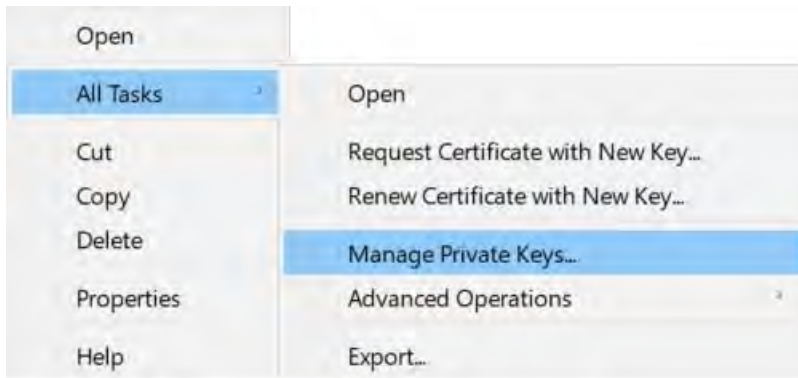


9. El certificado importado aparece en la lista.

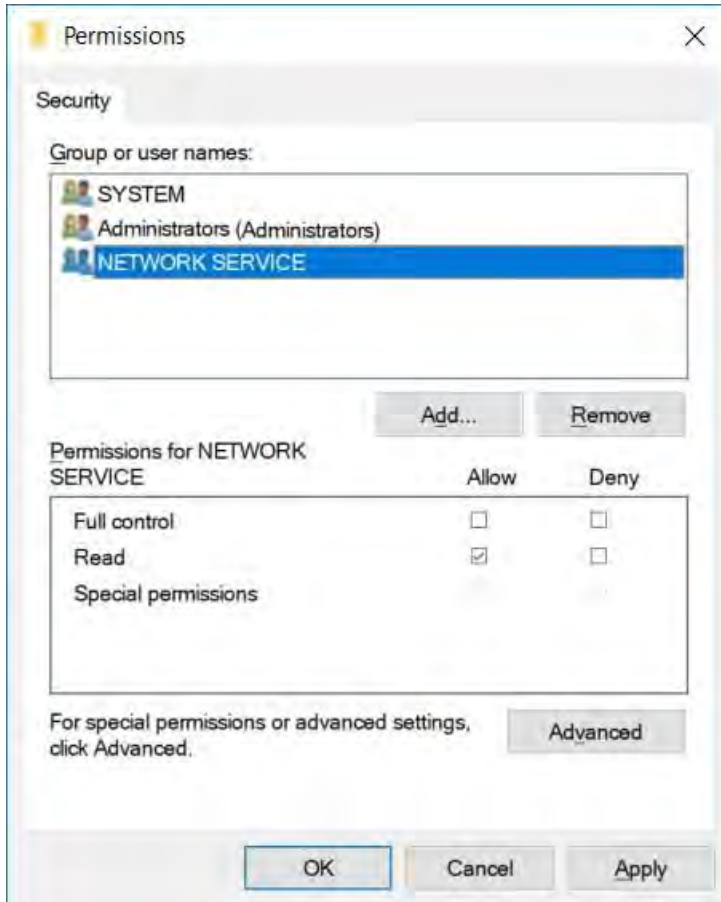


10. Para permitir que un servicio use la clave privada del certificado, haga clic con el botón secundario en el certificado y seleccione **Todas las tareas >**

**Administrar claves privadas.**



11. Añada permiso de lectura para el usuario que ejecuta los servicios de MOBOTIX HUB VMS y que necesita utilizar el certificado de servidor .



12. Continúe con el siguiente equipo, hasta que haya instalado todos los certificados de servidor.

## Creación de un certificado SSL para el servidor de administración de conmutación por error

La conmutación por error del servidor de gestión MOBOTIX HUB se configura en dos ordenadores. Para asegurarse de que los clientes confían en el servidor de administración en ejecución, instale el certificado SSL en el equipo principal y en el equipo secundario.

Para crear e instalar el certificado SSL para el clúster de conmutación por error, primero debe instalar el certificado de CA.

En el equipo donde creó el certificado de CA, desde la carpeta donde colocó el certificado de CA, ejecute el script de **certificado del servidor de administración de conmutación por error** para crear un certificado SSL para el equipo principal y el equipo secundario.



El equipo que use para crear certificados debe ejecutar Windows 10 o Windows Server 2016 o posterior.

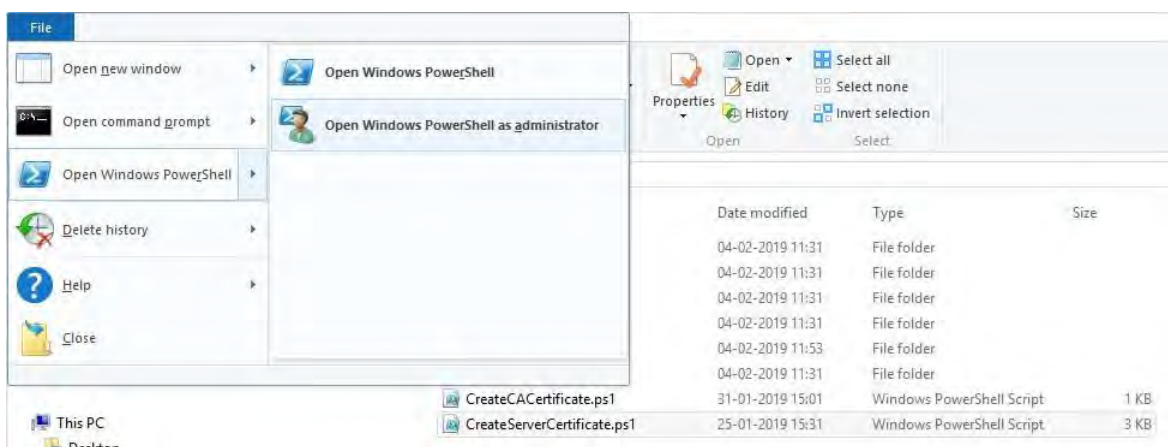
1. En el Apéndice C de esta guía, copie el script para crear certificados de servidor de administración de conmutación por error.
2. Abra el Bloc de notas y pegue el script.



Es muy importante que las líneas se rompan en los mismos lugares que se muestran en el Apéndice

C. Puede agregar los saltos de línea en el Bloc de notas o, alternativamente, volver a abrir este PDF con Google Chrome, copiar el contenido nuevamente y pegarlo

3. En el Bloc de notas, seleccione **Archivo -> Guardar como**, asigne al archivo el nombre **CreateFailoverCertificate.ps1** y guárdelo localmente en la misma carpeta que el certificado de CA: Ejemplo: C:\Certificates\CreateFailoverCertificate.ps1.
4. En el Explorador de archivos, vaya a C:\Certificates y seleccione el **archivo CreateFailoverCertificate.ps1**.
5. En el menú **Archivo**, seleccione **Abrir Windows PowerShell** y, a continuación, **Abrir Windows PowerShell como administrador**.



6. En PowerShell, escriba **.\CreateFailoverCertificate.ps1** en el símbolo del sistema y presione **Entrar**.

7. Especifique los FQDN y los nombres de host para el equipo principal y el equipo secundario, separados por una coma.

Ejemplo: pc1host, pc1host.domain, pc2host, pc2host.domain.

Presione **Entrar**.

8. Especifique la dirección IP virtual del clúster de conmutación por error. Presione **Entrar**.
9. Especifique una contraseña para el certificado y pulse **Intro** para finalizar la creación.



Esta contraseña se utiliza cuando se importa el certificado en el servidor.

El archivo [virtualIP].pfx aparece en la carpeta donde se ejecutó el script.

Importe el certificado de la misma manera que importaría un certificado SSL, consulte [Importar certificado SSL en la página 29](#). Importe el certificado en los equipos primario y secundario.



## Instalar certificados para la comunicación con el servidor móvil

Para utilizar un protocolo HTTPS para establecer una conexión segura entre el servidor móvil y los clientes y servicios, debe aplicar un certificado válido en el servidor. El certificado confirma que el titular del certificado está autorizado a establecer conexiones seguras.

En MOBOTIX HUB VMS, el cifrado se habilita o deshabilita por servidor móvil. El cifrado se activa o deshabilita durante la instalación del producto MOBOTIX HUB VMS o mediante Server Configurator. Cuando se habilita el cifrado en un servidor móvil, se utiliza la comunicación cifrada con todos los clientes, servicios e integraciones que recuperan flujos de datos.



Al configurar el cifrado para un grupo de servidores, debe estar habilitado con un certificado que pertenezca al mismo certificado de CA o, si el cifrado está deshabilitado, debe estar deshabilitado en todos los equipos del grupo de servidores.



Los certificados emitidos por CA (Autoridad de Certificación) tienen una cadena de certificados y en la raíz de esa cadena se encuentra el certificado raíz de CA. Cuando un dispositivo o navegador ve este certificado, compara su certificado raíz con los preinstalados en el sistema operativo (Android, iOS, Windows, etc.). Si el certificado raíz aparece en la lista de certificados preinstalados, el sistema operativo garantiza al usuario que la conexión con el servidor es lo suficientemente segura. Estos certificados se emiten para un nombre de dominio y no son gratuitos.

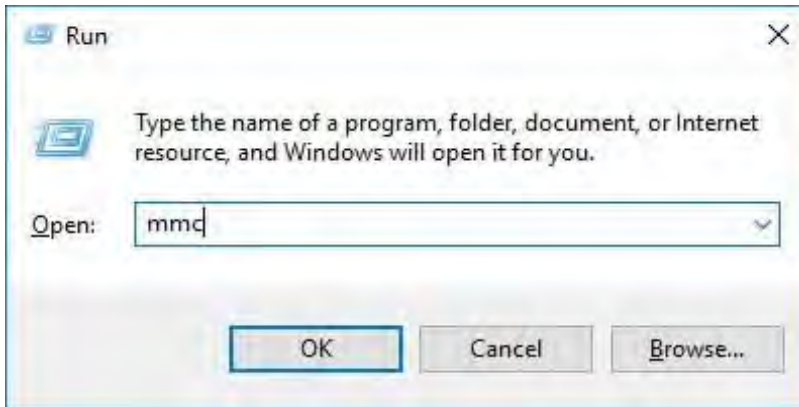
### Agregar un certificado de CA al servidor

Agregue el certificado de CA al servidor móvil haciendo lo siguiente.

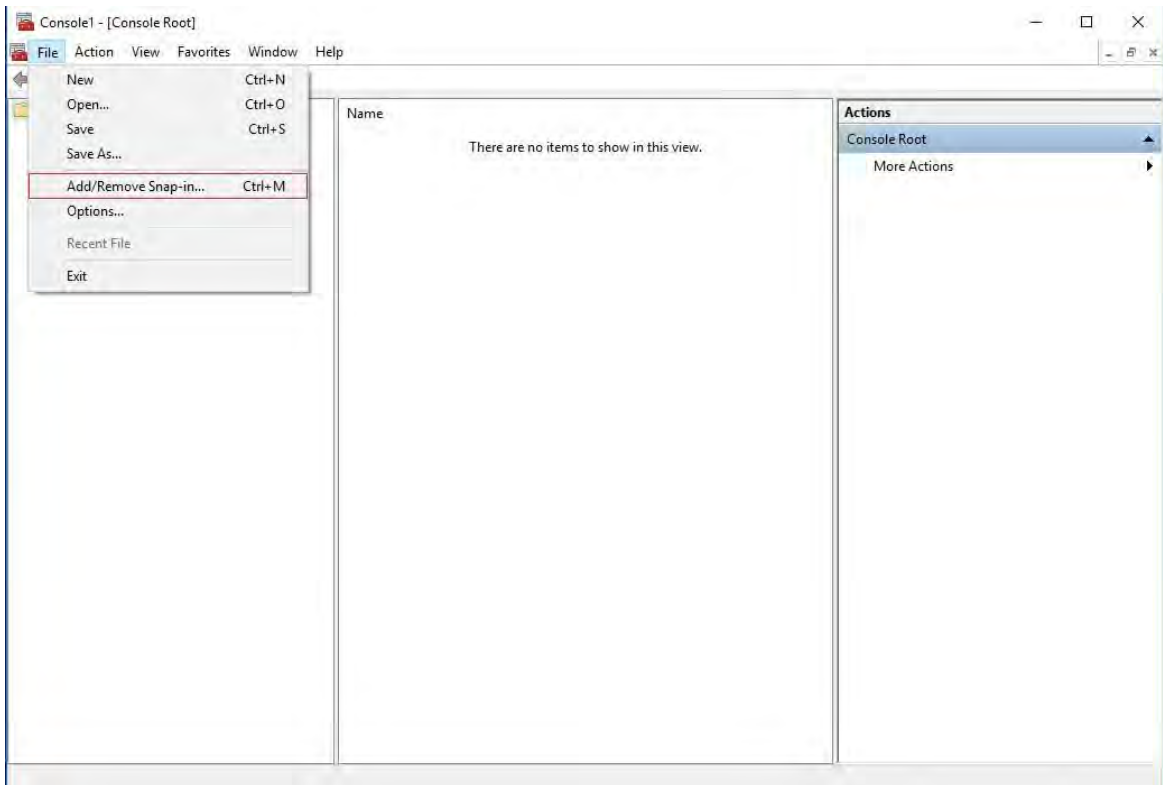


Los parámetros específicos dependen de la CA. Consulte la documentación de su CA antes de continuar.

1. En el equipo que aloja el servidor móvil, abra la Consola de administración de Microsoft.

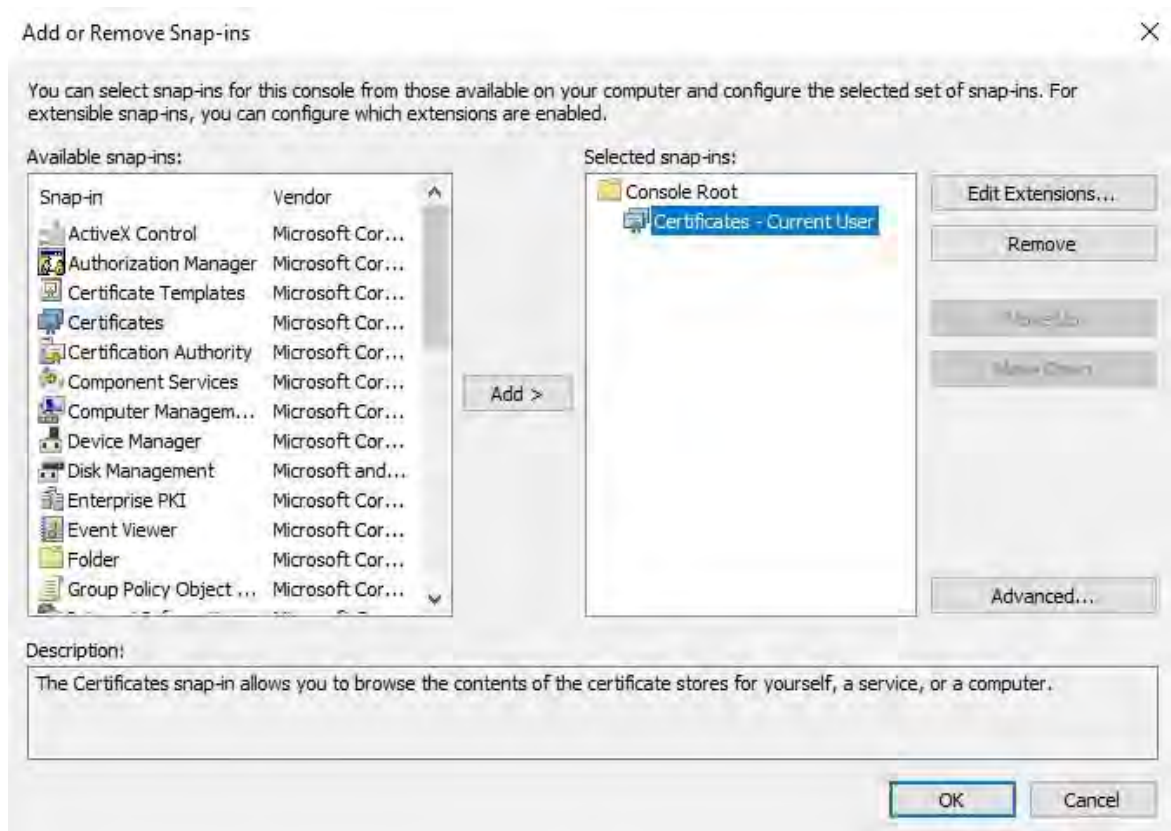


2. En Microsoft Management Console, en el menú **Archivo**, seleccione **Agregar o quitar complemento....**

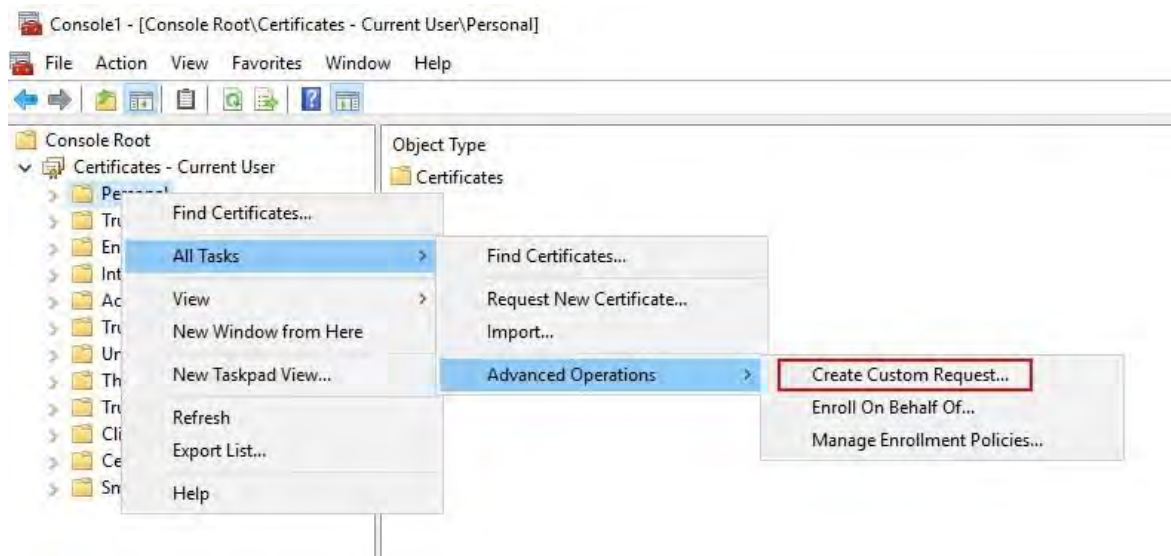


3. Seleccione el **complemento Certificados** y haga clic en **Agregar**.

Haga clic en **Aceptar**.

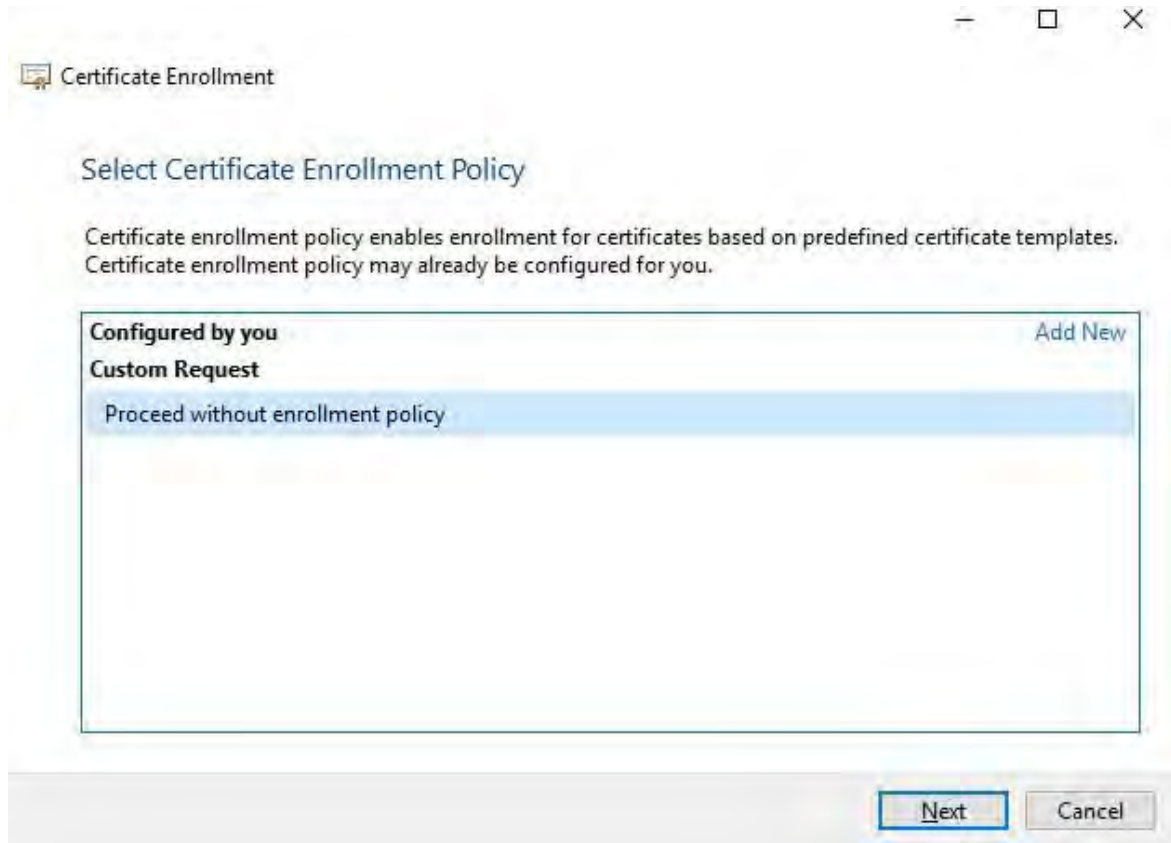


4. Expanda el objeto Certificados. Haga clic con el botón derecho en la **carpeta Personal** y seleccione **Todas las tareas > Operaciones avanzadas > Crear solicitud personalizada**.

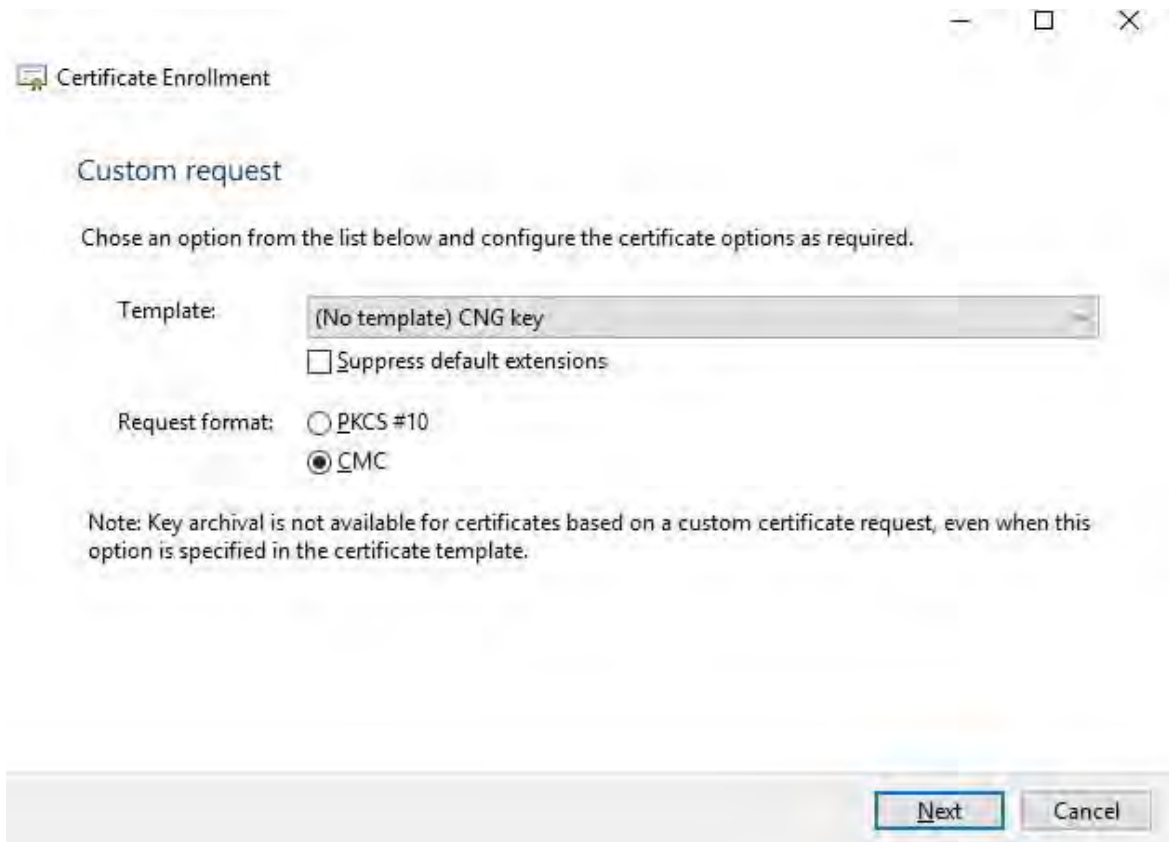



5. Haga clic en **Siguiente** en el Asistente para **inscripción de certificados** y seleccione **Continuar sin directiva de inscripción**.

Haga clic en **Siguiente**.



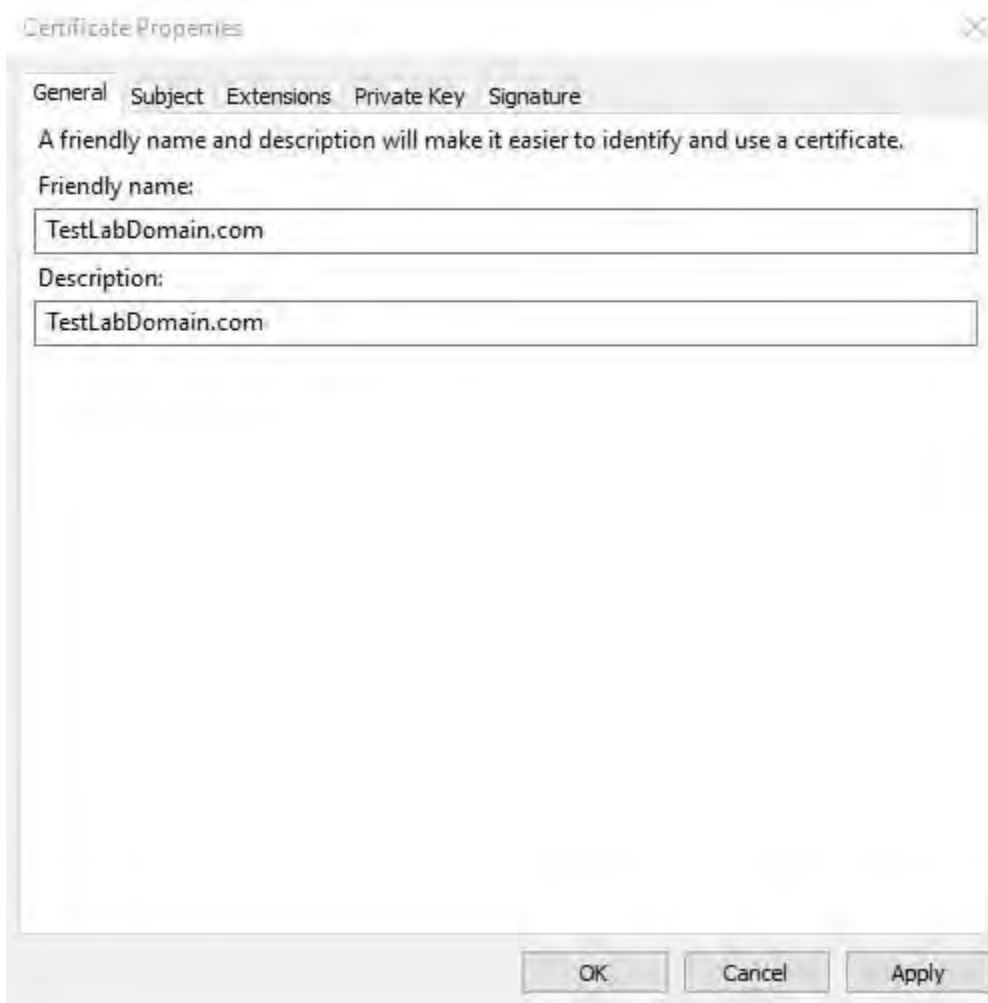
6. Seleccione la plantilla **de clave CNG (sin plantilla)** y el formato de solicitud de **CMC** y haga clic en **Siguiente**.



 El formato de la solicitud depende de la CA. Si se elige el formato incorrecto, la CA emitirá un error cuando se envíe la solicitud de firma de certificado (CSR). Consulte con la CA para asegurarse de que elige correctamente.

7. Expanda para ver los **detalles** de la solicitud personalizada y haga clic en **Propiedades**.

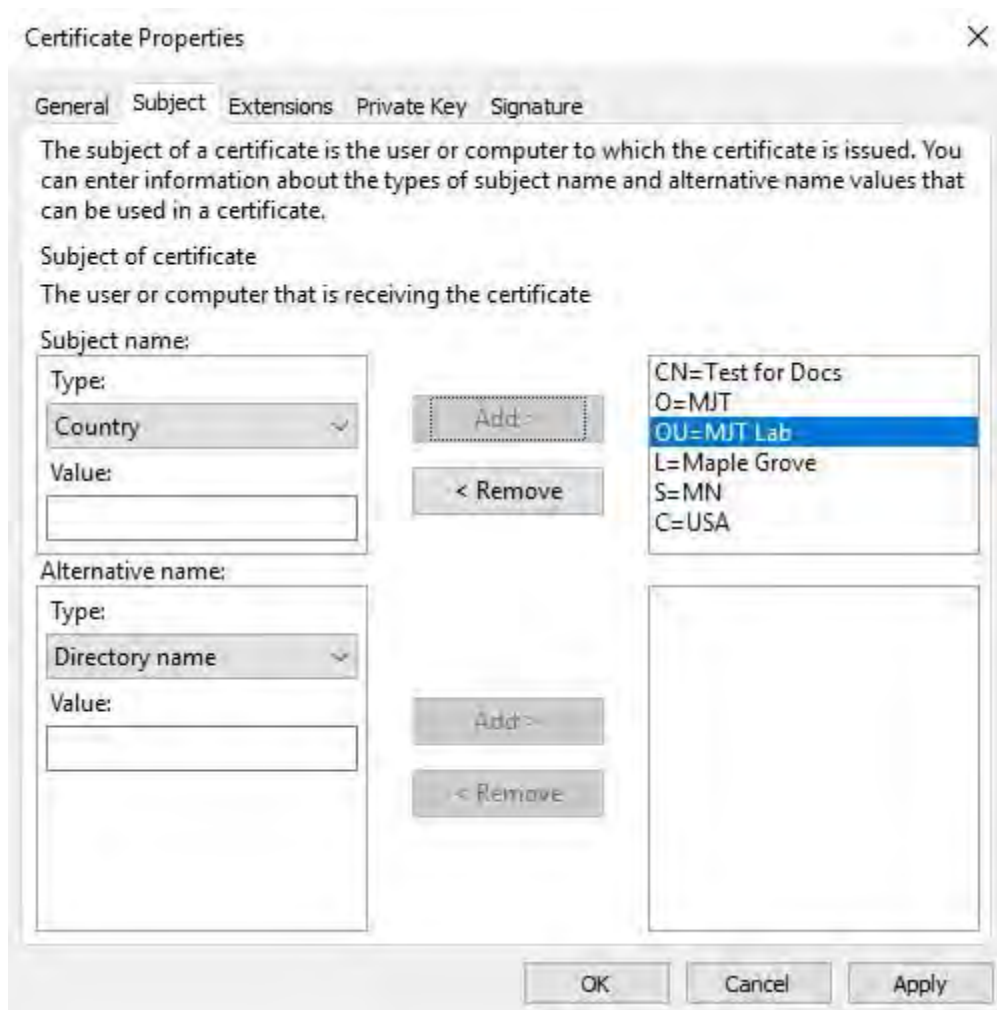
8. En la pestaña **General**, rellene los campos **Nombre descriptivo** y **Descripción** con el nombre de dominio registrado en la CA.



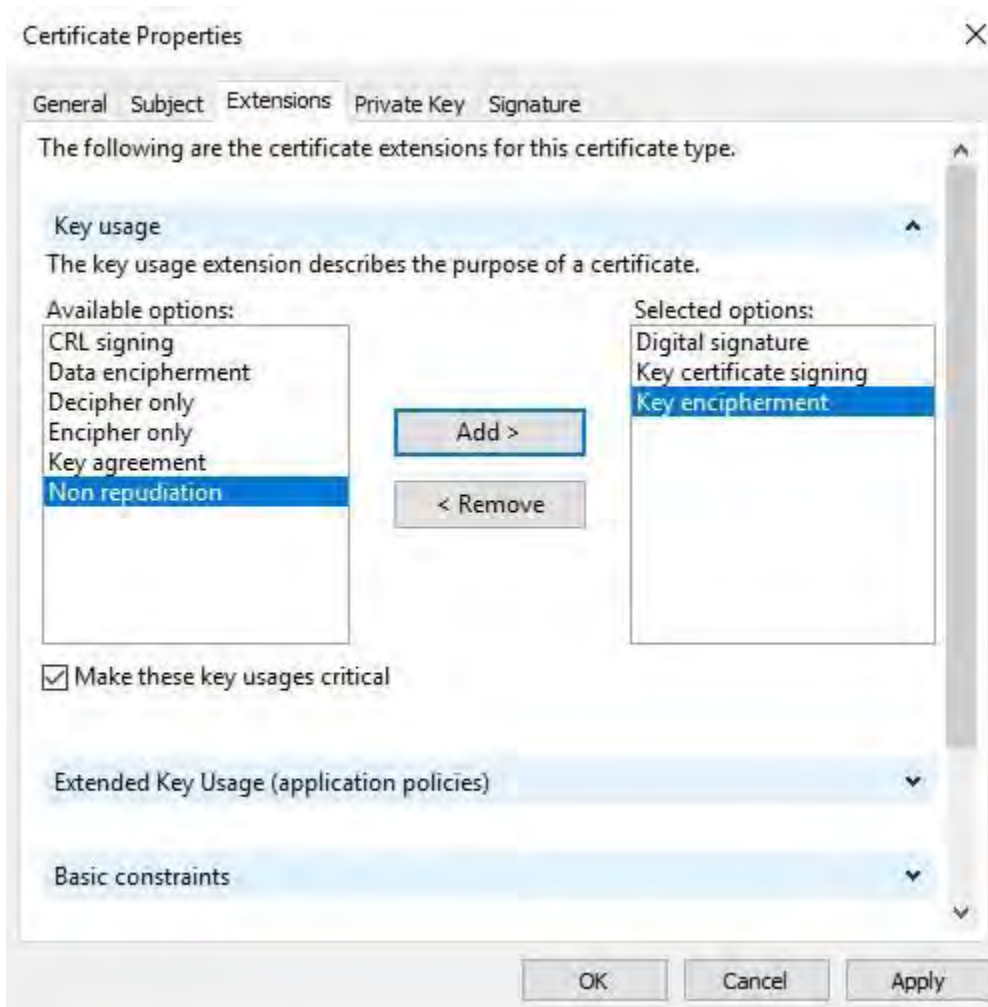
9. En la **pestaña Asunto**, introduzca los parámetros requeridos por la CA específica.

Por ejemplo, el nombre del firmante, el tipo y el **valor** son diferentes para cada CA. Un ejemplo es la siguiente información obligatoria:

- Nombre común:
- Organización:
- Unidad Organizativa :
- Ciudad/Localidad:
- Estado/Provincia:
- País/Región:




10. Algunas CA no requieren extensiones. Sin embargo, si es necesario, vaya a la **pestaña Extensiones** y expanda el menú Uso de **claves** . Agregue las opciones necesarias de la lista de **opciones disponibles** a la lista de **opciones seleccionadas**.

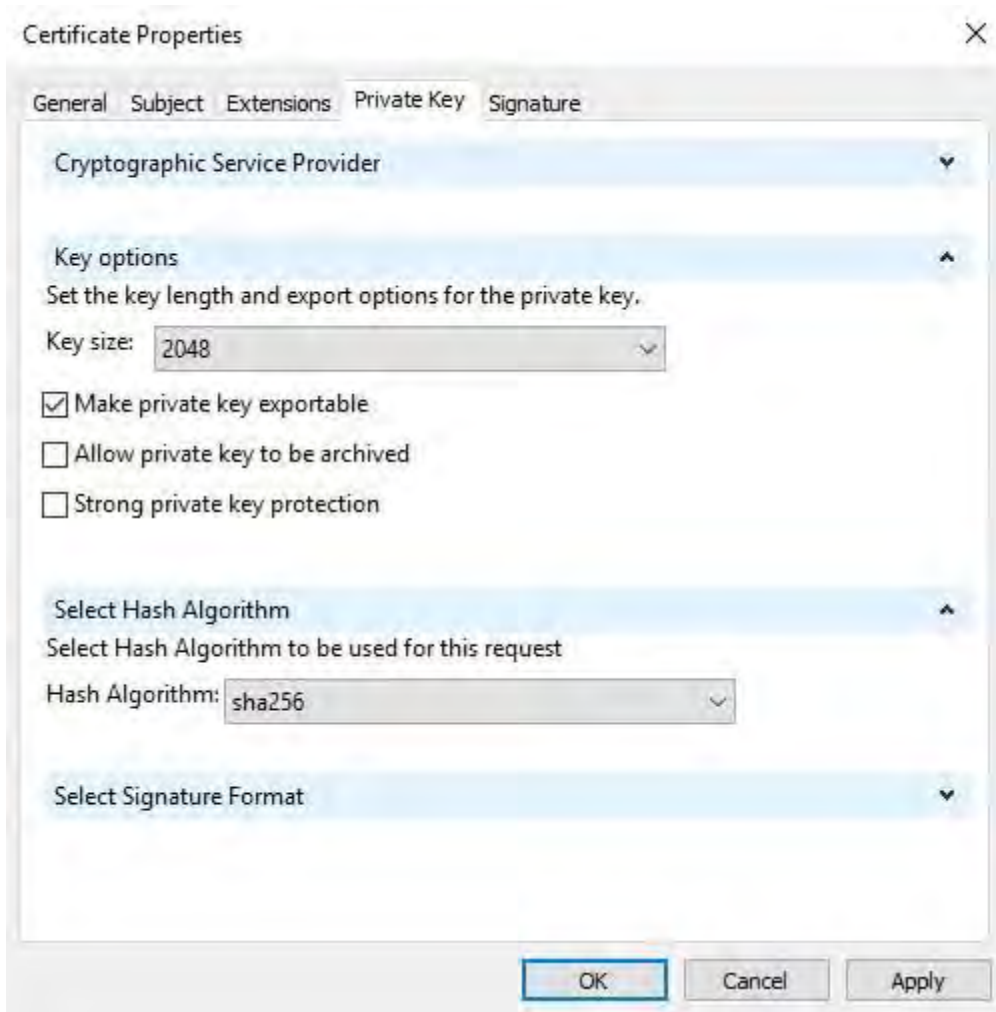




11. En la pestaña **Clave privada**, expanda el menú **Opciones de clave**.

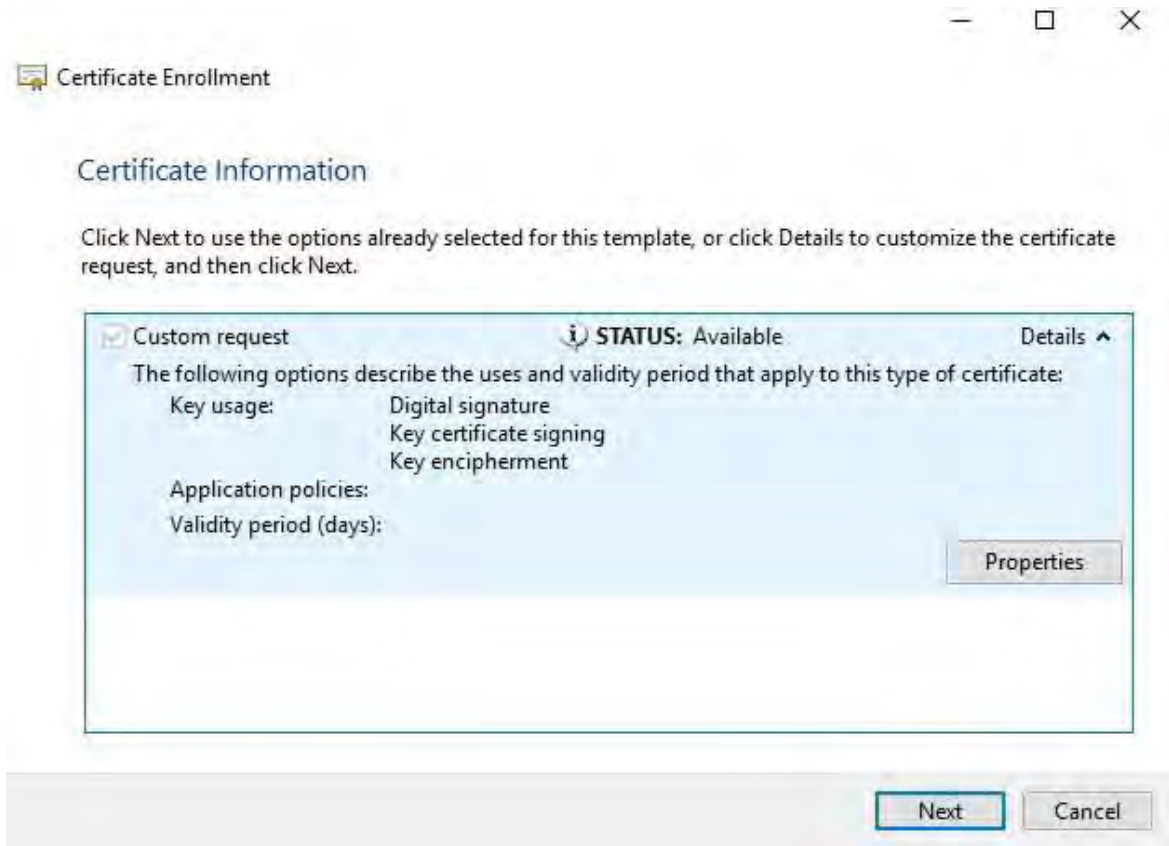
Establezca el tamaño de la clave en 2048 y seleccione la opción para que la clave privada sea exportable.

 La variable de tamaño de clave está determinada por la CA, por lo tanto, es posible que se requiera una clave de tamaño mayor. También pueden ser necesarias otras opciones, como un algoritmo hash específico (sha256). Ajuste todas las opciones necesarias antes de continuar con el siguiente paso.



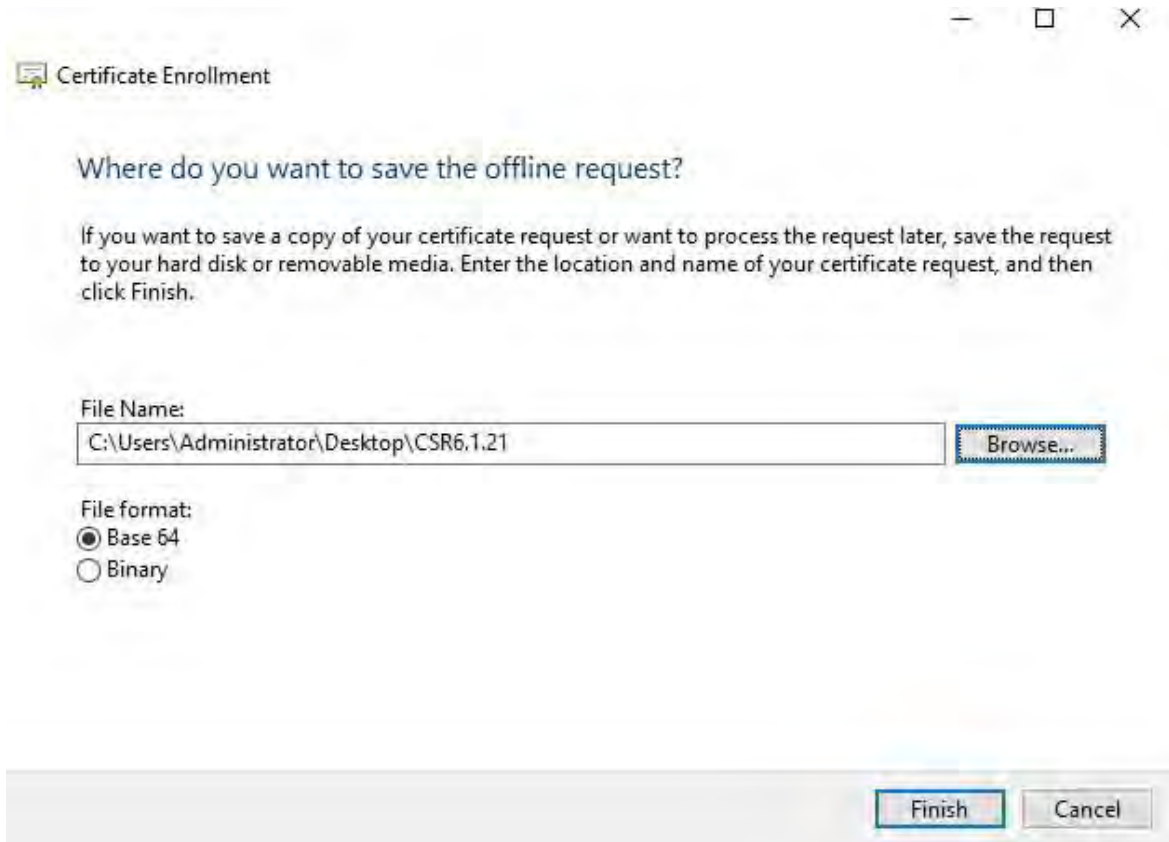
12. A menos que la CA requiera una firma, el siguiente paso es hacer clic en **Aceptar**.

13. Cuando se hayan definido todas las propiedades del certificado, haga clic **en Siguiente** en la inscripción de **certificados** hechicero.



14. Seleccione una ubicación para guardar la solicitud de certificado y un formato. Vaya a esa ubicación y especifique un nombre para el archivo .req. El formato predeterminado es base 64, sin embargo, algunas CA requieren el formato binario.

15. Haga clic en **Finalizar**.



Se genera un archivo .req, que debe utilizar para solicitar un certificado firmado.

### Cargue el archivo .req para recibir un certificado firmado a cambio



Cada CA tiene un proceso diferente para cargar archivos .req con el fin de recibir un certificado firmado a cambio. Consulte la documentación de la CA para obtener información sobre cómo recuperar un certificado firmado.

Al trabajar con el servidor móvil, se recomienda utilizar una CA de terceros. En la mayoría de las situaciones de CA de terceros, es necesario descargar un archivo .ZIP y extraer el contenido en el equipo que aloja el servidor móvil.

Hay varios tipos de archivos que se pueden incluir en el contenido del archivo .ZIP extraído.

. CER o . Los archivos CRT se pueden instalar mediante un proceso similar. Haga clic con el botón derecho en el archivo y elija **Instalar certificado** en el menú contextual.

En los siguientes pasos se utiliza un archivo . CER de una CA interna.

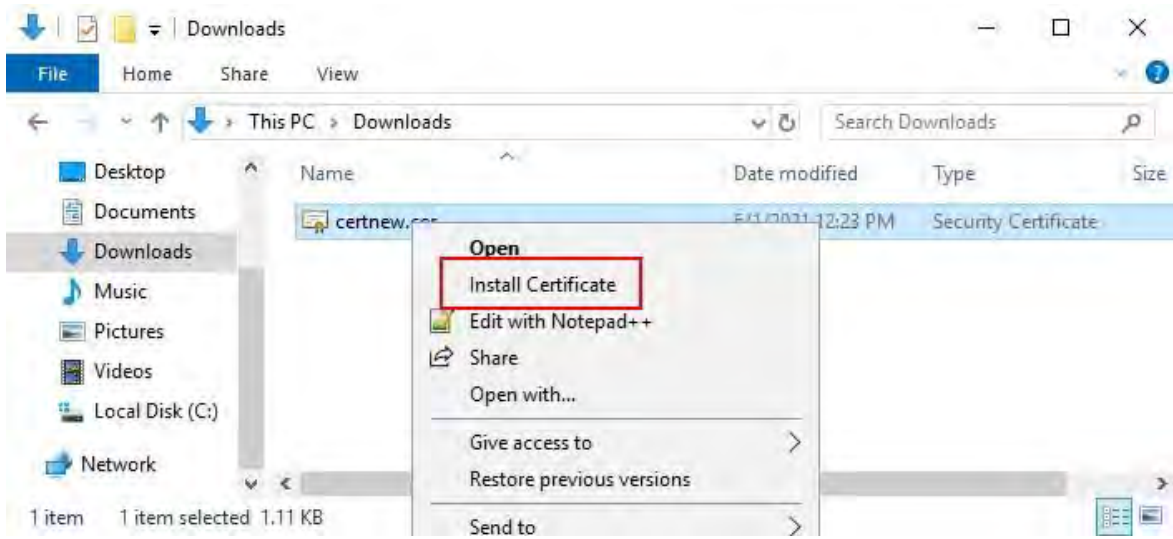
La CA necesitará el contenido del archivo .req. Se le pedirá que copie todo el texto del archivo .req, incluidas las líneas inicial y final, y que pegue el texto en un campo disponible en un portal administrado por la CA.

1. Vaya a la ubicación del archivo .req, ábralo en el Bloc de notas y pegue el texto en un campo disponible en un portal administrado por su CA.

```

CSR6.1.21 - Notepad
File Edit Format View Help
|-----BEGIN NEW CERTIFICATE REQUEST-----
MIIGBAYJKoZIhvcNAQcCoIIF9TCCBFECAQMsDzANBg1ghkgBZQMEAgEFADCCBEoG
CCsGAQUFBwwCoIIEPASCBDgwgGQ0MGQwYgIBAgYKKwYBBAGCNwoKATFRME8CAQA
AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QLTBBMDAwNDY3DB1JUC0wQTAw
MDQ2N1xBZG1pbm1zdHJhdG9yDAdNTUMuRvHfMIIDxqCCA8ICAQEwgG07MIICowIB
ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAGMAk1OMRQwEgYDVQQQHDAtdNYXBsZSBH
cm92ZTEQMA4GA1UECwwHTUpUEXhYjEMMAoGA1UECgwDTUpUMRYwFAYDVQQDDA1U
ZXN0IGZvcjBEBzNzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7G1/
5z1YrUG0o4dW1/b3o35rPcQQby0UE0K1MwjaIy4YrRPM9HjhKReThbcSnxddj6eR
Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ//Zi08bEPobLv8YnWieNDuw
lkaJWWRx3mb1/Yz0f1bwZrKFT3nkrXYOFYmZOR19W0J+Iin0BtziwiC8Dht+bxST
nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9qC47RP9yMjyuuEtpdR9ERoR
qJJo0K6CdrKLU5kZFIDTIVbs0F3mNqnHCyzs7cEEs18zBATRXkk/kRI+Po6cXNJp
Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEAYI3DQIDMQ4WDDewLjAuMTc3
NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/wQEAwICpDAdBgNVHQ4EFgQU
vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCNxUUMTYwNAIBBQwLSVAtMEEw
MDA0NjcMGU1QLTBBMDAwNDY3XEFkbWluaXN0cmF0b3IMB01NQy5FWEUwZgYKKwYB
BAGCNw0CAjFYMfYCAQAeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFMAbwBmAHQAdwBh
AHIAZQAgAEsAZQB5ACAuUwB0AG8AcgBhAGcAZQAgFAAACgBvAHYAaQBkAGUAcgMB
ADANBgkqhkiG9w0BAQsFAAOCAQEAAqtkB5HCh2a1BD2QcKdFuhVQbNhg+G5wcVkJt
7bXdwVuzoAxd9BFd+uVy4D3TmvXtineT3GVWQbKJCcxRZeTKPBFnHG0SeaYupUrG
cX4ySsKR1xGSu0hsfIVa/5NXiIYgYxMh1z3nt2CDw+RNqAp/lgLV2cLsui01y5ib
088po4/b9eiXV7A1DWfY7ecw/7Z20a07Sa00aRbwzGJ8He1IiVEjfyAt7KLoufAq
LkeSaJtjokkJuGPdr+ykjfuCmIF4hSbc0xzVkJPCQbiH0wSxDG1kqYH28Xru665Q6
0L7QgBXCc7tcecdieqbYmp50LJPPqEQDQiyjz57j3eYIFNYYjAAMAaxggGLMIIB
hwIBA4AUvruQxeU1yku5Cem3anpu1cbMEDAwDQYJYIZIAWUDBAIBBQCgSjAXBgkq
hkiG9w0BCQMxCgYIKwYBBQUHDAIwLwYJKoZIhvcNAQkEMSIEIck1SKp5MUjMa+vr
DU1UXU+V05r1F8bNdM0mDgYfmjCiMA0GCSqGSIb3DQEBAQUABIIBAEjqqe4GSGE4
oZQj0vbWvAP0Ab2u8epFm7ZIMZzsJSzR0z98m+R+1R2mCoqWC0SSafybJ701Jh1y
A3eqzDYxau9p9drJft317sGAERE/i1D3BFvKZZQH0sz0JNRwDp3qByHHzVCULUEI
JS0pYvI1s3S23ZYEedQLp35Xy87378zLLGLpgGKTK4teav1IitUJwVCKikL47uyF
uOY4XLagwI1WWALsPFL+5ZcVNZMvszsbuMEXvjBkFKyhMv49oisgFcLJ1AoMtWn
7Mbq8K6ckbKkVpuvmwThkVTp1W3hIS/i/J0X7c2unA25LxAC/P/LyWhPt/Vk/oqf
06jNaHC/zBQ=
-----END NEW CERTIFICATE REQUEST-----
Windows (CRLF) Ln 1, Col 1 100%
    
```

2. Cuando reciba el certificado de su CA, vaya a la carpeta de descargas (o a cualquier lugar que elija para almacenar la carpeta en el equipo), haga clic con el botón derecho en el certificado y seleccione **Instalar certificado**.

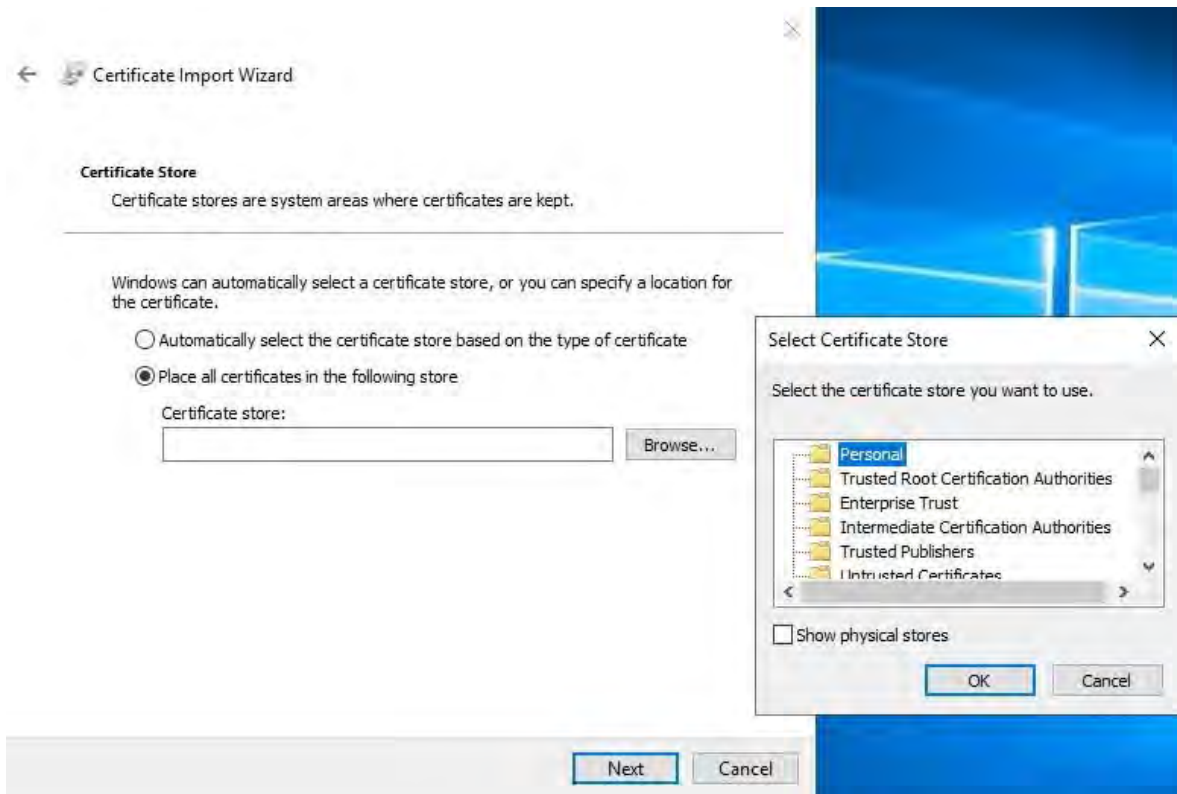


3. Acepte la advertencia de seguridad si aparece.

Seleccione instalar el certificado para el equipo local y haga clic en **Siguiente**.



4. Elija una ubicación de almacenamiento, vaya al almacén de certificados personales y haga clic en **Siguiente**.



5. Finalice el asistente **para instalar certificado**.

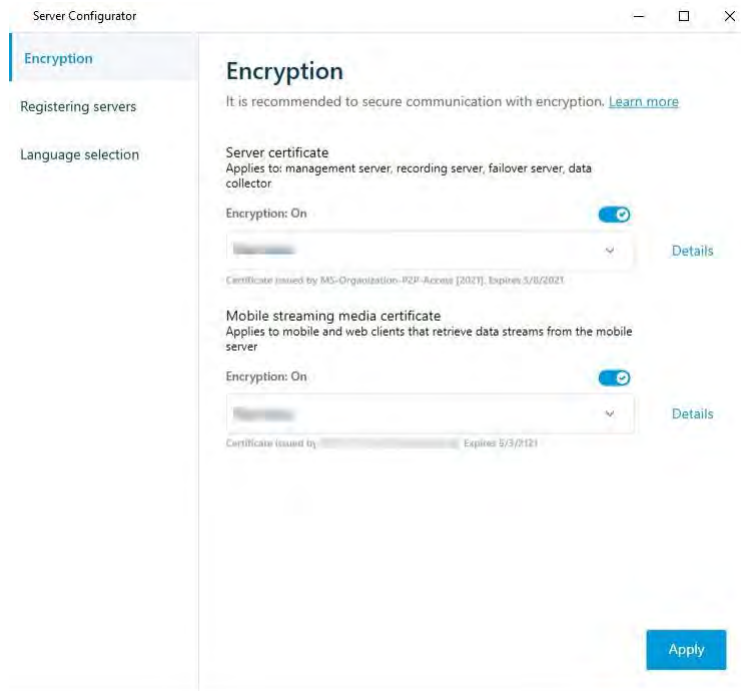
### Habilitar el cifrado en el servidor móvil

Una vez que el certificado esté instalado en el equipo que aloja el servidor móvil, haga lo siguiente.

1. En un ordenador con un servidor móvil instalado, abra el **Configurador de servidores** desde:
  - El menú Inicio de Windows
  - o
  - El Administrador de servidores móviles haciendo clic con el botón derecho en el icono del Administrador de servidores móviles en la barra de tareas del equipo
2. En Server **Configurador**, en **Certificado de medios de transmisión móvil**, active **Cifrado**.
3. Haga clic en **Seleccionar certificado** para abrir una lista con los nombres de los firmantes únicos de los certificados que tienen una clave privada y que están instalados en el equipo local en el Almacén de certificados de Windows.
4. Seleccione un certificado para cifrar la comunicación del cliente móvil MOBOTIX HUB y el cliente web MOBOTIX HUB con el servidor móvil.  
  
Seleccione **Detalles** para ver la información del Almacén de certificados de Windows sobre el certificado seleccionado.



Al usuario del servicio de servidor móvil se le ha dado acceso a la clave privada. Es necesario que este certificado sea de confianza para todos los clientes.



5. Haga clic en **Aplicar**.



Al aplicar certificados, se reinicia el servicio Mobile Server.

Para obtener más información, es posible que desee ver:

[Vídeo de proceso de Powershell.](#)

[Documento técnico sobre certificados con el servidor móvil.](#)

## Instale certificados de CA comerciales o de terceros para la comunicación con el servidor de administración o el servidor de grabación

Los servidores de administración y los servidores de grabación no requieren certificados de CA comerciales o de terceros de confianza para el cifrado, pero puede optar por usar estos certificados si forma parte de su política de seguridad y las estaciones de trabajo y los servidores cliente confiarán automáticamente en ellos.

El proceso es idéntico a la instalación del certificado de Mobile Server.



Al configurar el cifrado para un grupo de servidores, debe estar habilitado con un certificado que pertenezca al mismo certificado de CA o, si el cifrado está deshabilitado, debe estar deshabilitado en todos los equipos del grupo de servidores.



Los certificados emitidos por CA (Autoridad de Certificación) tienen una cadena de certificados y en la raíz de esa cadena se encuentra el certificado raíz de CA. Cuando un dispositivo o navegador ve este certificado, compara su certificado raíz con los preinstalados en el sistema operativo (Android, iOS, Windows, etc.). Si el certificado raíz aparece en la lista de certificados preinstalados, el sistema operativo garantiza al usuario que la conexión con el servidor es lo suficientemente segura. Estos certificados se emiten para un nombre de dominio y no son gratuitos.

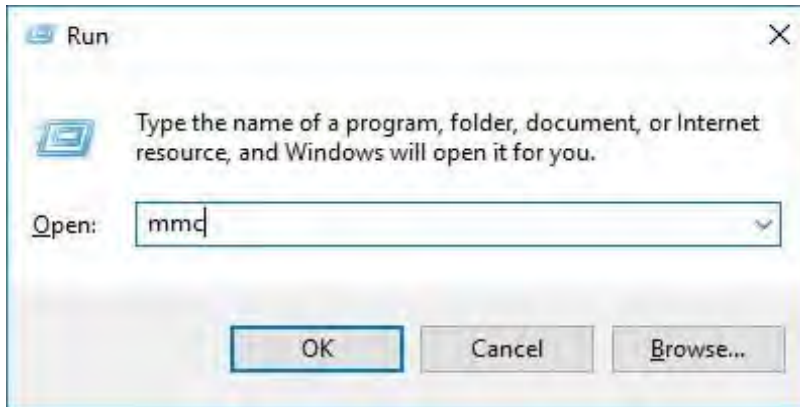
### Agregar un certificado de CA al servidor

Agregue el certificado de CA al servidor haciendo lo siguiente.

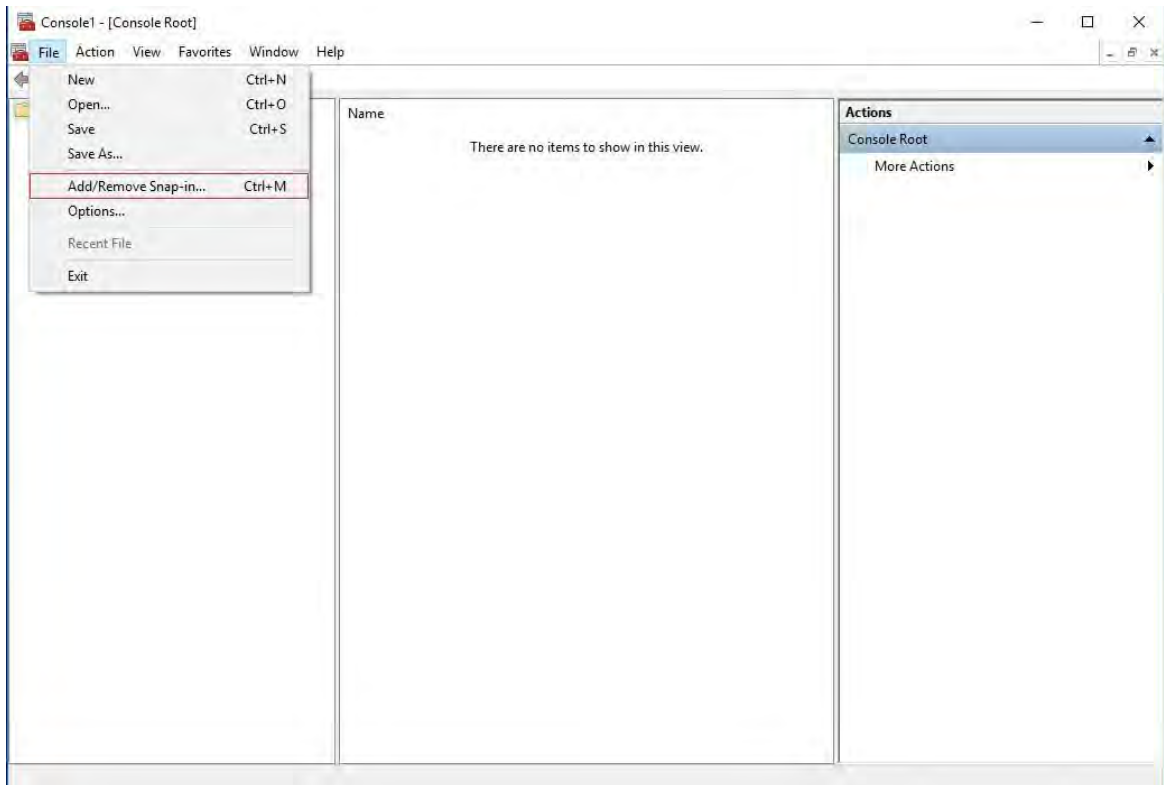


Los parámetros específicos dependen de la CA. Consulte la documentación de su CA antes de continuar.

1. En el ordenador que aloja el servidor MOBOTIX HUB, abra la consola de administración de Microsoft.

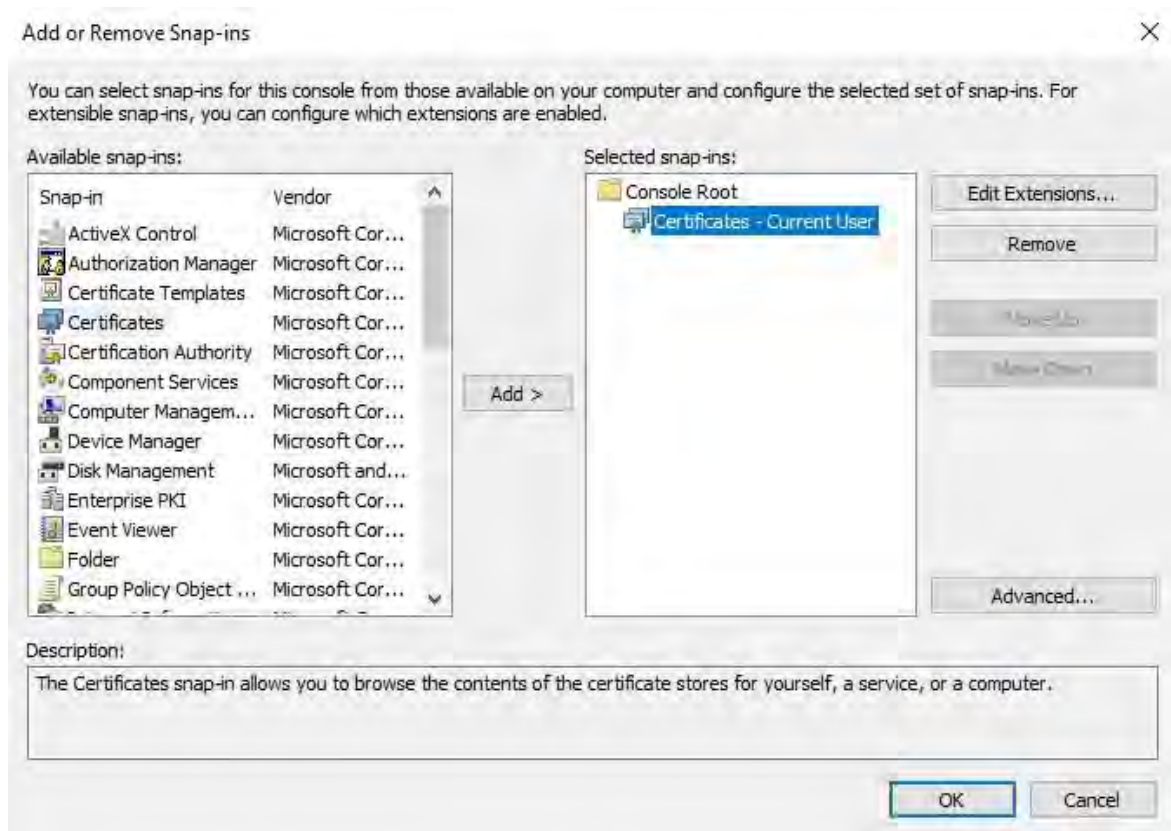


2. En Microsoft Management Console, en el menú **Archivo**, seleccione **Agregar o quitar complemento....**

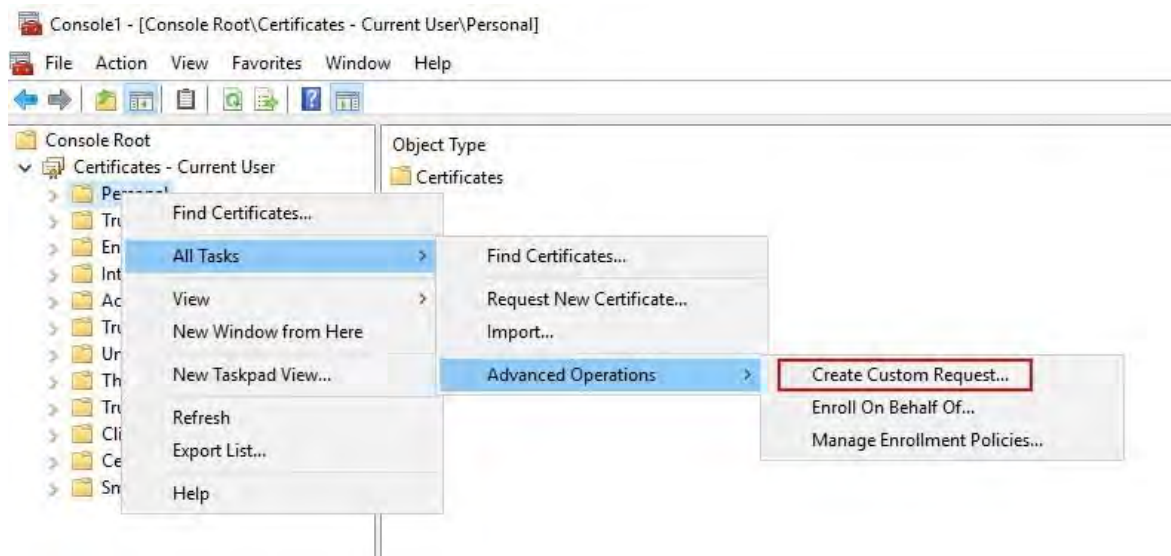


3. Seleccione el **complemento Certificados** y haga clic en **Agregar**.

Haga clic en **Aceptar**.

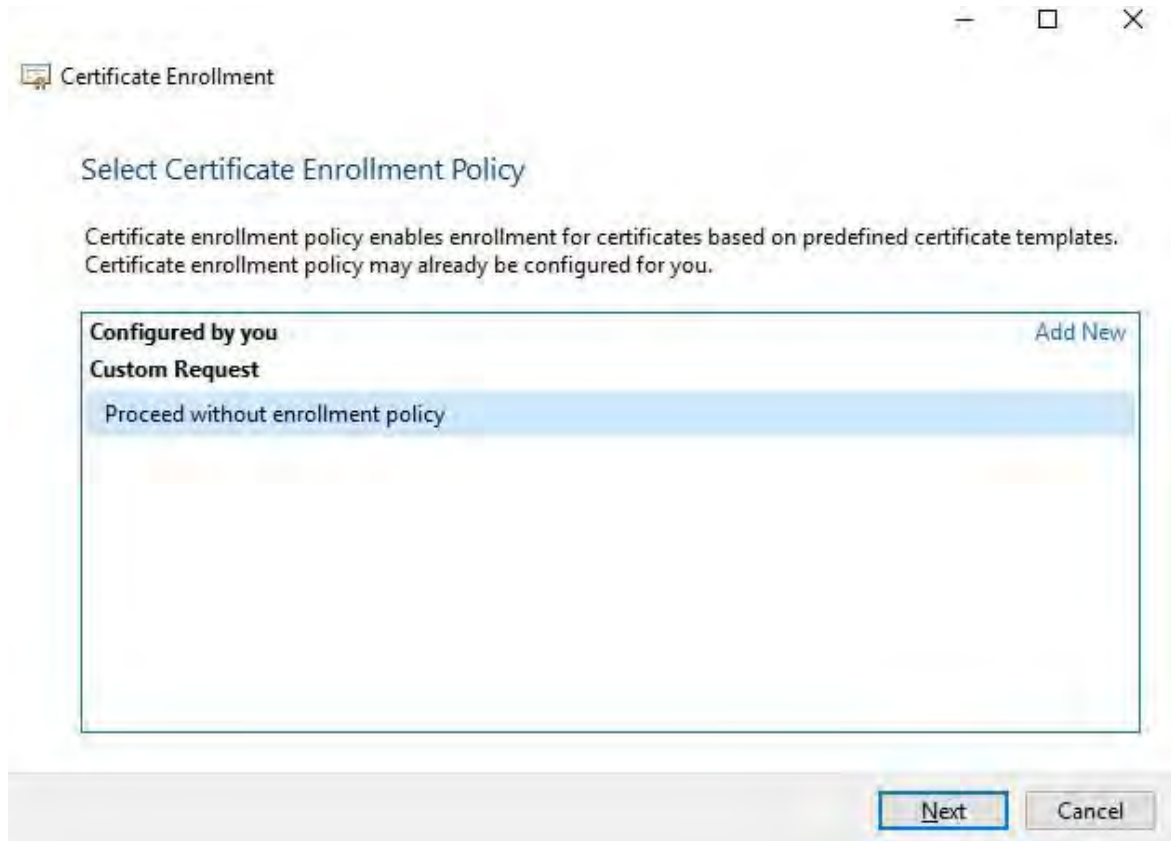


4. Expanda el objeto Certificados. Haga clic con el botón derecho en la **carpeta Personal** y seleccione **Todas las tareas > Operaciones avanzadas > Crear solicitud personalizada**.

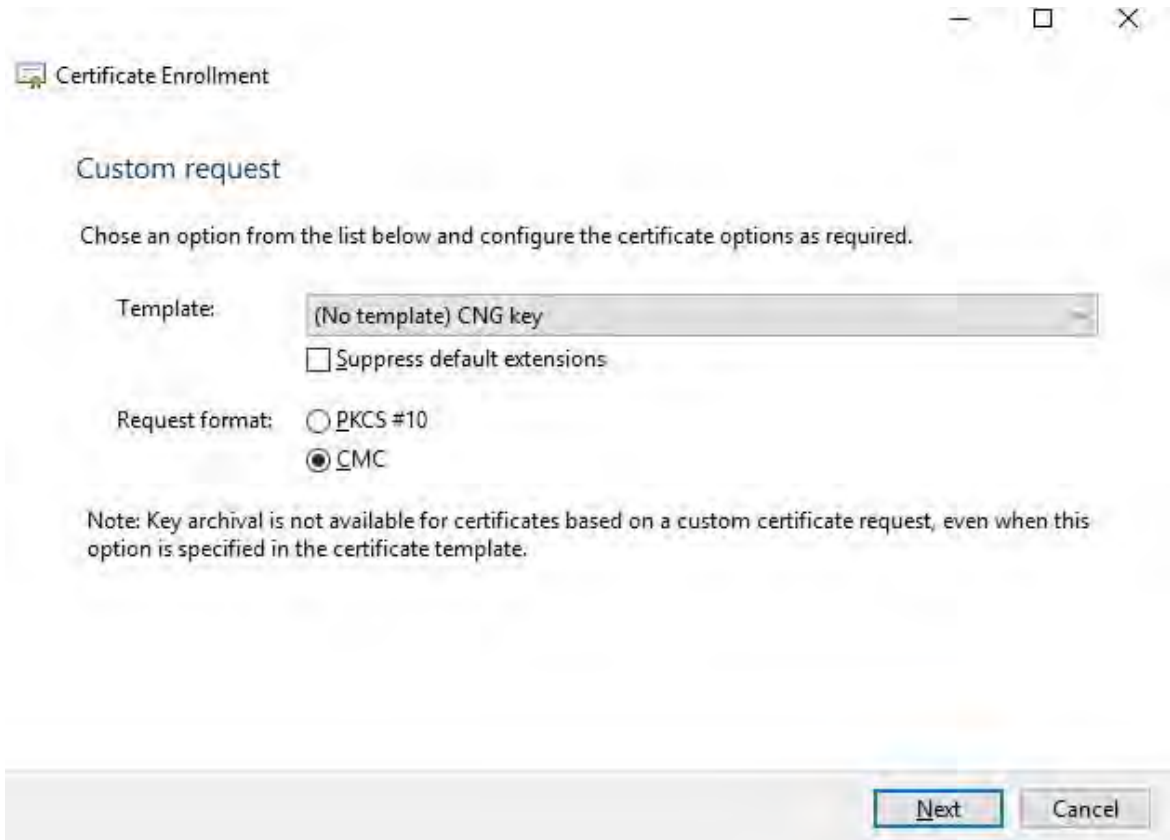



5. Haga clic en **Siguiente** en el Asistente para **inscripción de certificados** y seleccione **Continuar sin directiva de inscripción**.

Haga clic en **Siguiente**.



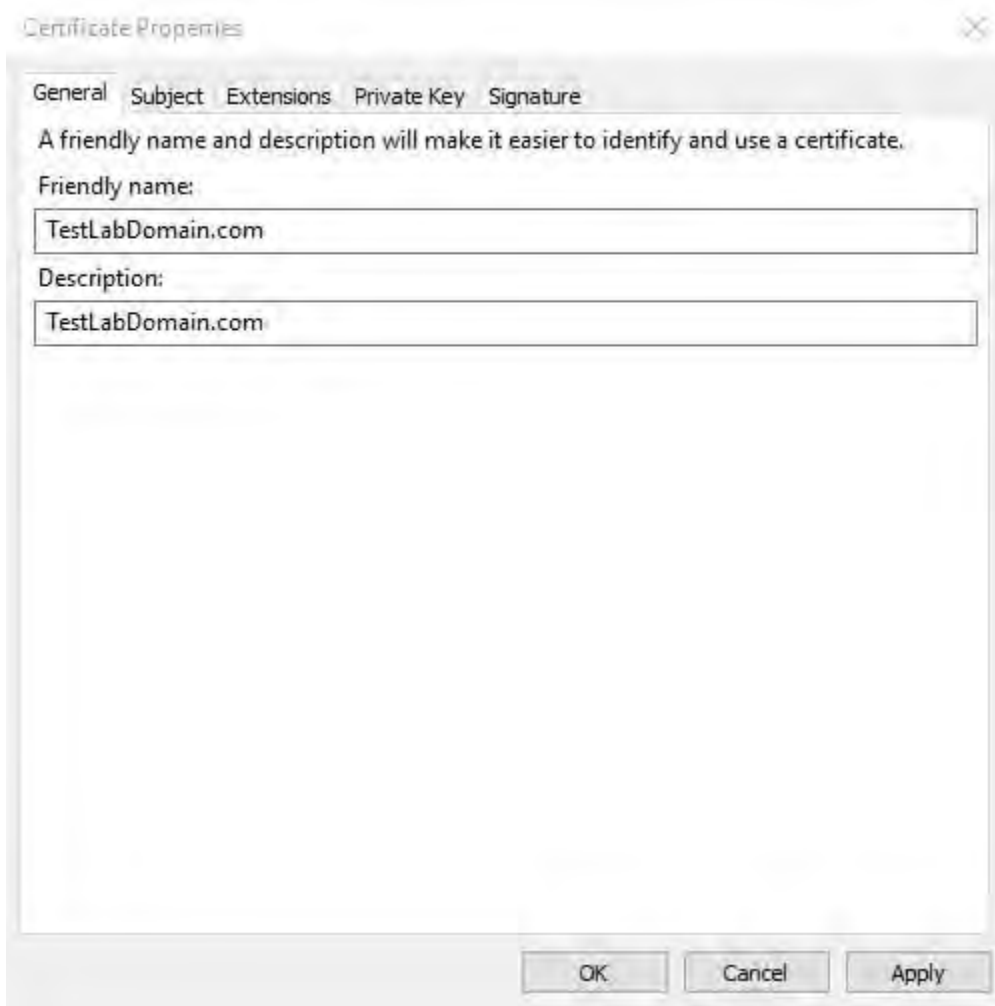
6. Seleccione la plantilla **de clave CNG (sin plantilla)** y el formato de solicitud de **CMC** y haga clic en **Siguiente**.



 El formato de la solicitud depende de la CA. Si se elige el formato incorrecto, la CA emitirá un error cuando se envíe la solicitud de firma de certificado (CSR). Consulte con la CA para asegurarse de que elige correctamente.

7. Expanda para ver los **detalles** de la solicitud personalizada y haga clic en **Propiedades**.

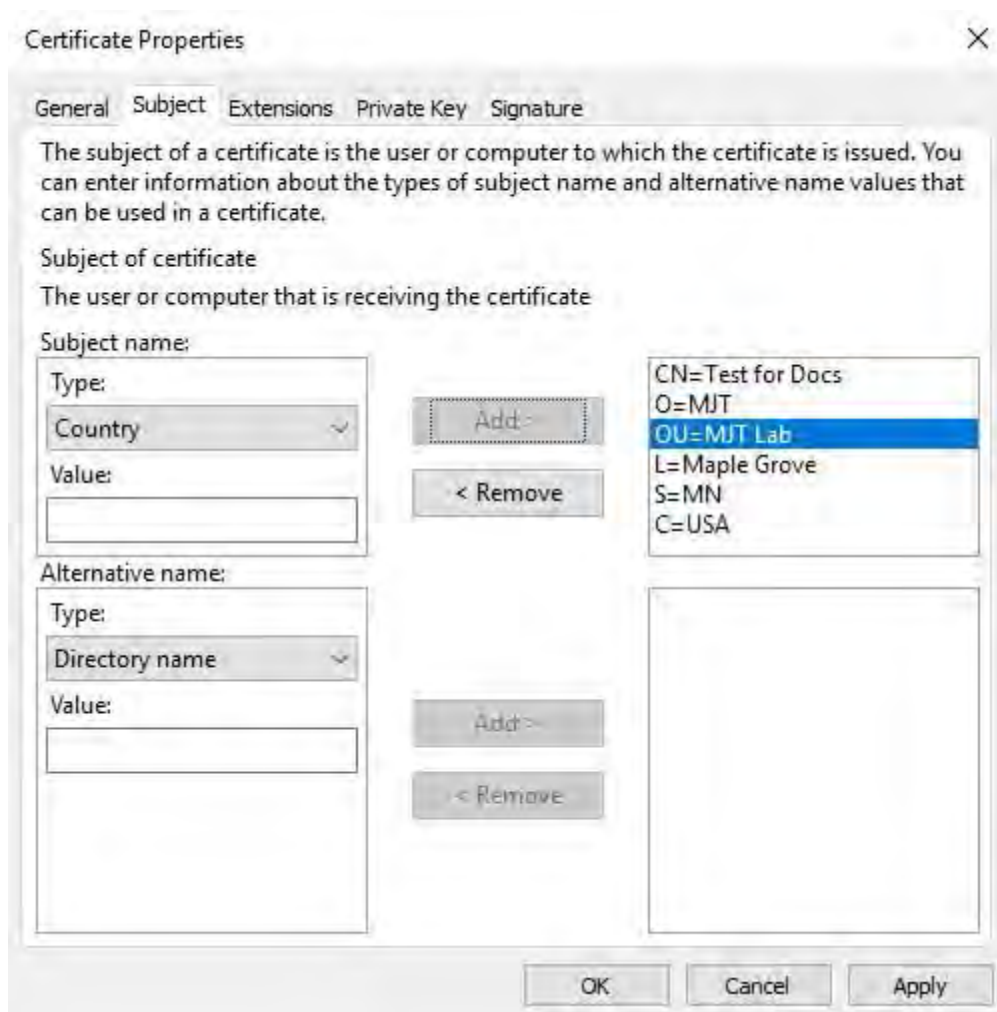
8. En la pestaña **General**, rellene los campos **Nombre descriptivo** y **Descripción** con el nombre de dominio registrado en la CA.



9. En la **pestaña Asunto**, introduzca los parámetros requeridos por la CA específica.

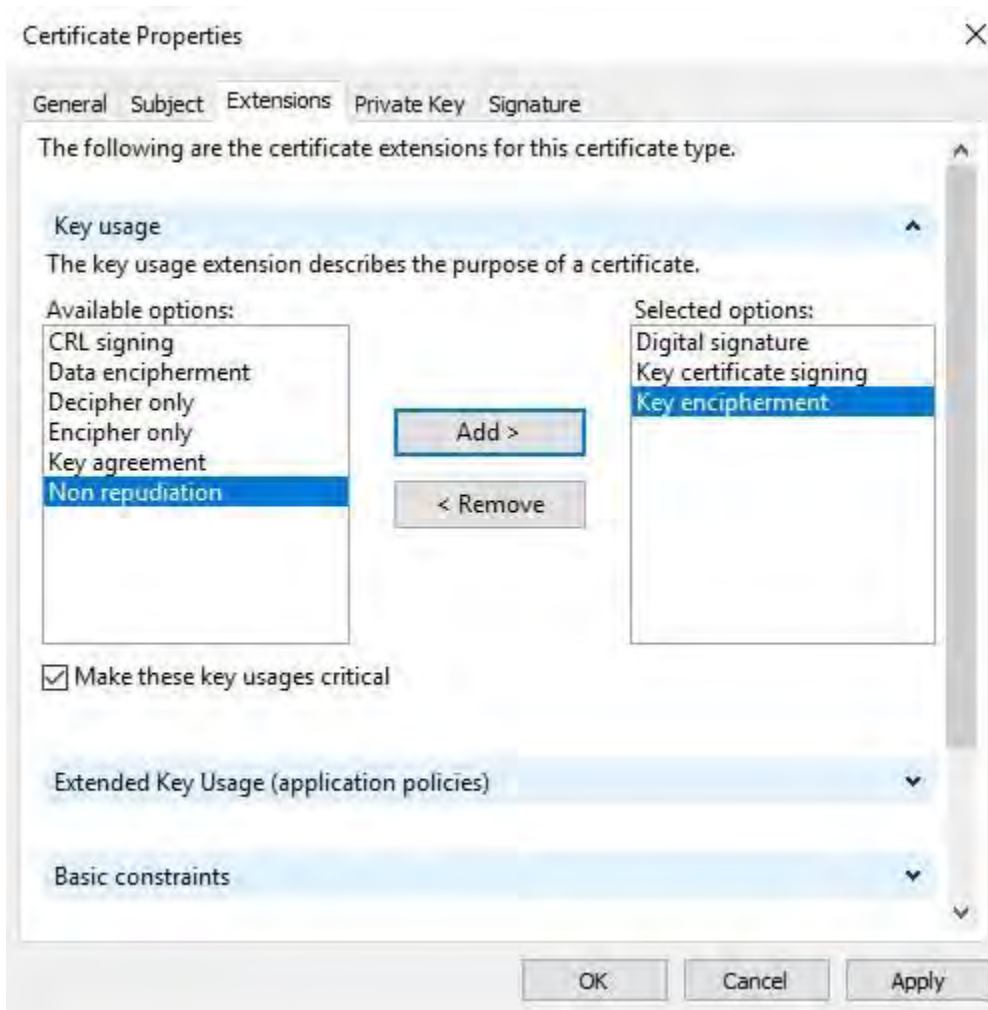
Por ejemplo, el nombre del firmante, el tipo y el **valor** son diferentes para cada CA. Un ejemplo es la siguiente información obligatoria:

- Nombre común:
- Organización:
- Unidad Organizativa :
- Ciudad/Localidad:
- Estado/Provincia:
- País/Región:






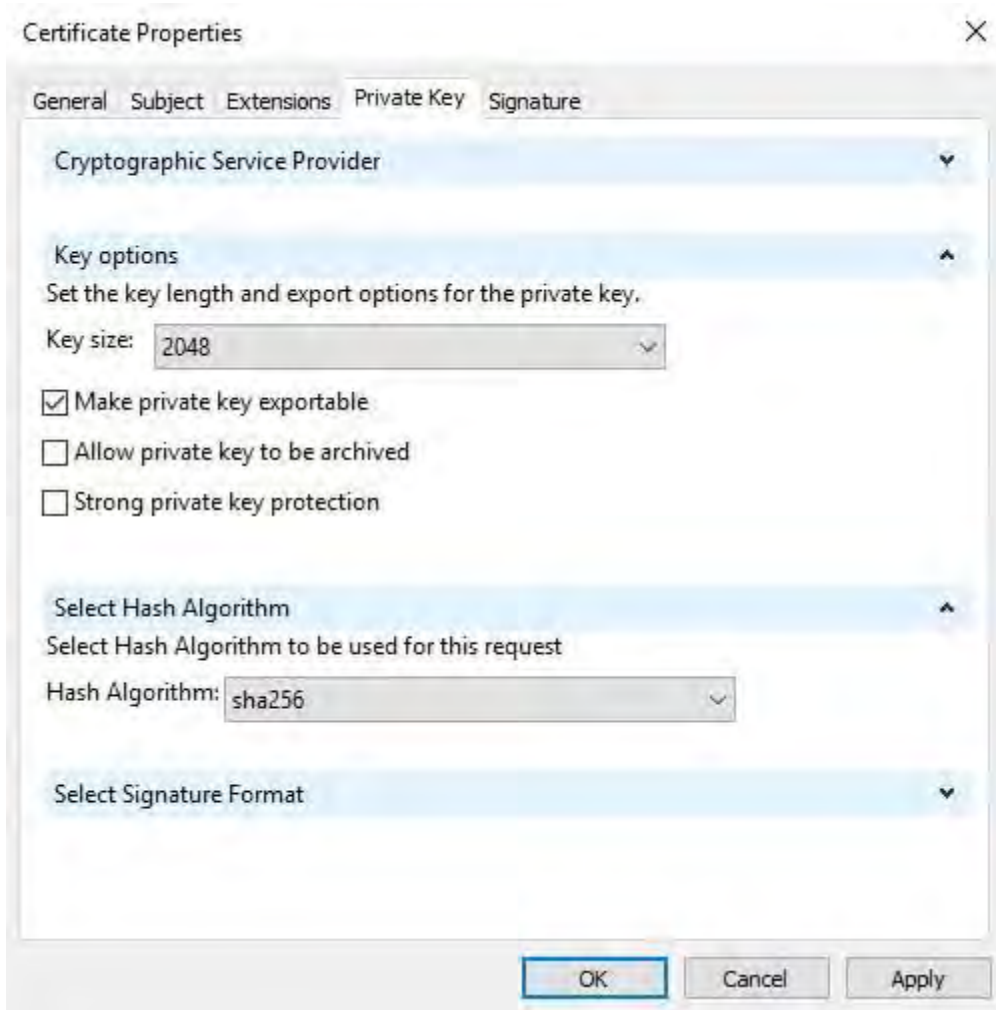
10. Algunas CA no requieren extensiones. Sin embargo, si es necesario, vaya a la **pestaña Extensiones** y expanda el menú Uso de **claves** . Agregue las opciones necesarias de la lista de **opciones disponibles** a la lista de **opciones seleccionadas**.



11. En la pestaña **Clave privada**, expanda el menú **Opciones de clave**.

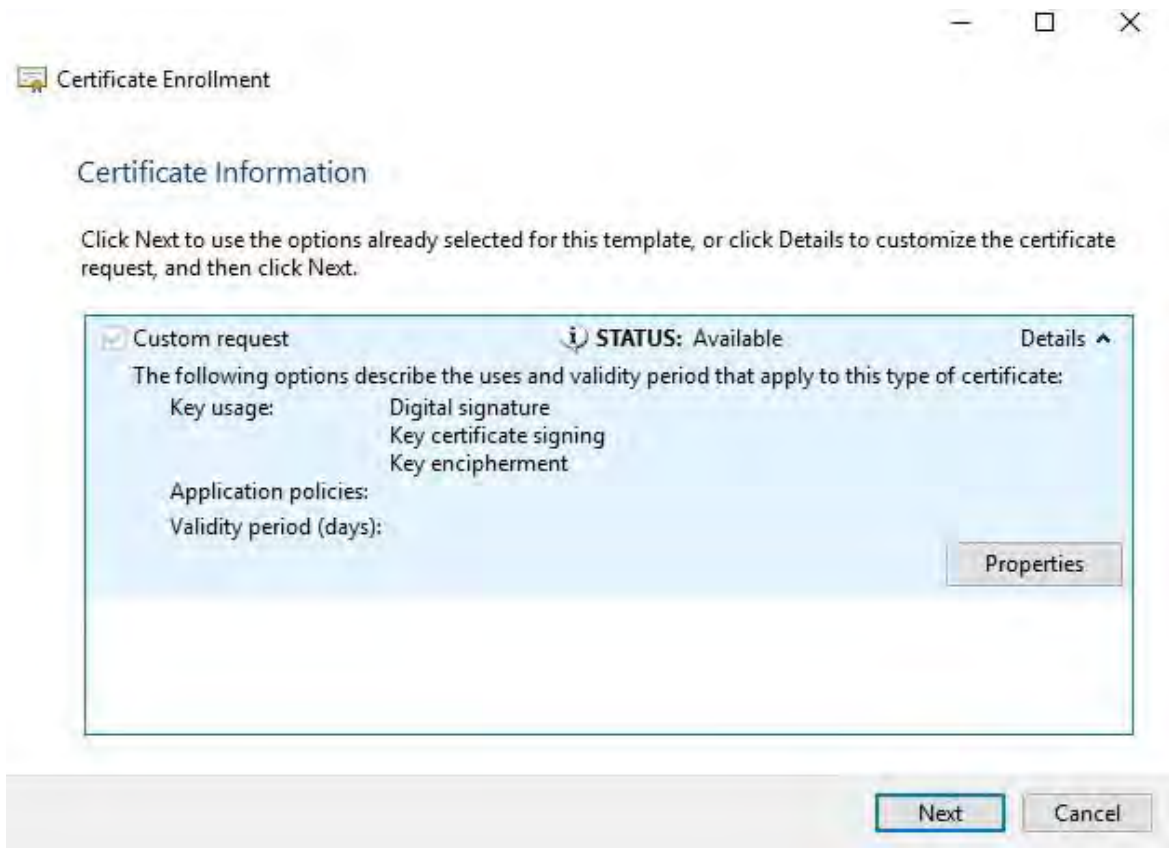
Establezca el tamaño de la clave en 2048 y seleccione la opción para que la clave privada sea exportable.

 La variable de tamaño de clave está determinada por la CA, por lo tanto, es posible que se requiera una clave de tamaño mayor. También pueden ser necesarias otras opciones, como un algoritmo hash específico (sha256). Ajuste todas las opciones necesarias antes de continuar con el siguiente paso.



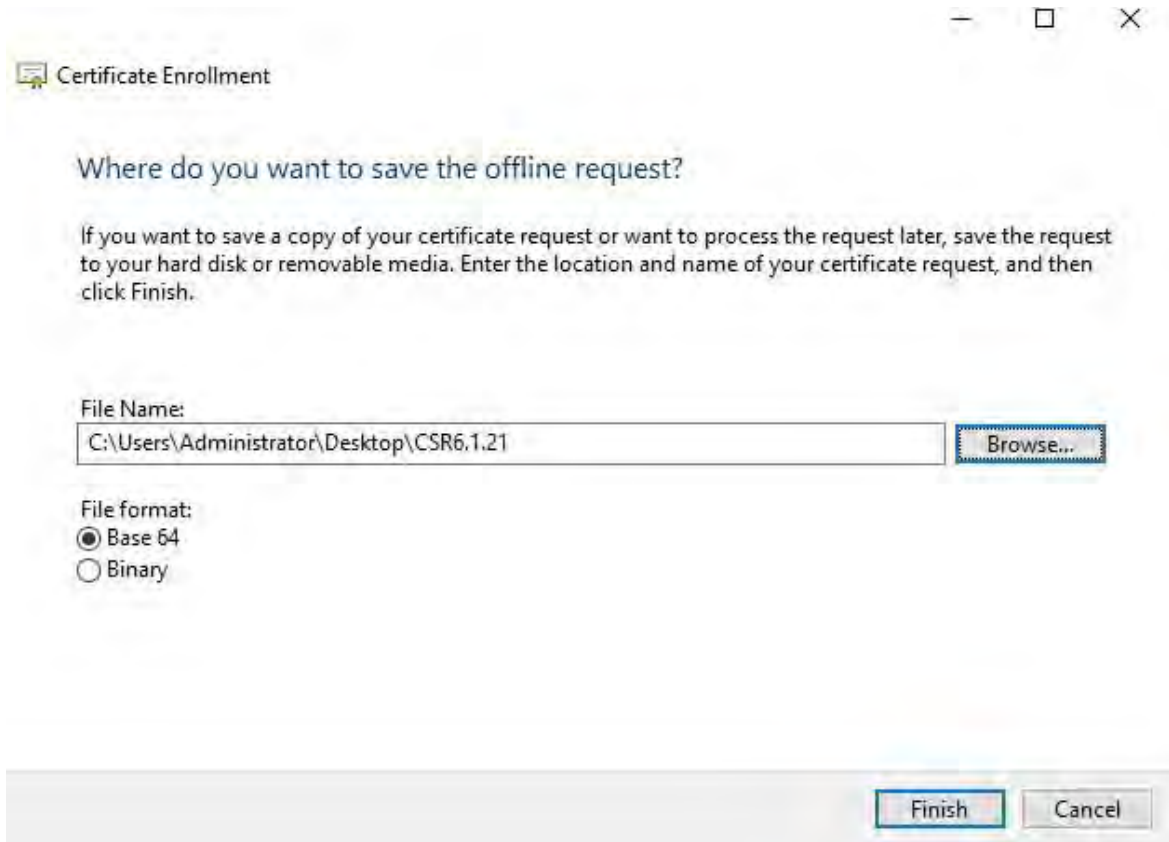
12. A menos que la CA requiera una firma, el siguiente paso es hacer clic en **Aceptar**.

13. Cuando se hayan definido todas las propiedades del certificado, haga clic **en Siguiente** en la inscripción de **certificados** hechicero.



14. Seleccione una ubicación para guardar la solicitud de certificado y un formato. Vaya a esa ubicación y especifique un nombre para el archivo .req. El formato predeterminado es base 64, sin embargo, algunas CA requieren el formato binario.

15. Haga clic en **Finalizar**.



Se genera un archivo .req, que debe utilizar para solicitar un certificado firmado.

### Cargue el archivo .req para recibir un certificado firmado a cambio



Cada CA tiene un proceso diferente para cargar archivos .req con el fin de recibir un certificado firmado a cambio. Consulte la documentación de la CA para obtener información sobre cómo recuperar un certificado firmado.

En la mayoría de las situaciones de CA de terceros, es necesario descargar un archivo .ZIP y extraer el contenido en el ordenador que aloja el servidor MOBOTIX HUB.

Hay varios tipos de archivos que se pueden incluir en el contenido del archivo .ZIP extraído.

. CER o . CRT. Los archivos CRT se pueden instalar mediante un proceso similar. Haga clic con el botón derecho en el archivo y elija **Instalar certificado** en el menú contextual.

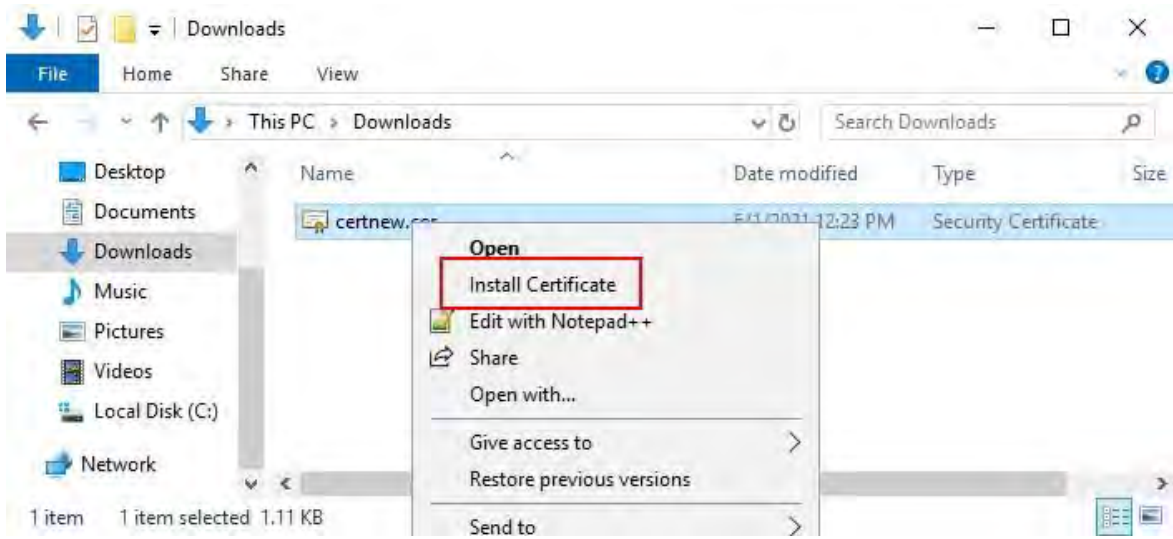
En los siguientes pasos se utiliza un archivo . CER de una CA interna.

La CA necesitará el contenido del archivo .req. Se le pedirá que copie todo el texto del archivo .req, incluidas las líneas inicial y final, y que pegue el texto en un campo disponible en un portal administrado por la CA.

1. Vaya a la ubicación del archivo .req, ábralo en el Bloc de notas y pegue el texto en un campo disponible en un portal administrado por su CA.



2. Cuando reciba el certificado de su CA, vaya a la carpeta de descargas (o a cualquier lugar que elija para almacenar la carpeta en el equipo), haga clic con el botón derecho en el certificado y seleccione **Instalar certificado**.

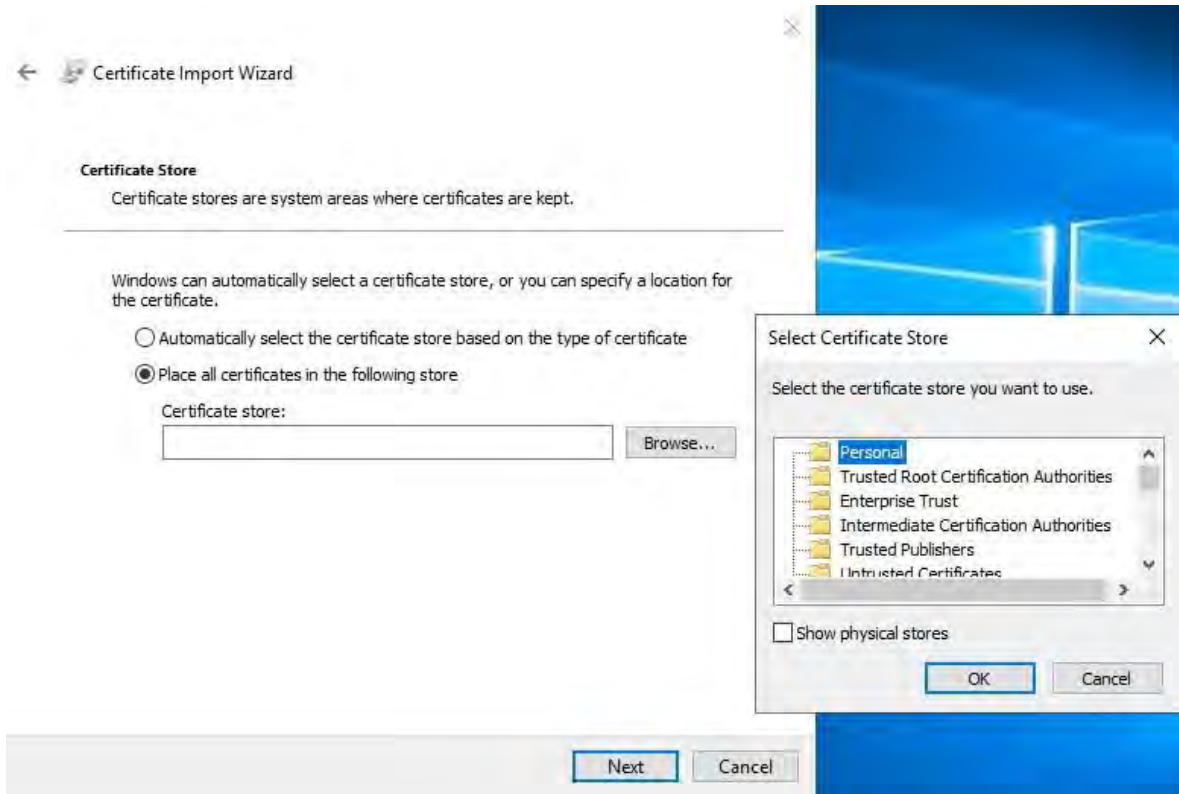


3. Acepte la advertencia de seguridad si aparece.

Seleccione instalar el certificado para el equipo local y haga clic en **Siguiente**.



4. Elija una ubicación de almacenamiento, vaya al almacén de certificados personales y haga clic en **Siguiente**.



5. Finalice el asistente **para instalar certificado**.

### Habilitar el cifrado hacia y desde el servidor de administración

Puede cifrar la conexión bidireccional entre el servidor de administración y el recopilador de datos afiliado cuando tenga un servidor remoto del siguiente tipo:

- Servidor de grabación
- Servidor de eventos
- Servidor de registro
- Servidor LPR
- Servidor móvil

Si su sistema contiene varios servidores de grabación o servidores remotos, debe habilitar el cifrado en todos ellos.



Al configurar el cifrado para un grupo de servidores, debe estar habilitado con un certificado que pertenezca al mismo certificado de CA o, si el cifrado está deshabilitado, debe estar deshabilitado en todos los equipos del grupo de servidores.



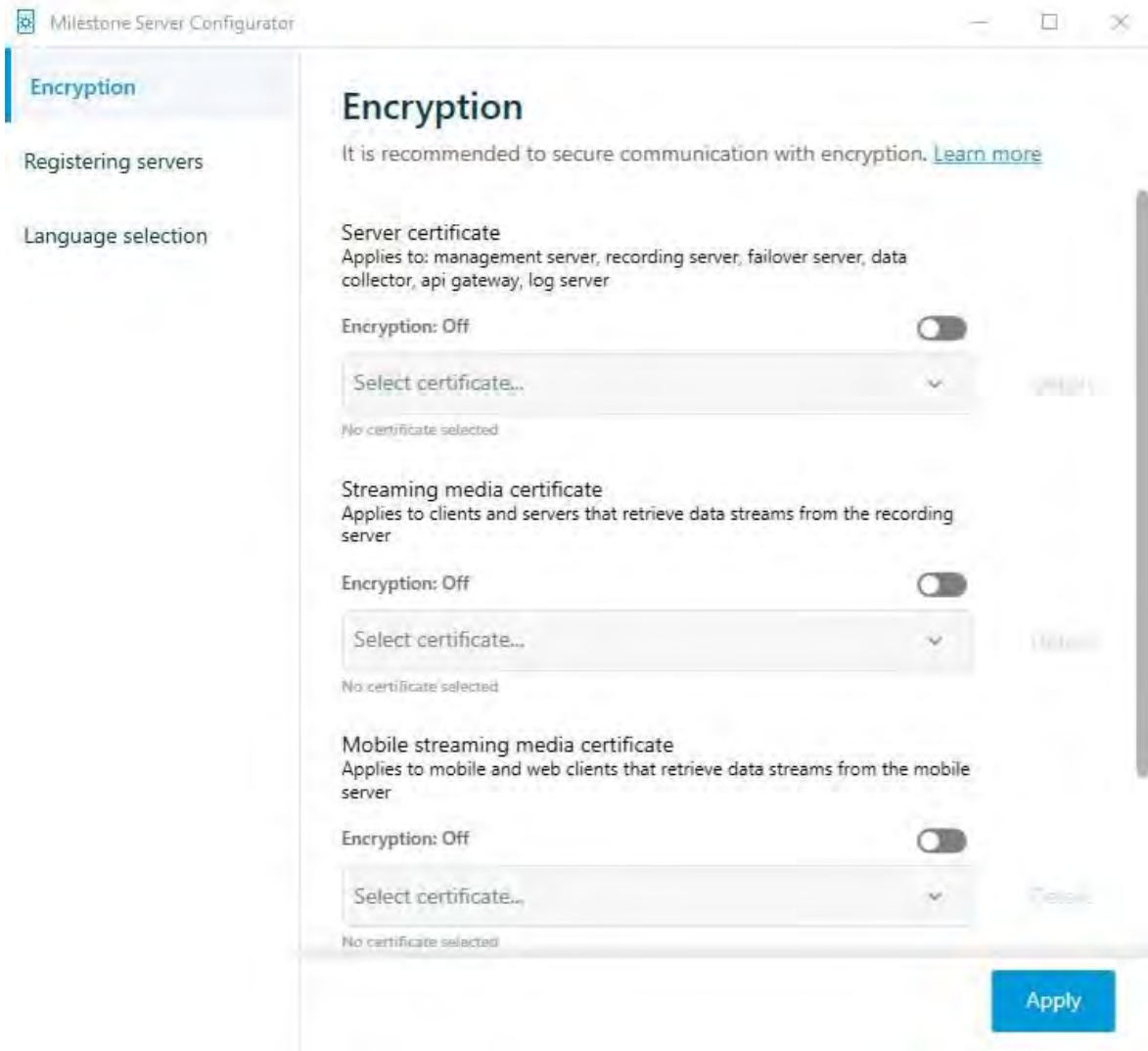
**Prerrequisitos:**

- Un certificado de autenticación de servidor es de confianza en el equipo que hospeda el servidor de administración. En primer lugar, habilite el cifrado en el servidor de administración.

**Pasos:**

1. En un equipo con un servidor de administración instalado, abra el **Configurador de servidores** desde:
  - El menú Inicio de Windows
  - o
  - El Administrador del servidor de administración haciendo clic con el botón derecho en el icono del Administrador del servidor de administración en la barra de tareas del equipo
2. En Server **Configurator**, en **Certificado de servidor**, active **Cifrado**.
3. Haga clic en **Seleccionar certificado** para abrir una lista con los nombres de los firmantes únicos de los certificados que tienen una clave privada y que están instalados en el equipo local en el Almacén de certificados de Windows.
4. Seleccione un certificado para cifrar la comunicación entre el servidor de grabación, el servidor de administración, el servidor de conmutación por error y el servidor del recopilador de datos.

Seleccione **Detalles** para ver la información del Almacén de certificados de Windows sobre el certificado seleccionado.



5. Haga clic en **Aplicar**.

Para completar la habilitación del cifrado, el siguiente paso es actualizar la configuración de cifrado en cada servidor de grabación y en cada servidor que tenga un recopilador de datos (servidor de eventos, servidor de registros, servidor LPR y servidor móvil).

## Instalación de Servicios de certificados de Active Directory

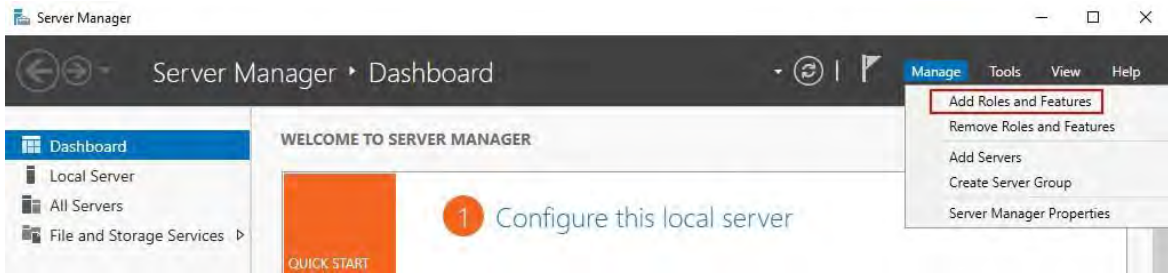
Servicios de certificados de Active Directory (AD CS) es un producto de Microsoft que realiza la funcionalidad de infraestructura de clave pública (PKI). Actúa como un rol de servidor que le permite construir una infraestructura de clave pública (PKI) y proporcionar criptografía de clave abierta, autenticación computarizada y capacidades de marcado avanzadas para su asociación.

En este documento, AD CS se utiliza al instalar certificados:

- En un entorno de dominio (consulte [Instalación de certificados en un dominio para la comunicación con el servidor de administración o el servidor de grabación en la página 86](#))
- En un entorno de grupo de trabajo (consulte [Instalación de certificados en un entorno de grupo de trabajo para la comunicación con el servidor de gestión o el servidor de grabación en la página 104](#))

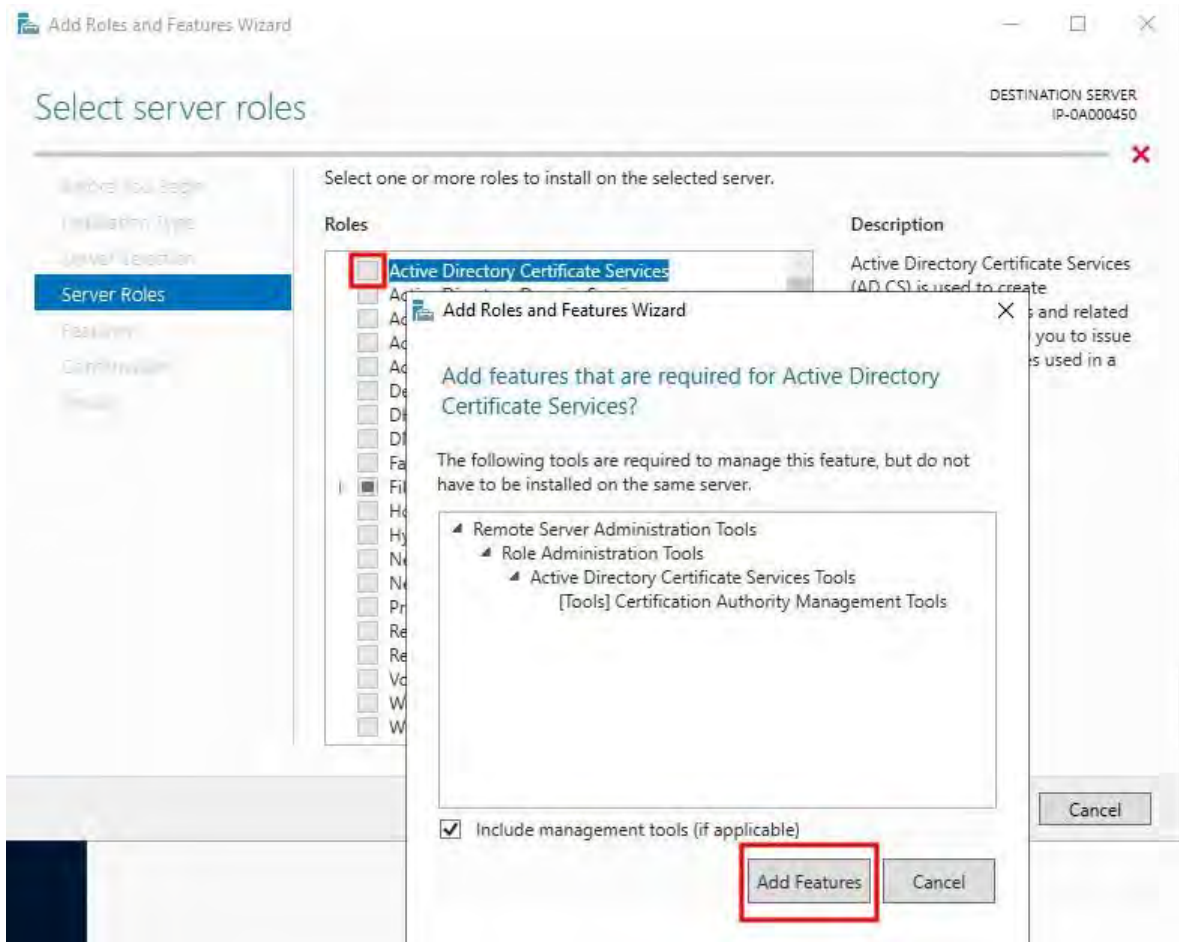
Para instalar AD CS:

1. En la aplicación **Administrador del servidor**, seleccione **Administrar > Agregar roles y características**.



2. En **Antes de comenzar**, haga clic en **Siguiente**.
3. En **Tipo de instalación**, seleccione **Instalación basada en roles o en características** y haga clic en **Siguiente**.
4. En **Selección de servidor**, seleccione el servidor local como destino para la instalación y haga clic en **Siguiente**.

5. En **Roles de servidor**, seleccione el rol **Servicios de certificados de Active Directory**. Revise la lista de características para instalar y haga clic en **Agregar características**.



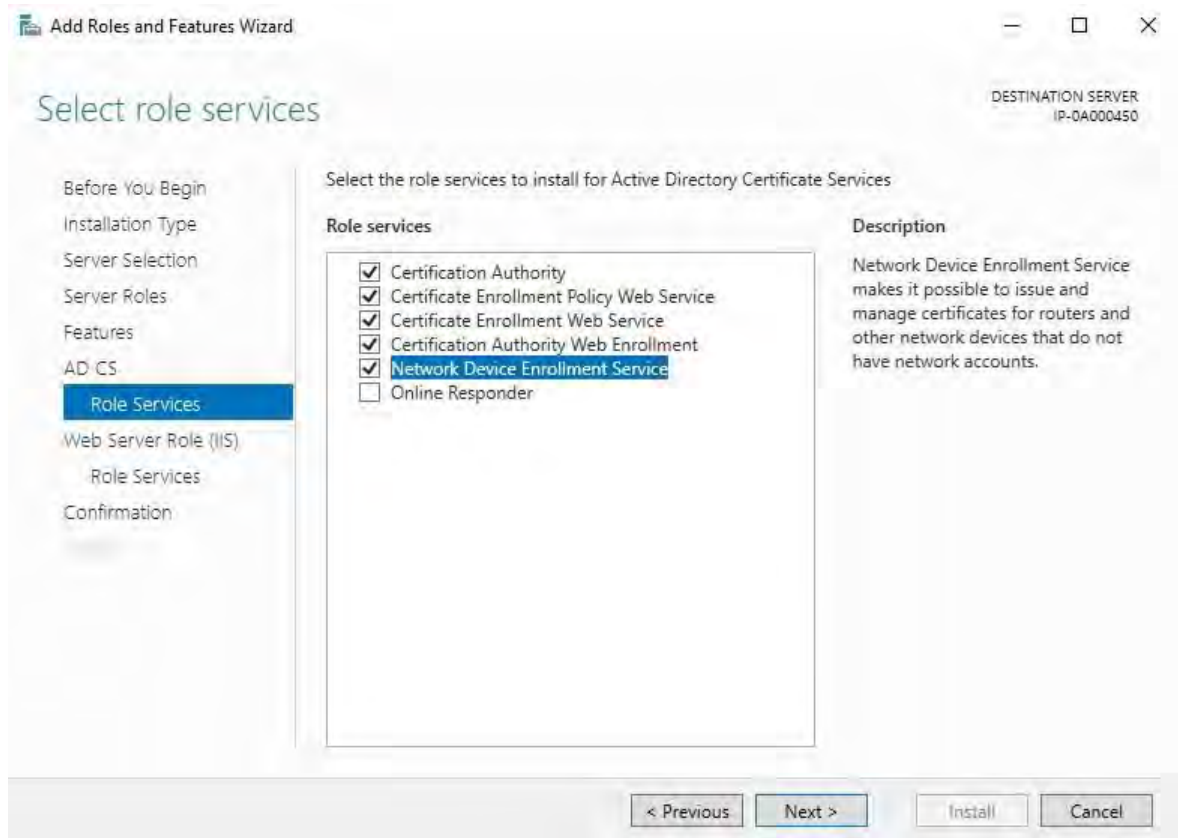
Haga clic en **Siguiente**.

6. En **Características**, haga clic en **Siguiente**. Se seleccionan todas las funciones necesarias para la instalación.
7. En **AD CS**, lea la descripción de los servicios certificados de Active Directory y haga clic en **Siguiente**.

8. En Servicios de rol, seleccione lo siguiente:

- **Autoridad de Certificación**
- **Servicio web de política de inscripción de certificación**
- **Servicio web de inscripción de certificación**
- **Inscripción web de la autoridad de certificación**
- **Servicio de inscripción de dispositivos de red**

Al seleccionar cada uno de los servicios de rol, agregue las características necesarias para admitir la instalación de cada servicio.

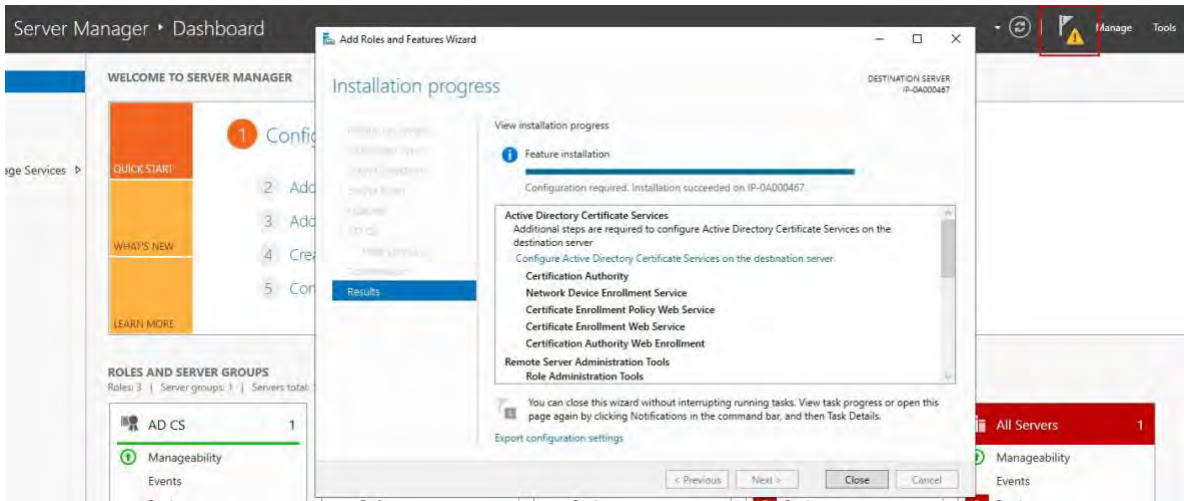


Haga clic en **Siguiente**.

9. En **Confirmación**, seleccione **Reiniciar el servidor de destino automáticamente si es necesario** y haga clic en **Instalar**.

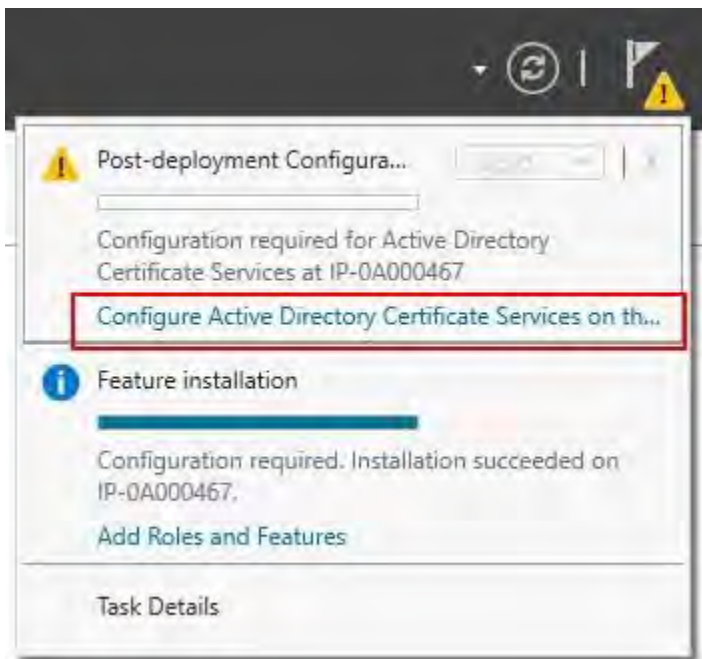
10. Una vez finalizada la instalación, haga clic en el **botón Cerrar**.

Seleccione la **marca de notificación** en la aplicación **Administrador del servidor**.



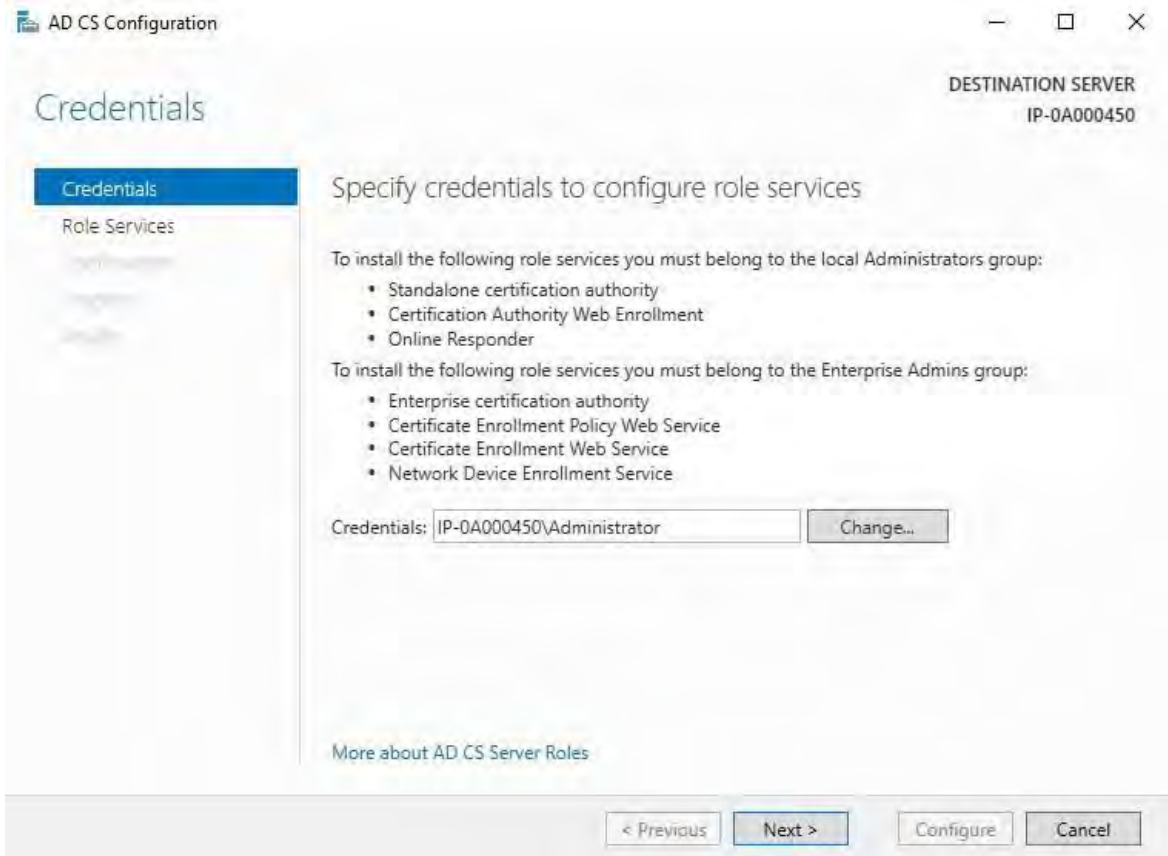
11. Un mensaje para comenzar la configuración posterior a la implementación se muestra debajo de la **marca de notificación**.

Haga clic en el enlace para comenzar la configuración de los servicios instalados.



12. Se inicia el Asistente para la configuración **de Servicios de Certificate Services de Active Directory**.

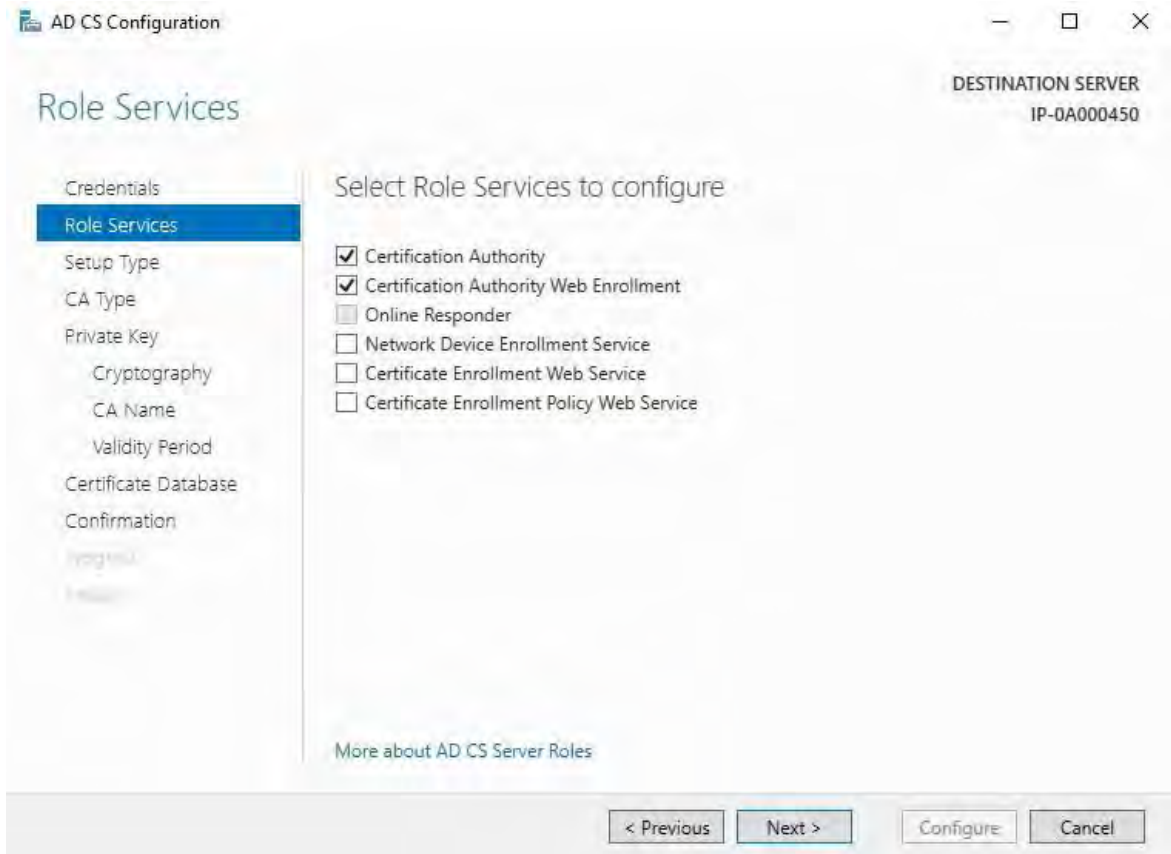
En **Credenciales**, seleccione la cuenta de usuario necesaria para ejecutar los servicios instalados. Como se indica en el texto, se requiere ser miembro de los grupos de administrador local y administrador de empresa. Ingrese la información de cuenta requerida y haga clic en **Siguiente**.



13. En **Servicios de rol**, seleccione los siguientes servicios:

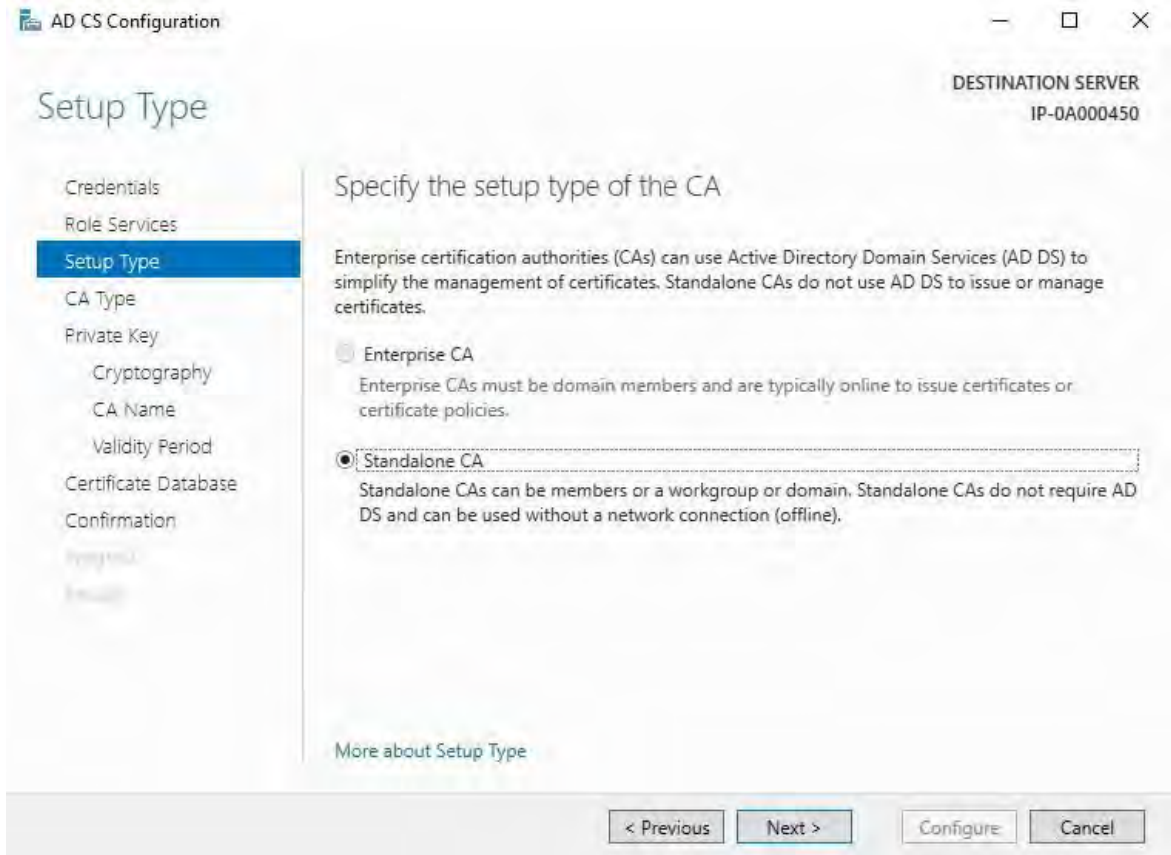
- **Autoridad de Certificación**
- **Inscripción web de la autoridad de certificación**

Haga clic en **Siguiente**.

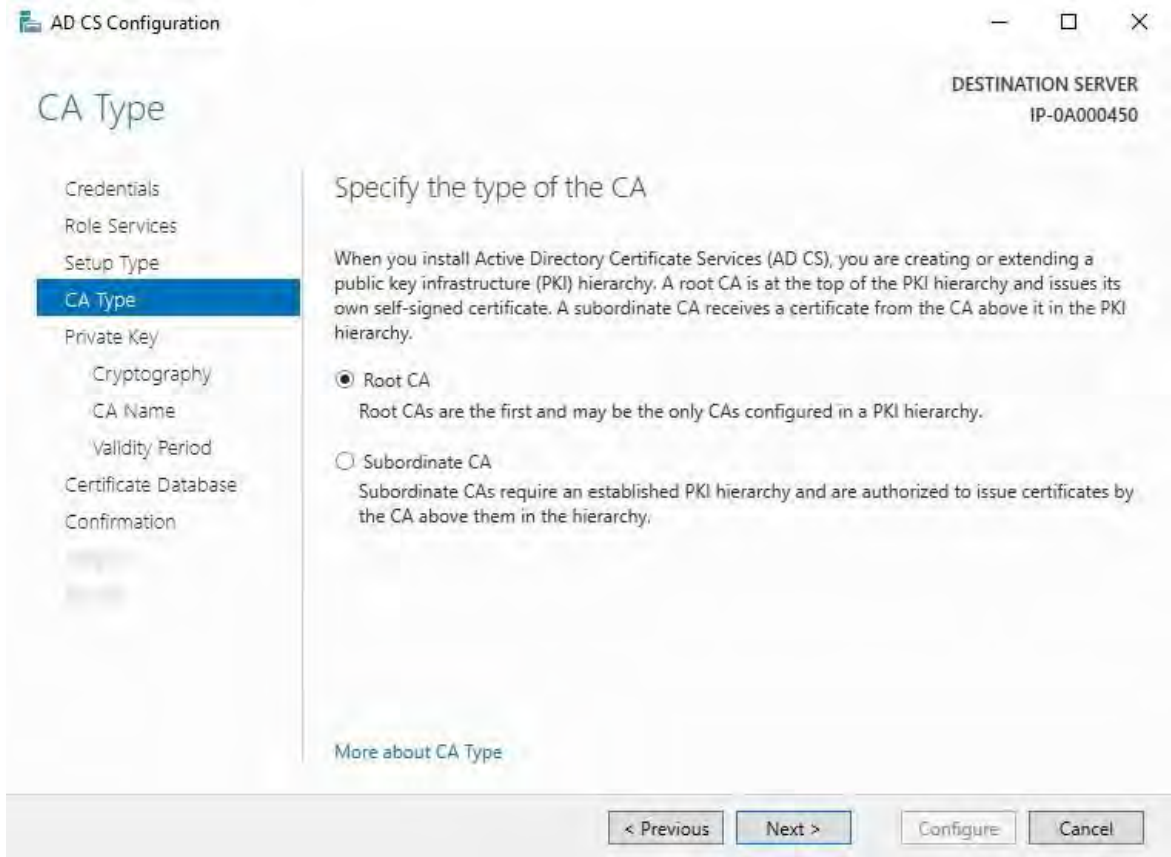




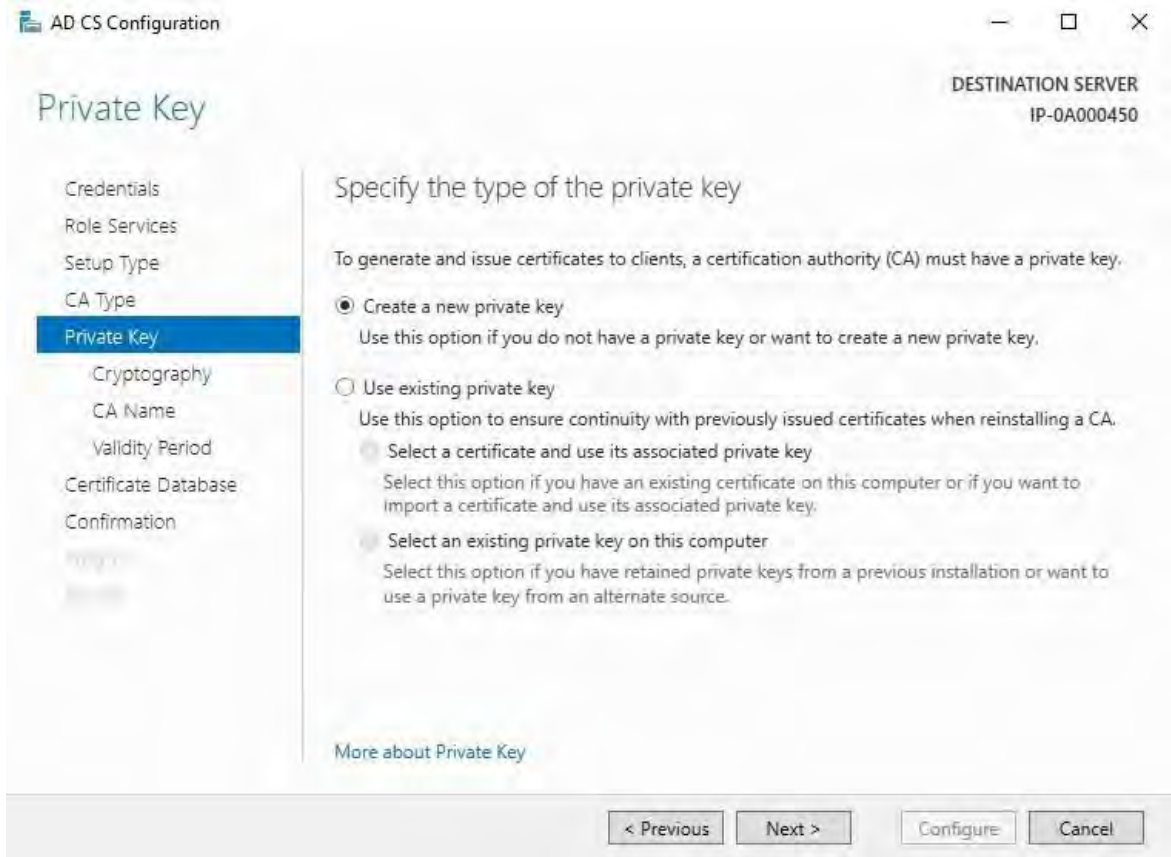
14. En **Tipo de configuración**, seleccione la opción **CA independiente** y haga clic en **Siguiente**.



15. En **Tipo** de CA, seleccione la opción para instalar una **CA raíz** y haga clic en **Siguiente**.

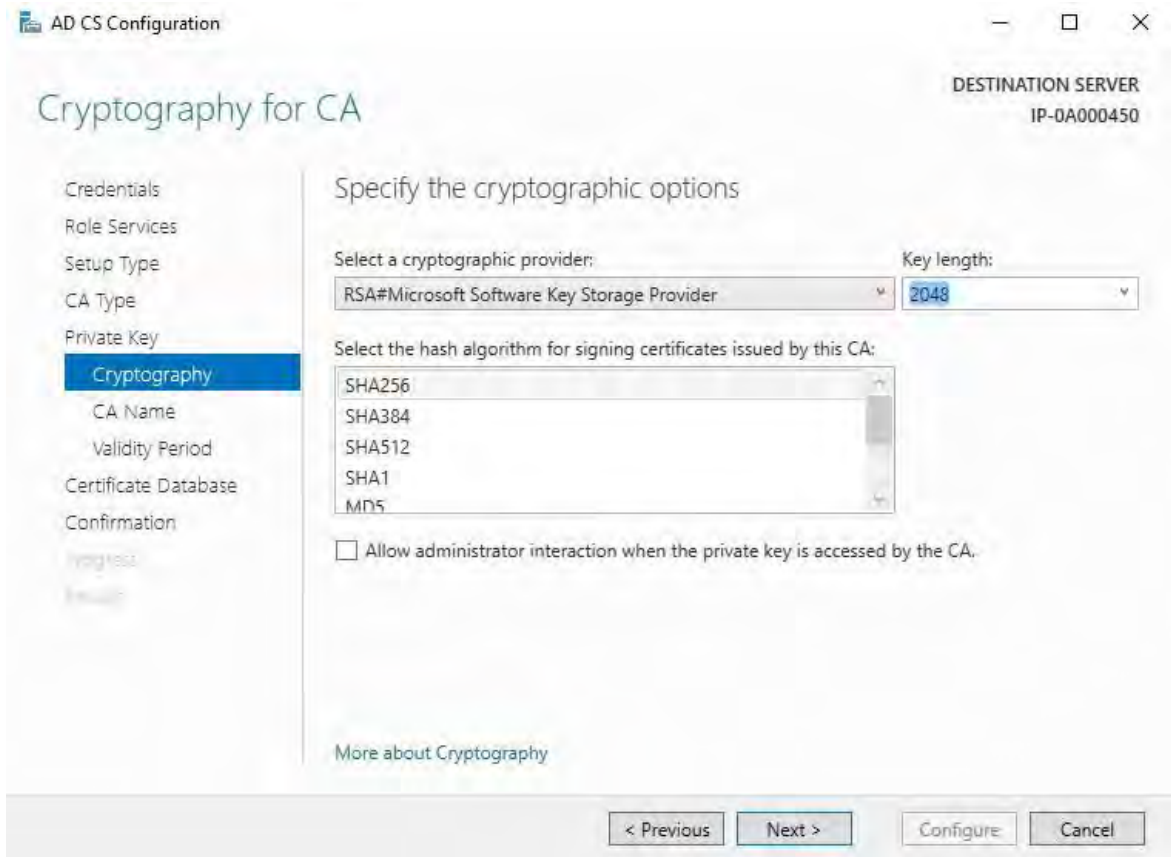


16. En **Clave privada**, seleccione la opción para crear una nueva clave privada y haga clic en **Siguiente**.



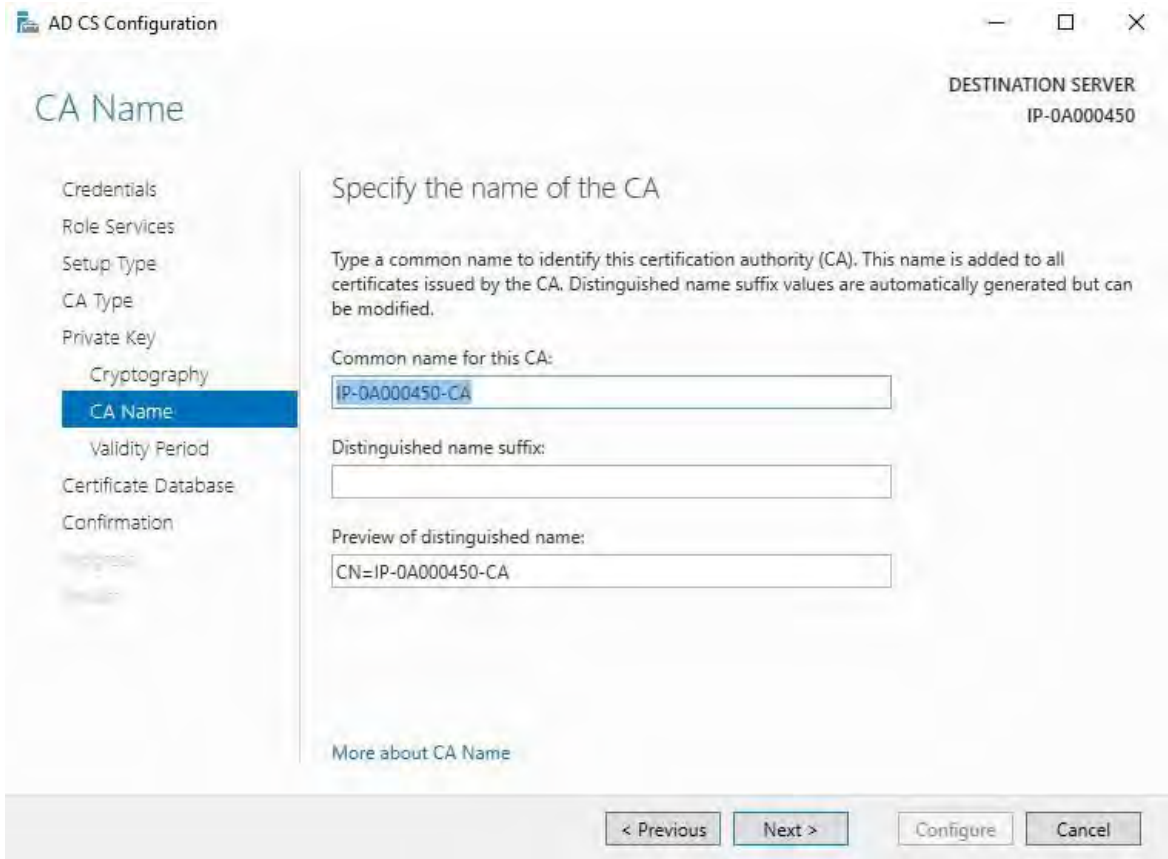
17. En **Criptografía**, seleccione **RSA#Proveedor de almacenamiento de claves de software de Microsoft** para la opción de proveedor criptográfico con una **longitud de clave** de 2048 y un algoritmo hash de SHA256.

Haga clic en **Siguiente**.

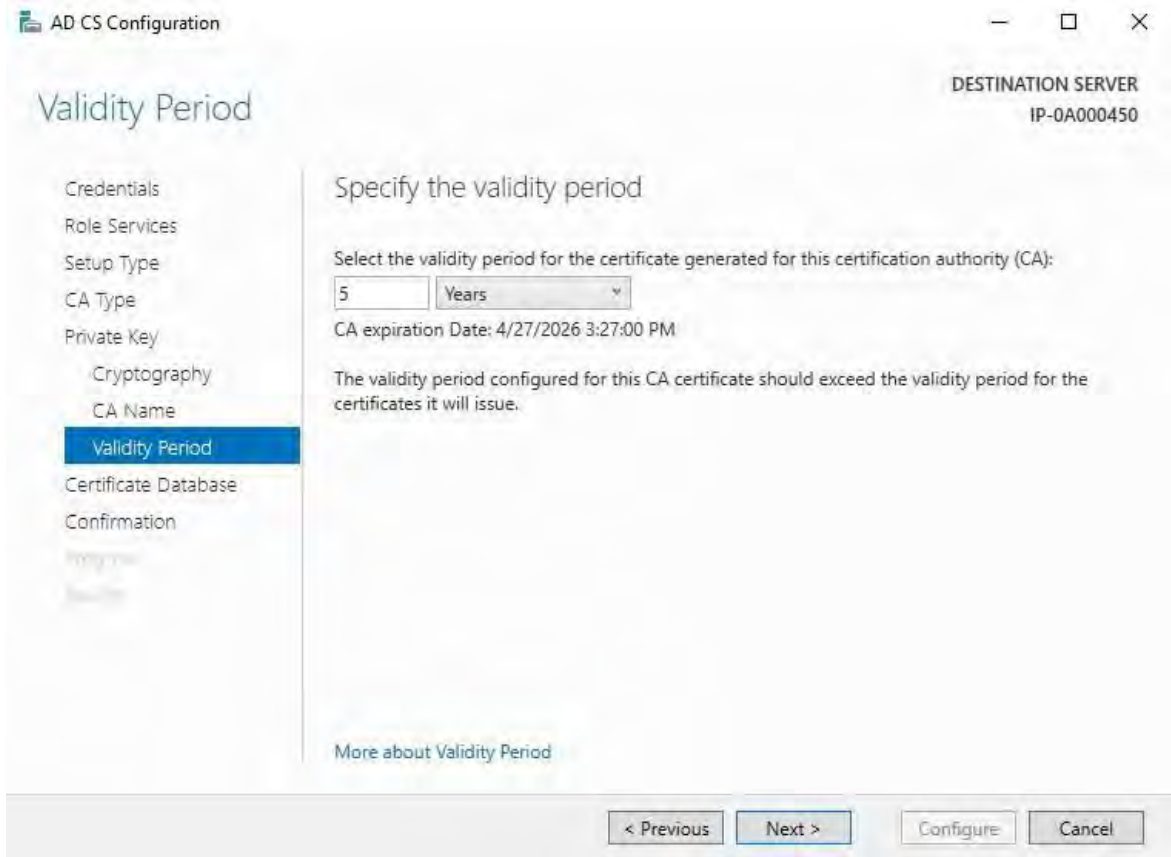


18. En **Nombre** de la CA, escriba el nombre de la CA y haga clic en **Siguiente**.

De forma predeterminada, el nombre es "localhost-CA", suponiendo que el nombre del equipo del servidor local es "localhost".



19. En **Período de validez**, seleccione el período de validez predeterminado de 5 años y haga clic en **Siguiente**.



20. En **Base de datos** de certificados, introduzca las ubicaciones de la base de datos y la base de datos de registros. Las ubicaciones de base de datos predeterminadas para el almacén de certificados son: `C:\Windows\system32\CertLog`. Haga clic en **Siguiente**.
21. En **Confirmación**, revise las opciones de configuración seleccionadas y haga clic en **Configurar** para comenzar el proceso de configuración.
22. Una vez finalizada la configuración, haga clic en **Cerrar**. Cuando se le solicite que configure cualquier servicio de rol adicional, haga clic en **No**.
23. Reinicie el servidor local para asegurarse de que está listo para servir como servidor de certificados de Active Directory.

## Instalar certificados en un dominio para la comunicación con el servidor de administración o el servidor de grabación

Cuando todos los puntos de conexión de cliente y servidor funcionan dentro de un entorno de dominio, no es necesario distribuir certificados de CA a las estaciones de trabajo cliente. La directiva de grupo dentro del dominio controla la distribución automática de todos los certificados de CA de confianza a todos los usuarios y equipos del dominio.

Esto se debe a que, al instalar una CA raíz empresarial, usa la directiva de grupo para propagar su certificado al almacén de certificados de entidades de certificación raíz de confianza para todos los usuarios y equipos del dominio.

Debe ser un administrador de dominio o un administrador con acceso de escritura a Active Directory para instalar una CA raíz empresarial.

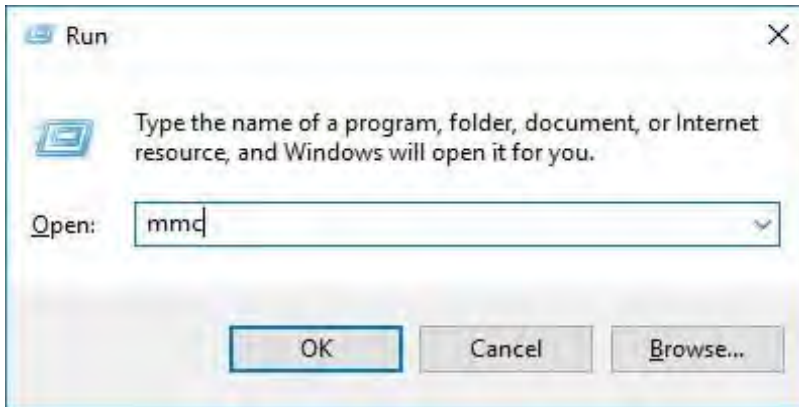


Microsoft proporciona una amplia documentación para los sistemas operativos Windows Server, que incluye plantillas para certificados de servidor, la instalación de la CA y la implementación de certificados que se pueden encontrar en [la descripción general de la implementación de certificados de servidor de Microsoft](#).

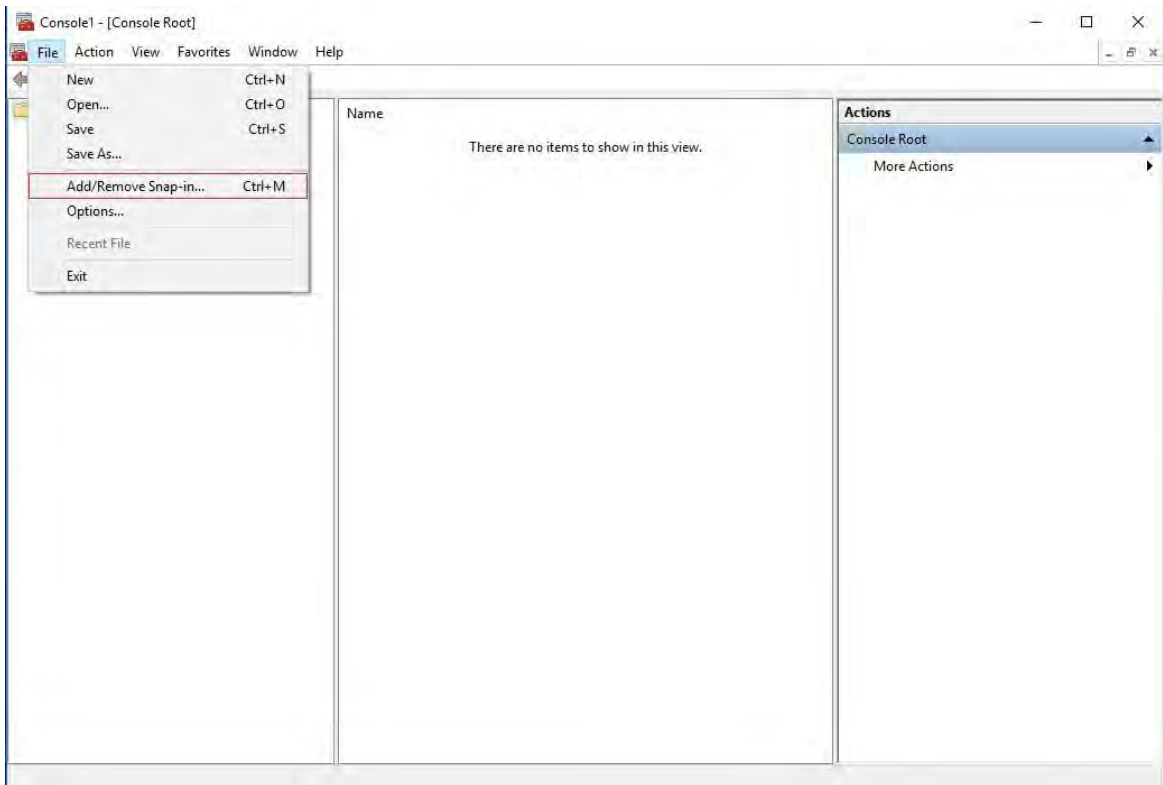
### Agregar un certificado de CA al servidor

Agregue el certificado de CA al servidor haciendo lo siguiente.

1. En el ordenador que aloja el servidor MOBOTIX HUB, abra la consola de administración de Microsoft.

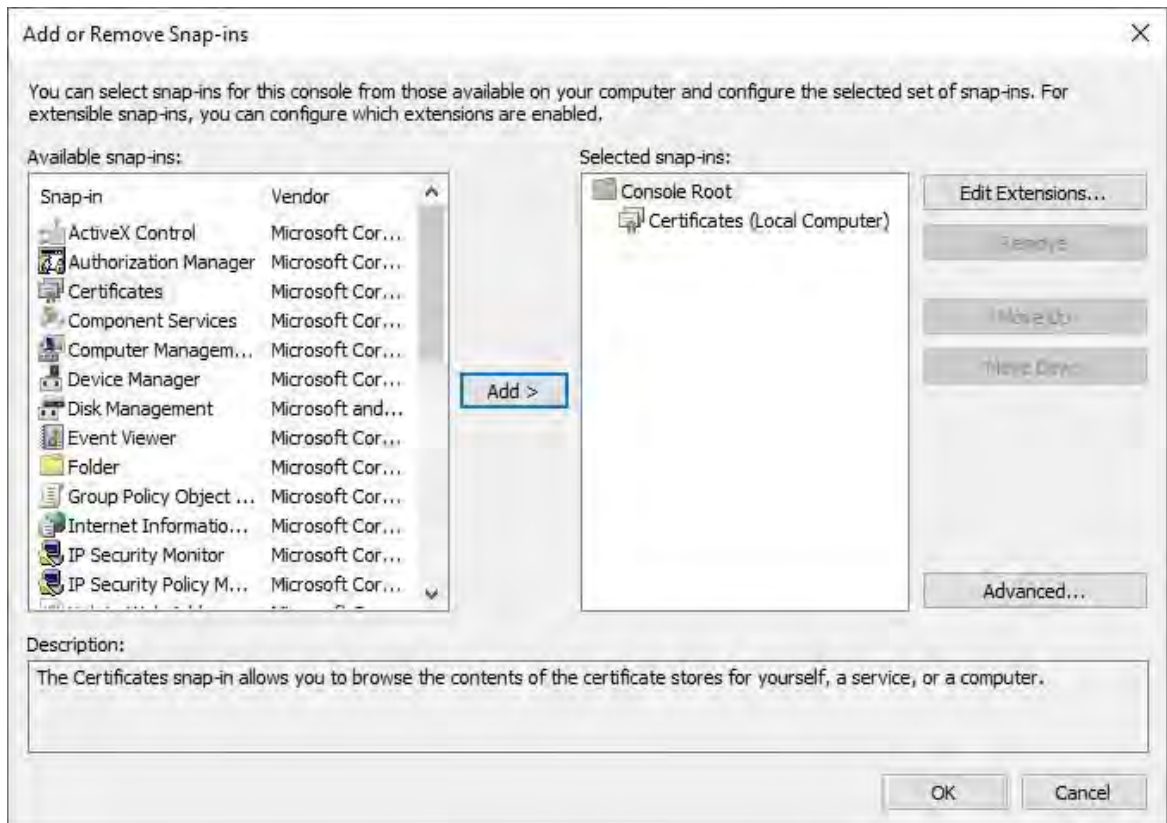


2. En Microsoft Management Console, en el menú **Archivo**, seleccione **Agregar o quitar complemento....**

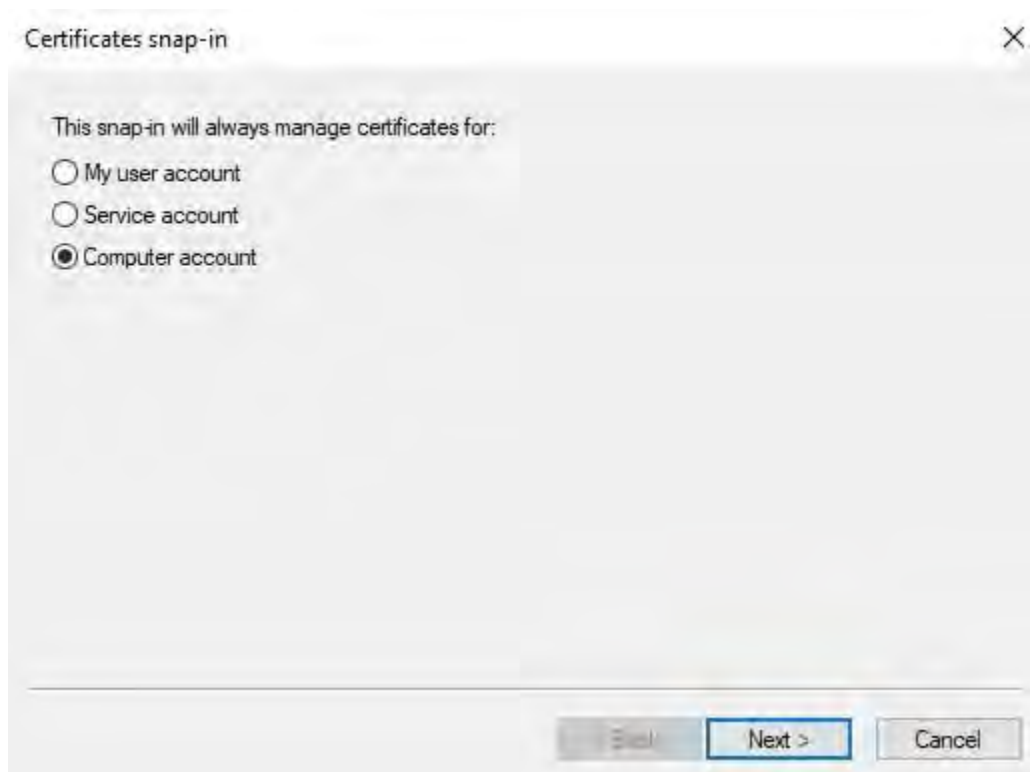




3. Seleccione el **complemento Certificados** y haga clic en **Agregar**

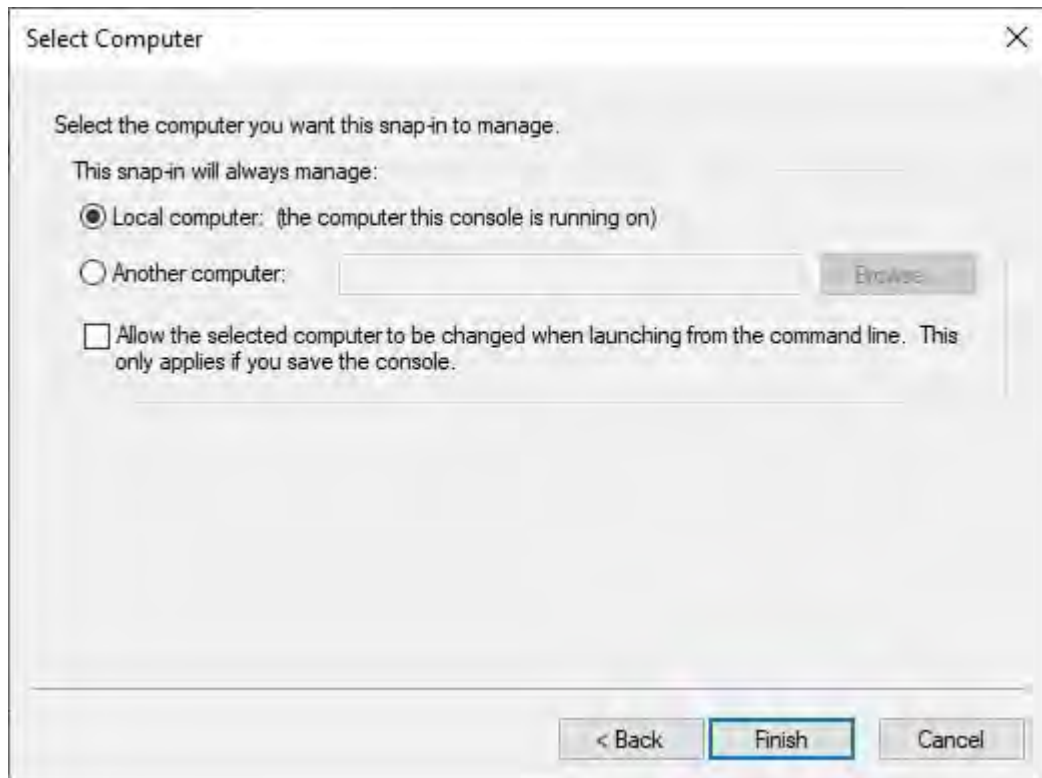


4. En el complemento **Certificados**, seleccione **Cuenta de equipo**.

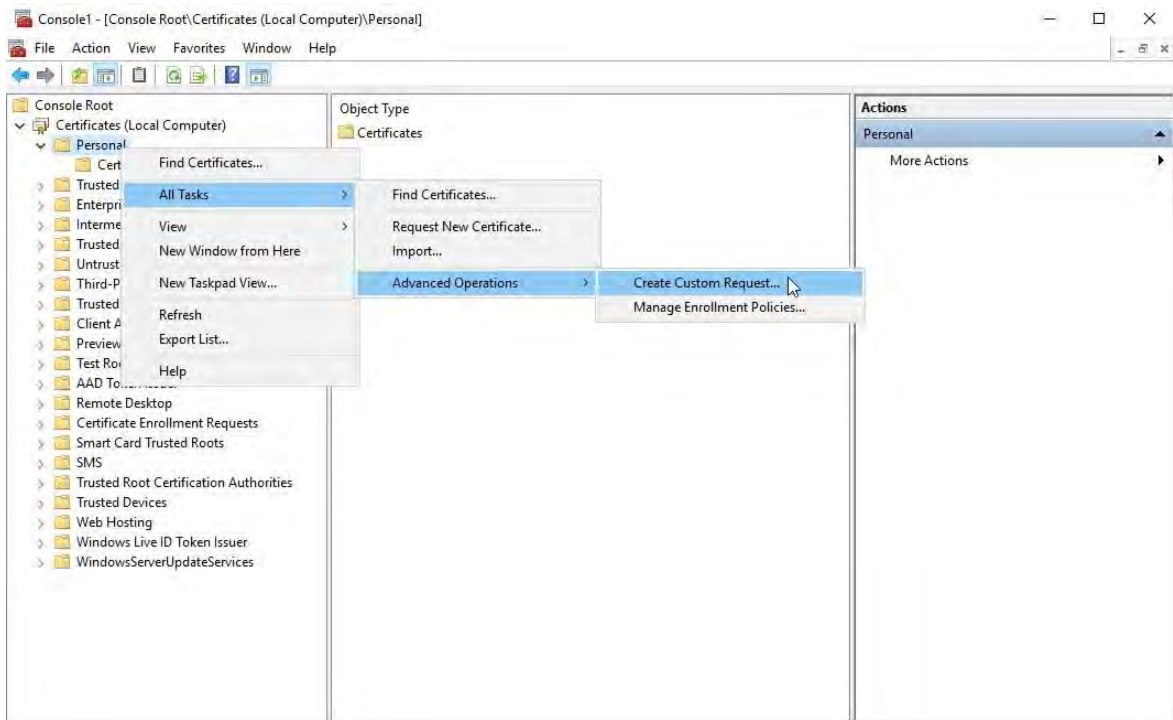


5. En **Seleccionar equipo**, seleccione **Equipo local**.


Seleccione **Finalizar** y, a continuación, **Aceptar**.



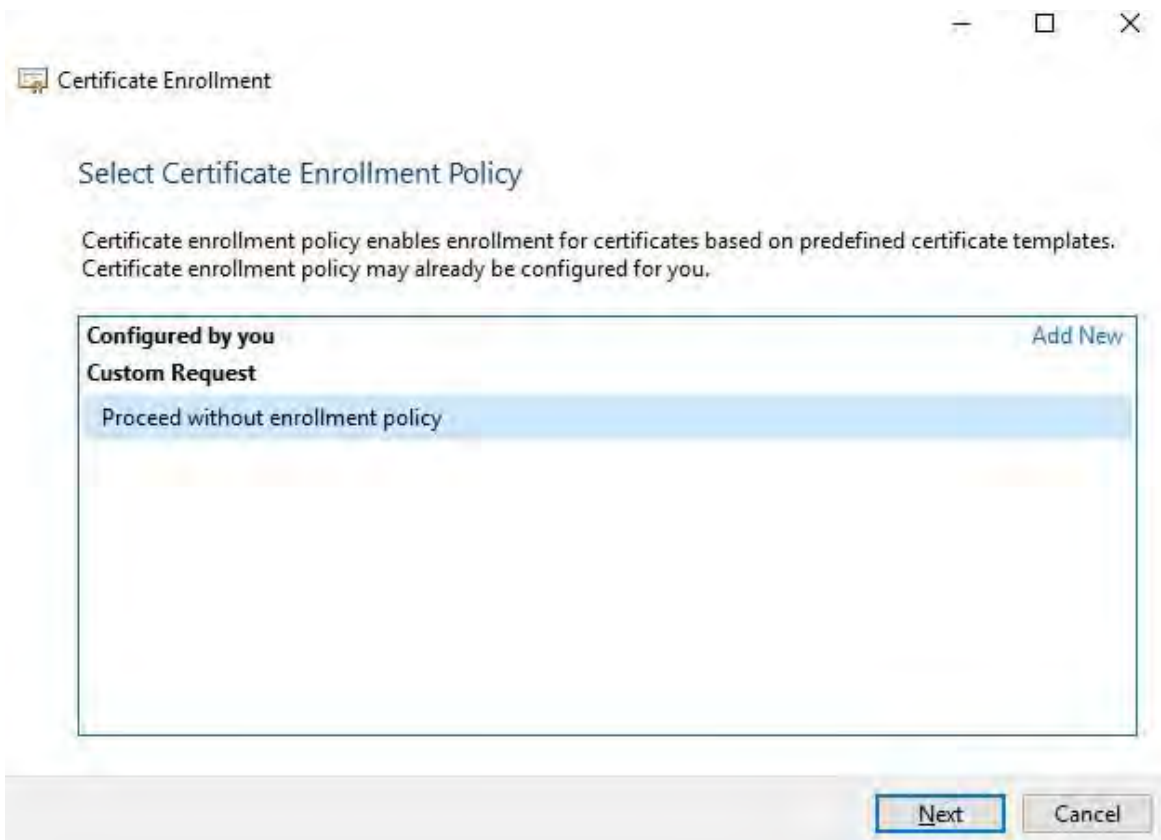
6. Expanda el objeto Certificates. Haga clic con el botón derecho en la **carpeta Personal** y seleccione **Todas las tareas > Operaciones avanzadas > Crear solicitud personalizada**.



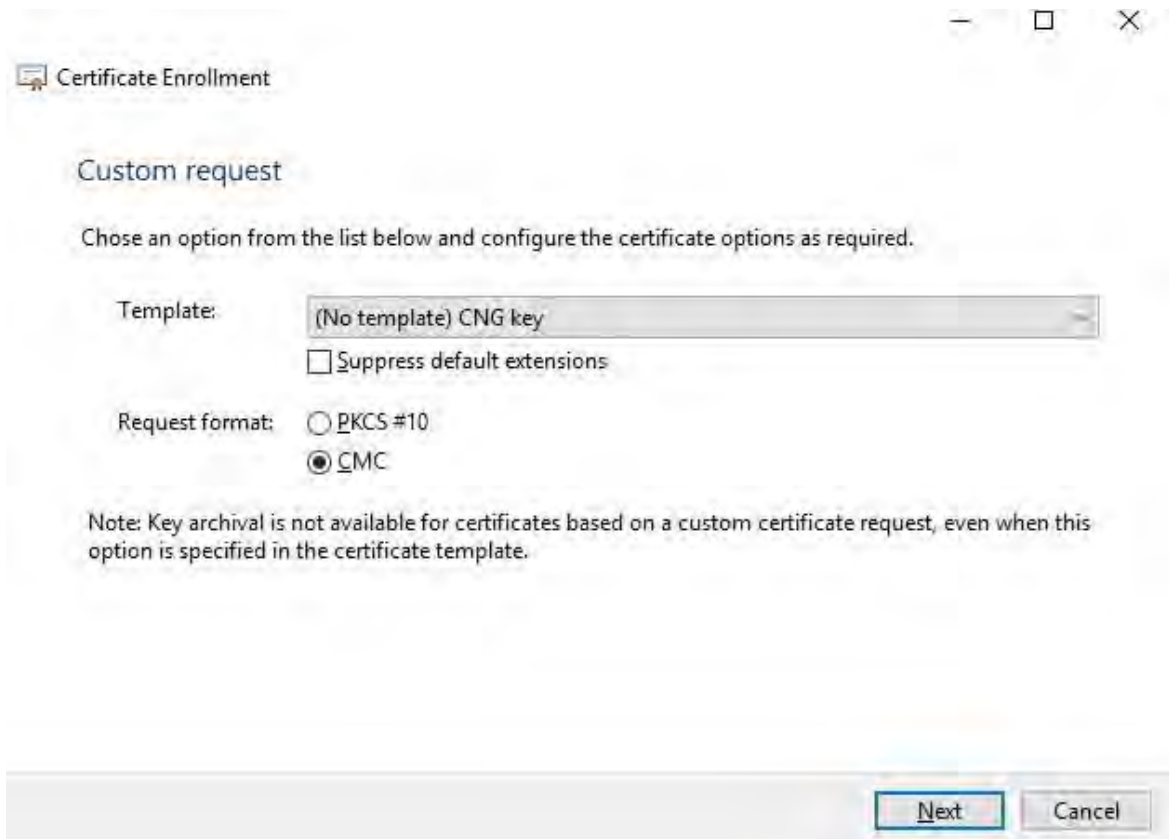
7. Haga clic en **Siguiente** en el Asistente para **inscripción de certificados** y seleccione **Continuar sin directiva de inscripción**.

 Si su política de grupo ya contiene una política de inscripción de certificados, querrá confirmar el resto de este proceso con su equipo de administración de dominio antes de continuar.

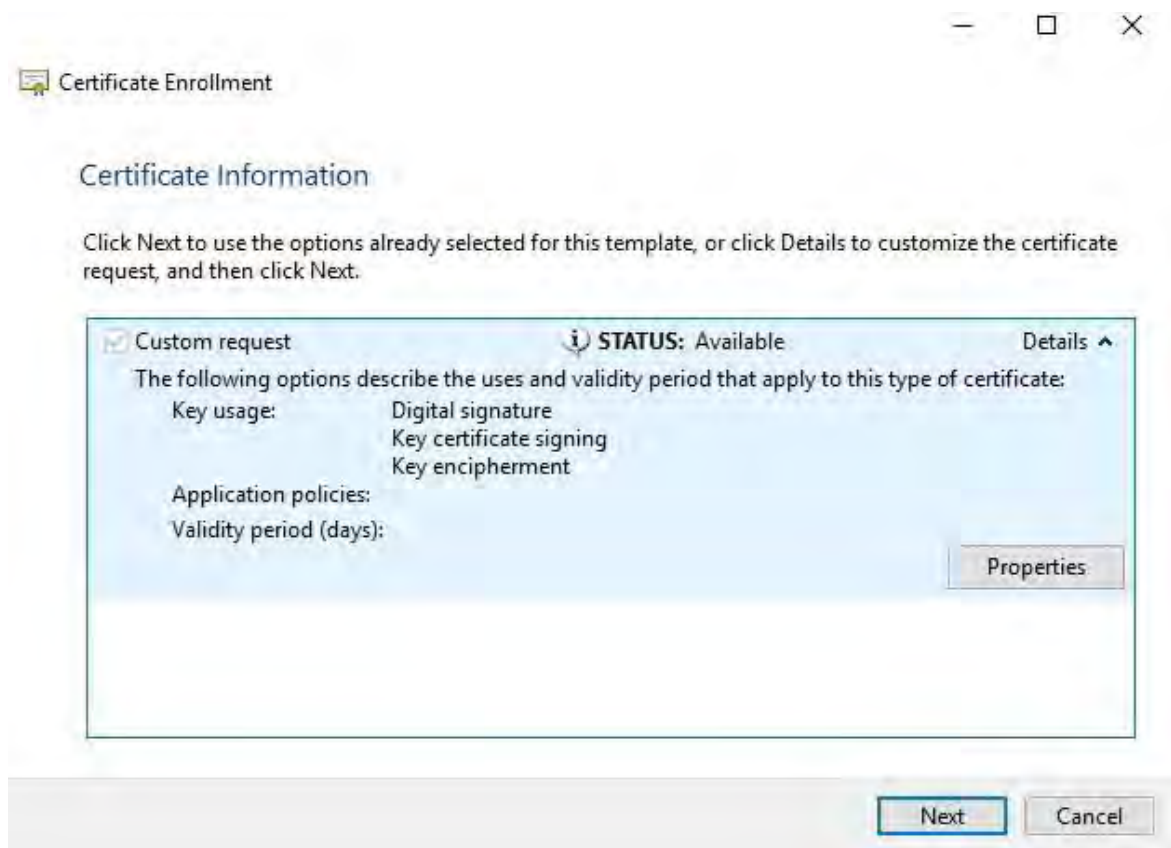
Haga clic en **Siguiente**.



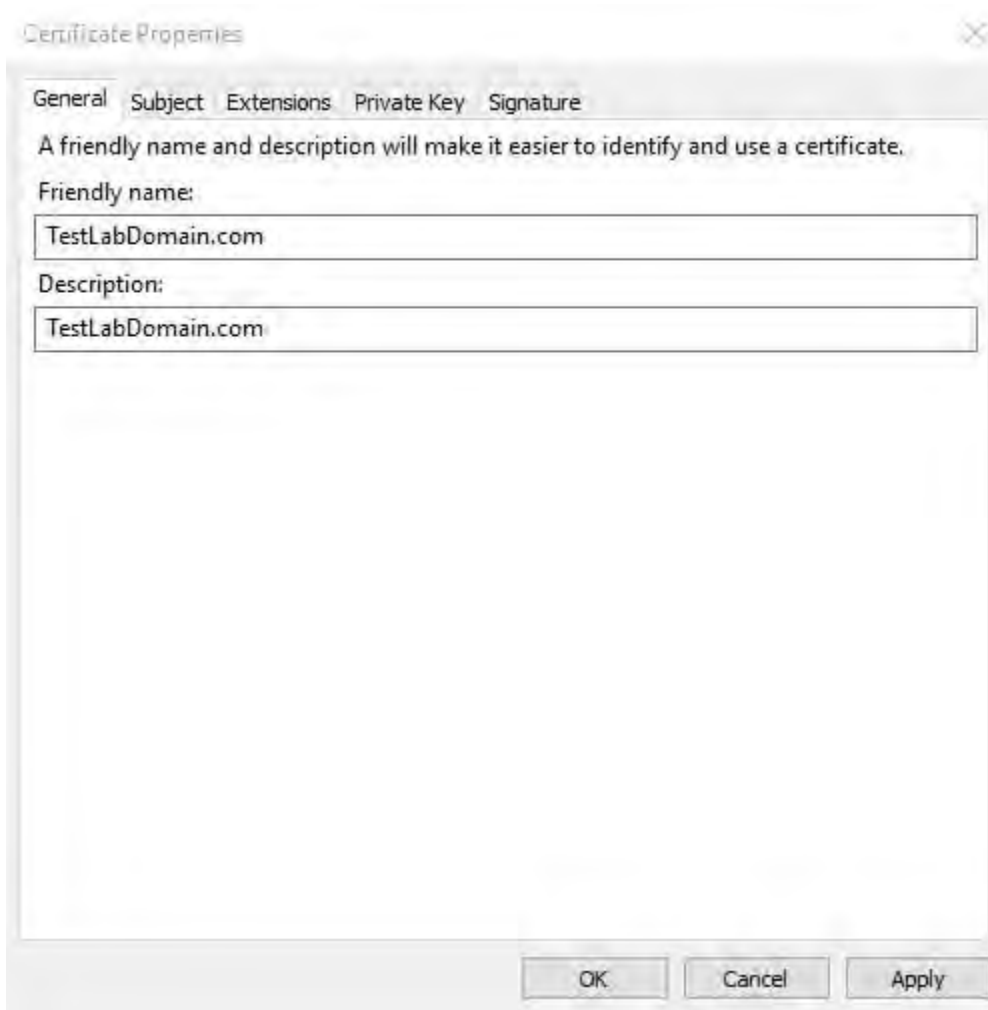
8. Seleccione la plantilla **de clave CNG (sin plantilla)** y el formato de solicitud de **CMC** y haga clic en **Siguiente**.



9. Expanda para ver los **detalles** de la solicitud personalizada y haga clic en **Propiedades**.



10. En la pestaña **General**, rellene los campos **Nombre descriptivo** y **Descripción** con el nombre de dominio, el nombre del equipo o la organización.



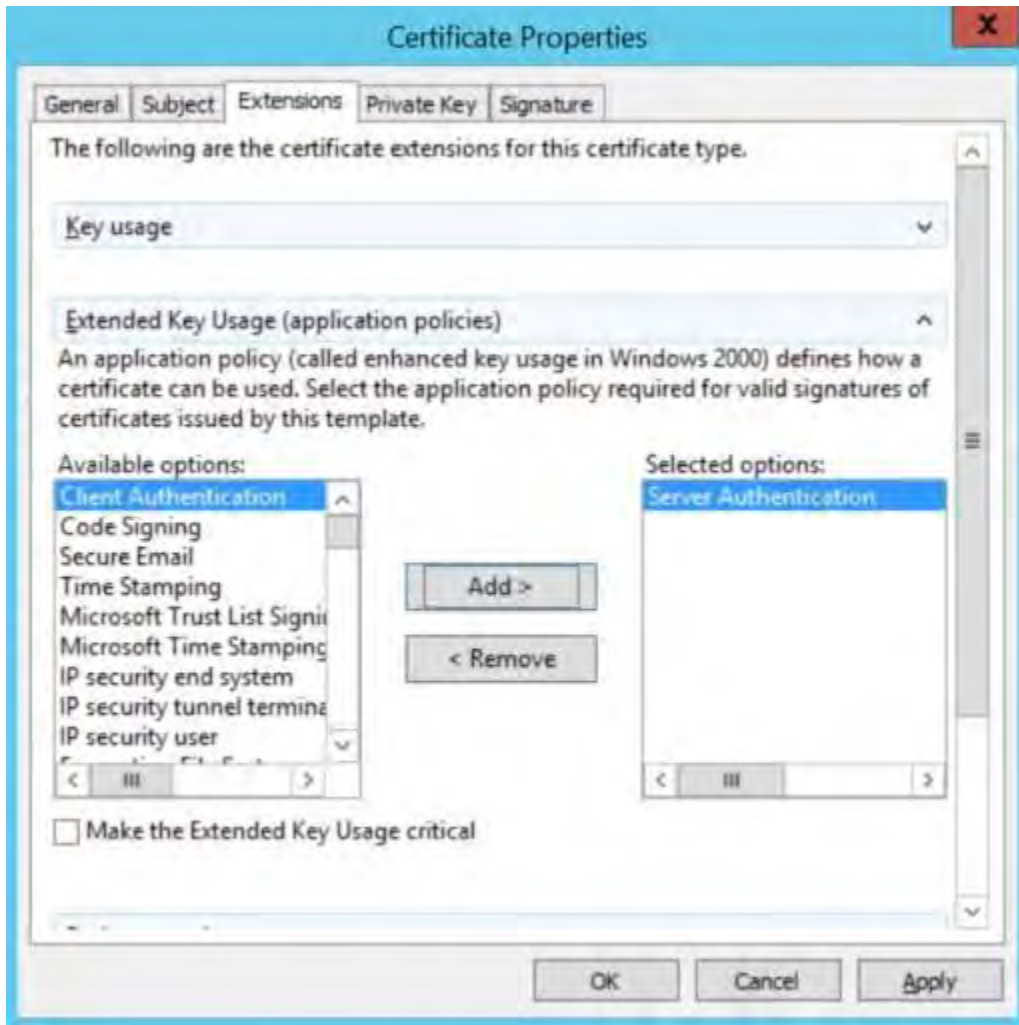


11. En la **pestaña Asunto**, introduzca los parámetros necesarios para el nombre del sujeto.

En el nombre del asunto **Tipo**, escriba en **Nombre común** el nombre de host del equipo donde se instalará el certificado.

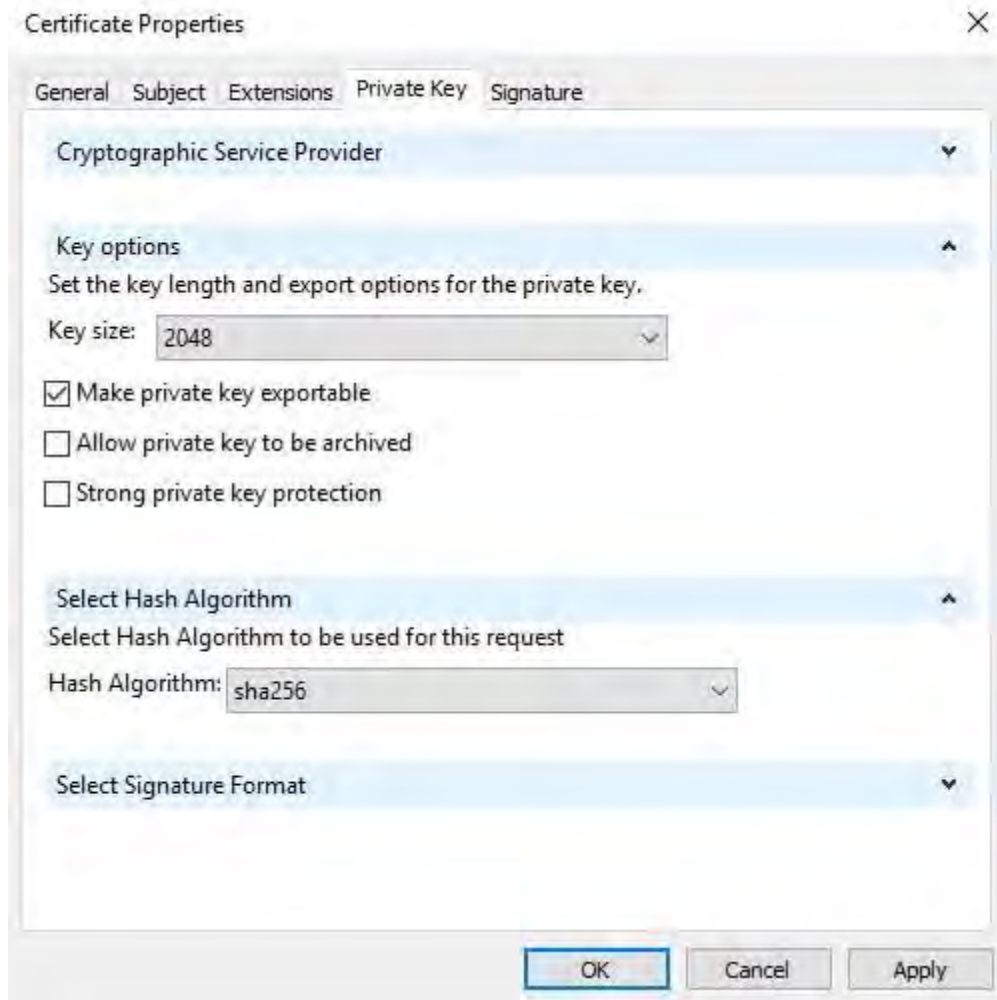


12. En la **pestaña Extensiones** y **expanda el** menú **Uso extendido de claves (directivas de aplicación)** .  
Agregue **la autenticación del servidor** de la lista de opciones disponibles.



13. En la pestaña **Clave privada**, expanda el menú **Opciones de clave**.

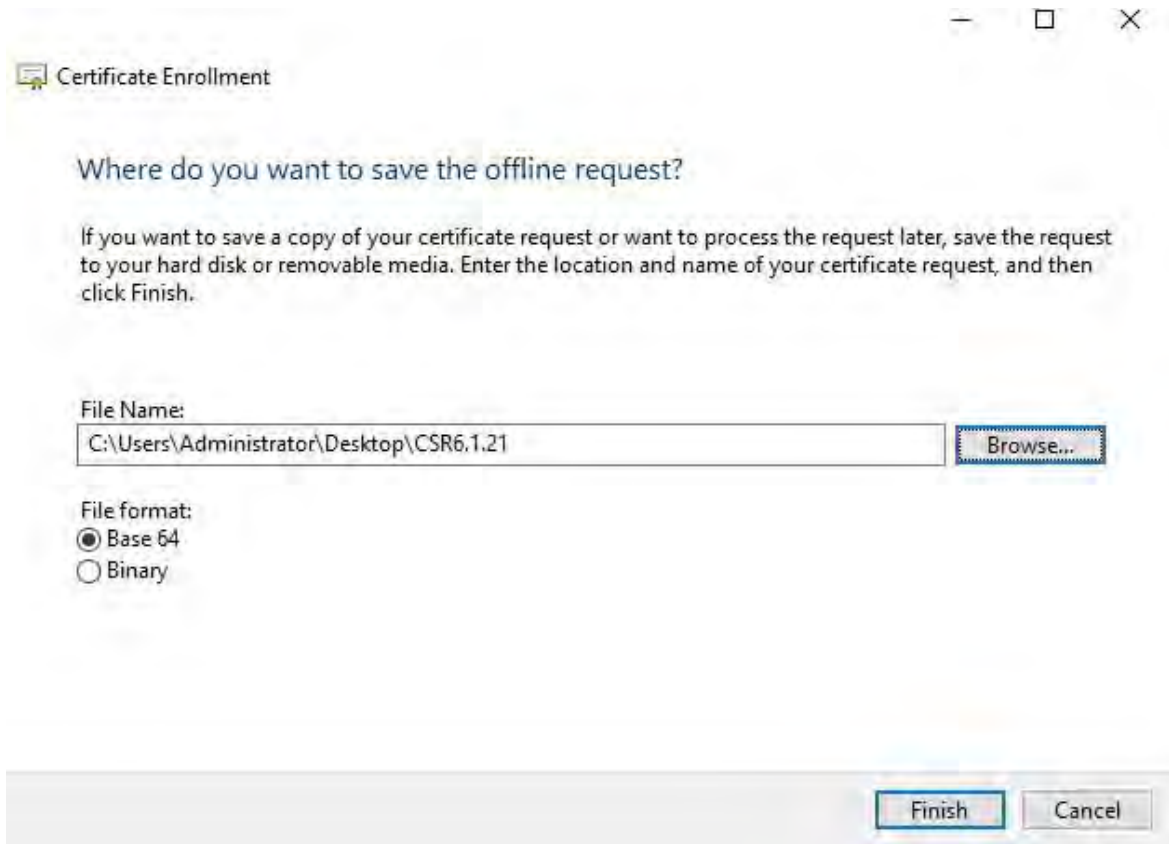
Establezca el tamaño de la clave en 2048 y seleccione la opción para que la clave privada sea exportable. Haga clic en **Aceptar**.



14. Cuando se hayan definido todas las propiedades del certificado, haga clic **en Siguiente** en el Asistente para inscripción de **certificados**.

15. Seleccione una ubicación para guardar la solicitud de certificado y un formato. Vaya a esa ubicación y especifique un nombre para el archivo .req. El formato predeterminado es base 64.

16. Haga clic en **Finalizar**.



Se genera un archivo .req, que debe utilizar para solicitar un certificado firmado.

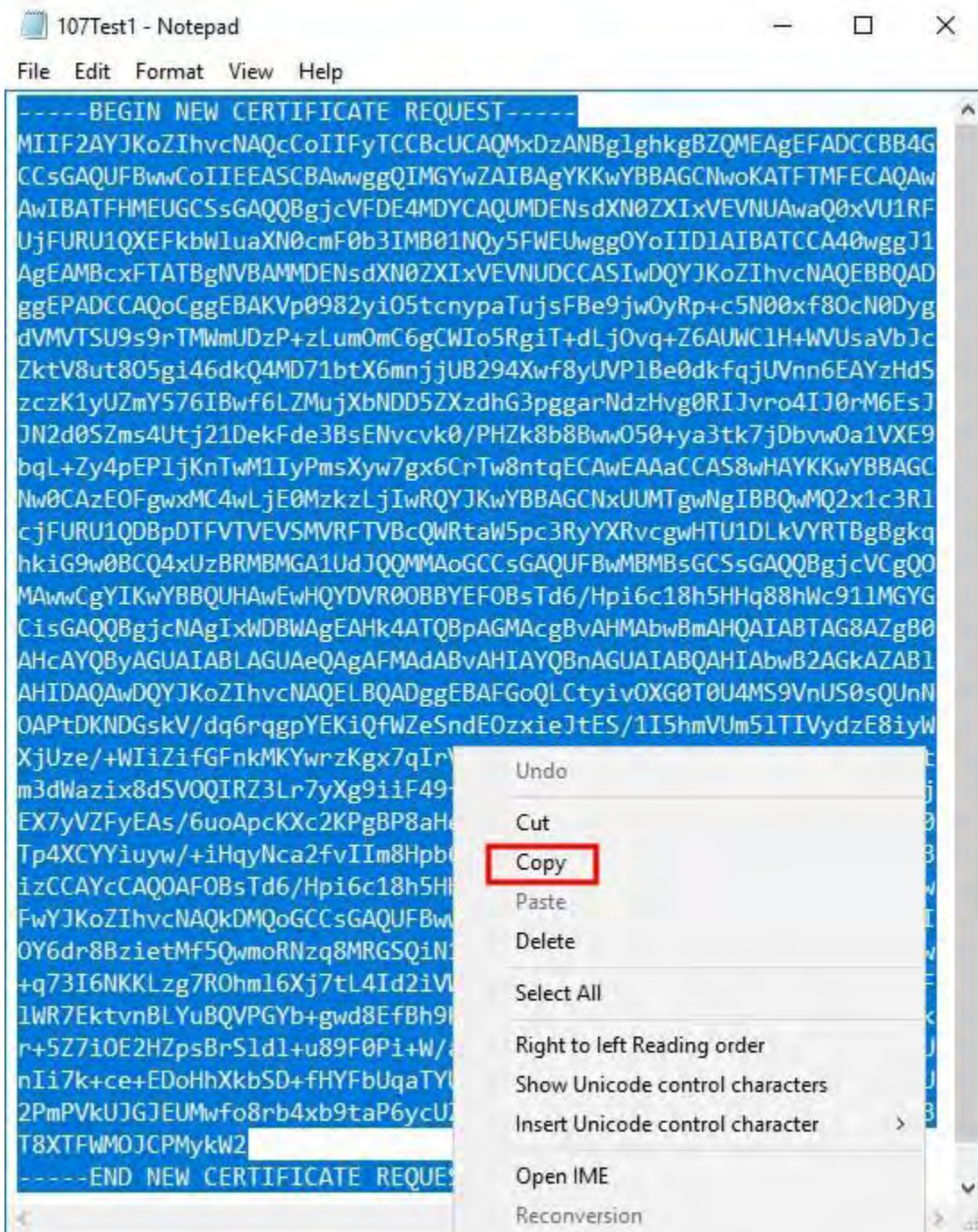
### **Cargue el archivo .req para recibir un certificado firmado a cambio**

Debe copiar todo el texto del archivo .req, incluidas las líneas inicial y final, y pegar el texto en la entidad de certificación interna de Servicios de certificados de Active Directory en la red. Consulte [Instalar Servicios de certificados de Active Directory en la página 74](#).



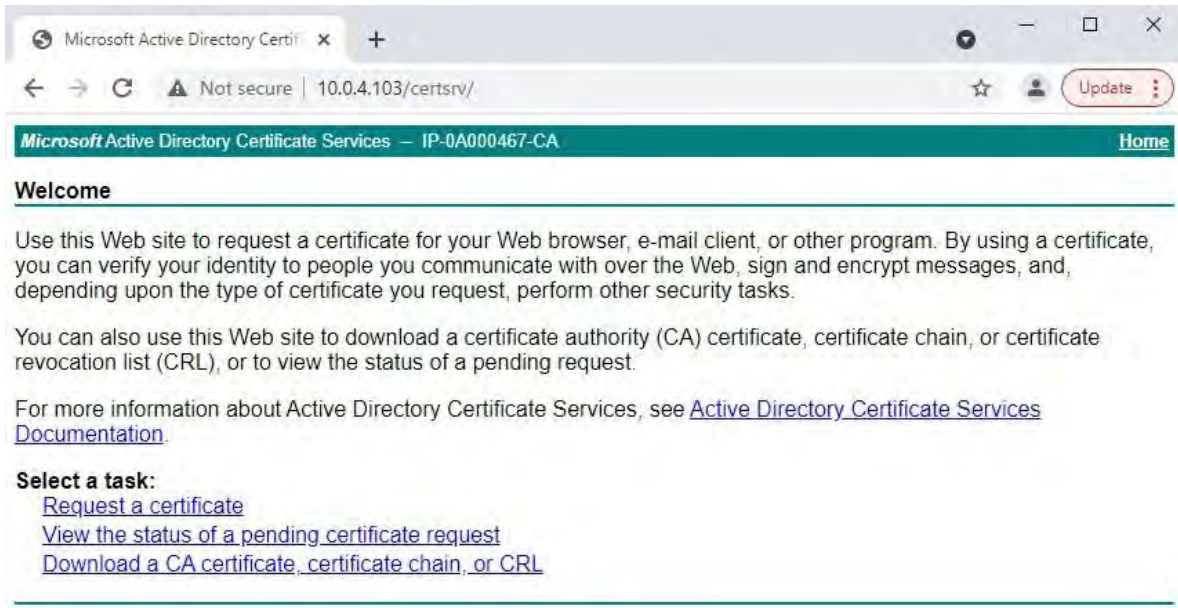
A menos que su dominio haya instalado recientemente los Servicios de Certificados de Active Directory, o que se haya instalado solo para este propósito, deberá enviar esta solicitud siguiendo un procedimiento separado configurado por su equipo de Administración de Dominio. Confirme este proceso con ellos antes de continuar.

1. Busque la ubicación del archivo .req y ábralo en el Bloc de notas.

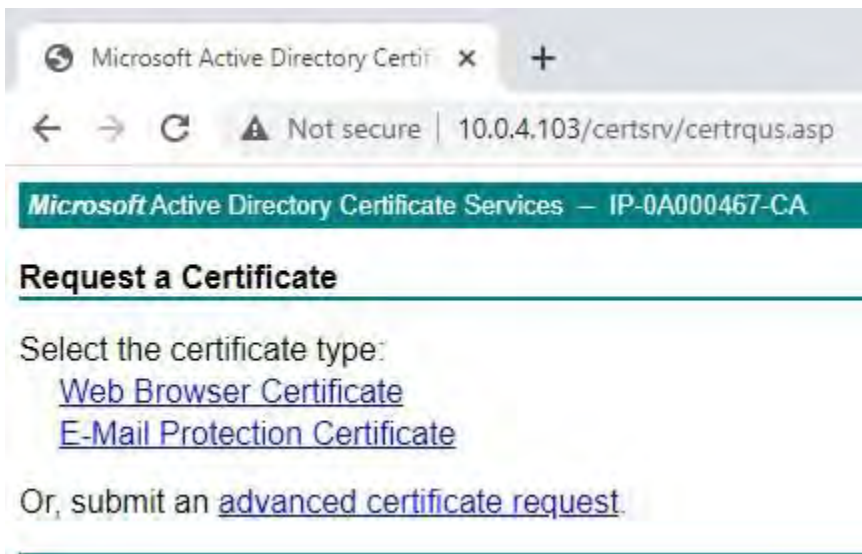


2. Copie todo el contenido del archivo. Esto incluye las líneas discontinuas que marcan el principio y el final de la solicitud de certificado.

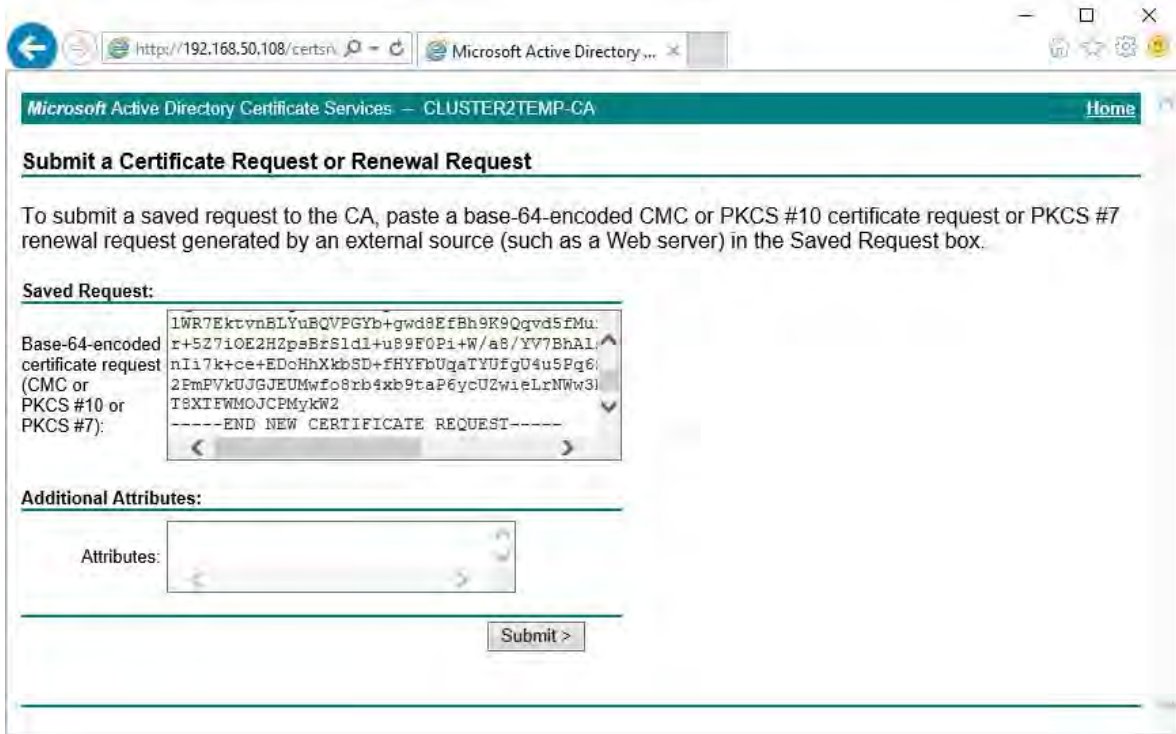
3. Abra un navegador web e introduzca la dirección de la CA de dominio.



4. Haga clic en el **enlace Solicitar un certificado**.
5. Haga clic en el enlace de **solicitud de certificado avanzado**.



6. Pegue el contenido del archivo .req en el formulario. Si es necesario seleccionar una plantilla de certificado, seleccione **Servidor web** de la lista Plantilla de certificado.



7. Haga clic en **Enviar**.

El sitio muestra un mensaje que indica que el certificado se emitirá en unos días.

Es probable que el equipo de administración de dominios distribuya e instale el certificado por usted. Sin embargo, si se le entrega el certificado, puede instalarlo manualmente.

### Instalar el certificado manualmente

Si se le entrega el certificado, puede instalarlo manualmente.

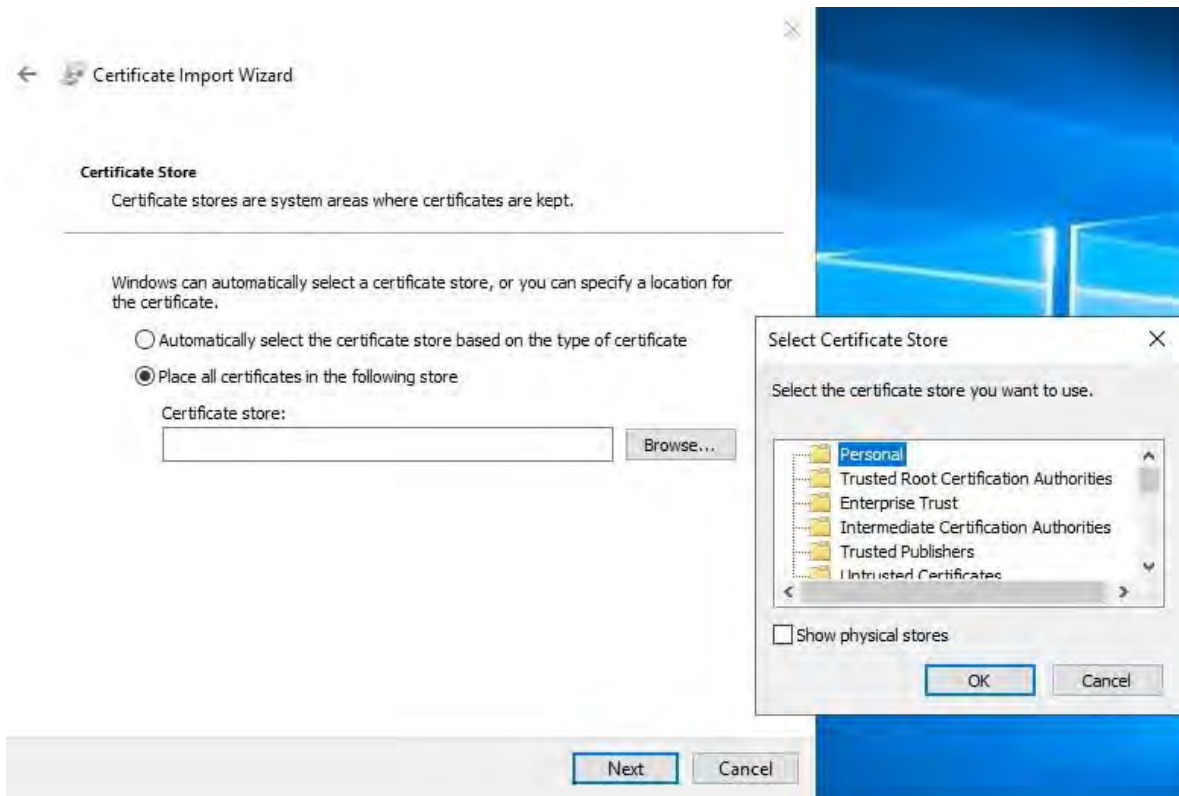
1. Localice el archivo de certificado en el equipo que aloja el servidor de administración o el servidor de grabación .
2. Haga clic con el botón derecho en el certificado y seleccione **Instalar certificado**.
3. Acepte la advertencia de seguridad si aparece.

Seleccione esta opción para instalar el certificado para el usuario actual y haga clic en **Siguiente**.

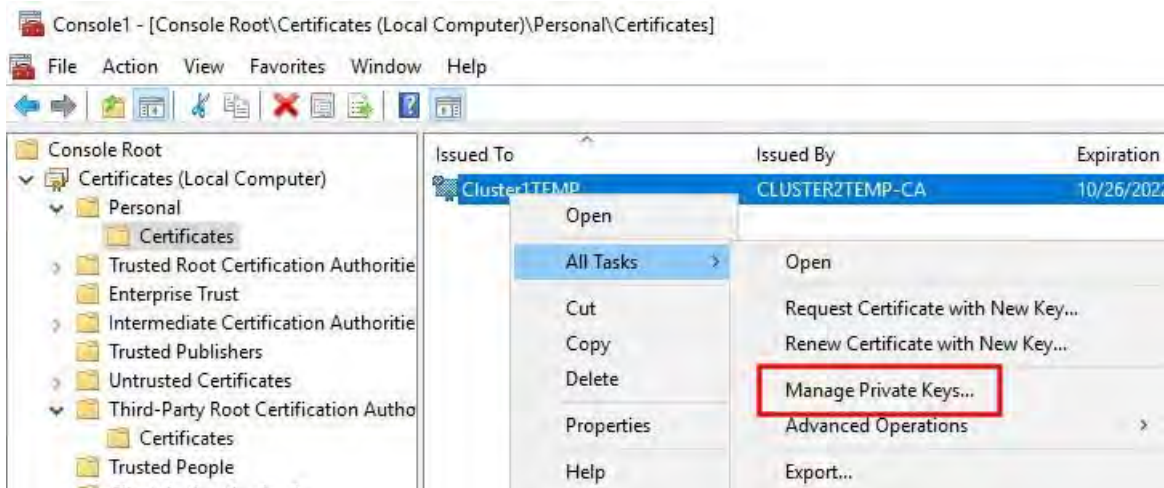




4. Elija una ubicación de almacenamiento, vaya al almacén de certificados personales y haga clic en **Siguiente**.



5. Finalice el asistente **para instalar certificado**.
6. Vaya al complemento Certificados de Microsoft Management Console (MMC).
7. En la consola, vaya a la tienda personal donde está instalado el certificado. Haga clic con el botón derecho en el certificado y seleccione **Todas las tareas > Administrar claves privadas**.



8. Compruebe que la cuenta que ejecuta el software MOBOTIX HUB Management Server, Recording Server o Mobile Server está en la lista de usuarios con permiso para utilizar el certificado.

Asegúrese de que el usuario tenga habilitados los permisos Control total y Lectura.



De forma predeterminada, el software MOBOTIX HUB utiliza la cuenta NETWORK SERVICE. En un entorno de dominio, las cuentas de servicio se utilizan normalmente para instalar y ejecutar los servicios de MOBOTIX HUB. Tendrás que hablar de esto con tu equipo de administración de dominios y hacer que se agreguen los permisos adecuados a las cuentas de servicio si aún no se han configurado correctamente. Confirme esto antes de continuar.

### Habilitar el cifrado de servidor para servidores de administración y servidores de grabación

Una vez instalado el certificado con las propiedades y los permisos correctos, haga lo siguiente.

1. En un equipo con un servidor de administración o un servidor de grabación instalado, abra el **configurador de servidores**

De:

- El menú Inicio de Windows

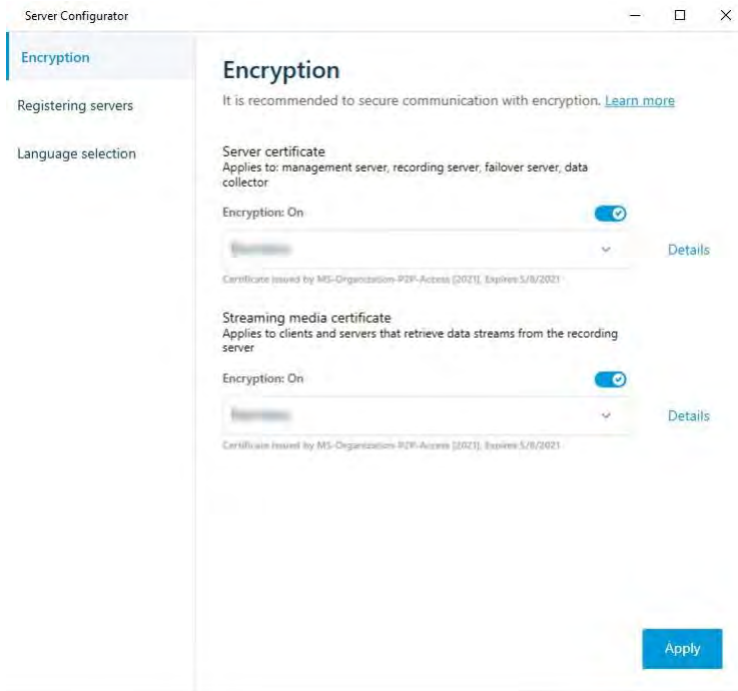
o

- El administrador del servidor, haciendo clic con el botón derecho en el icono del administrador del servidor en la barra de tareas del equipo

2. En Server **Configurator**, en **Certificado de servidor**, active **Cifrado**.
3. Haga clic en **Seleccionar certificado** para abrir una lista con los nombres de los firmantes únicos de los certificados que tienen una clave privada y que están instalados en el equipo local en el Almacén de certificados de Windows.
4. Seleccione un certificado para cifrar la comunicación entre el servidor de grabación, el servidor de administración, el servidor de conmutación por error y el servidor del recopilador de datos.

Seleccione **Detalles** para ver la información del Almacén de certificados de Windows sobre el certificado seleccionado.

Al usuario del servicio del servidor de grabación se le ha dado acceso a la clave privada. Es necesario que este certificado sea de confianza en todos los clientes.



5. Haga clic en **Aplicar**.



Al aplicar certificados, el servidor de grabación se detendrá y se reiniciará. Detener el servicio del servidor de grabación significa que no puede grabar ni ver vídeo en directo mientras verifica o cambia la configuración básica del servidor de grabación.

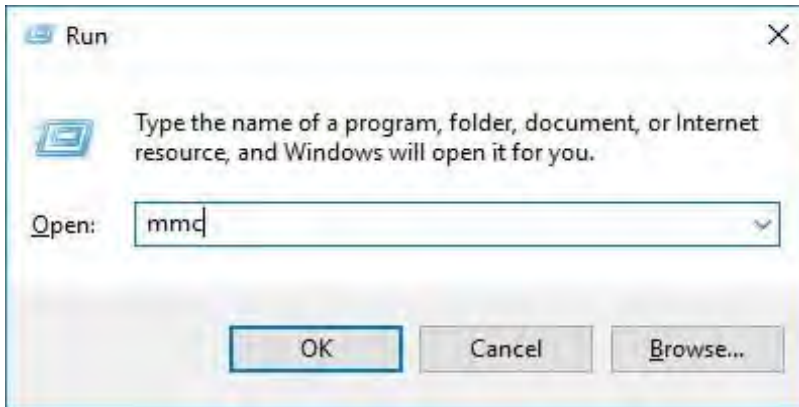
## **Instalar certificados en un entorno de grupo de trabajo para la comunicación con el servidor de administración o el servidor de grabación**

Cuando se opera en un entorno de grupo de trabajo, se supone que no hay infraestructura de autoridad de certificación. Para distribuir certificados, es necesario crear una infraestructura de autoridad de certificación. También es necesario distribuir las claves de certificado a las estaciones de trabajo cliente. A excepción de estos requisitos, el proceso de solicitud e instalación de un certificado en un servidor es similar a los escenarios de dominio y CA comercial.

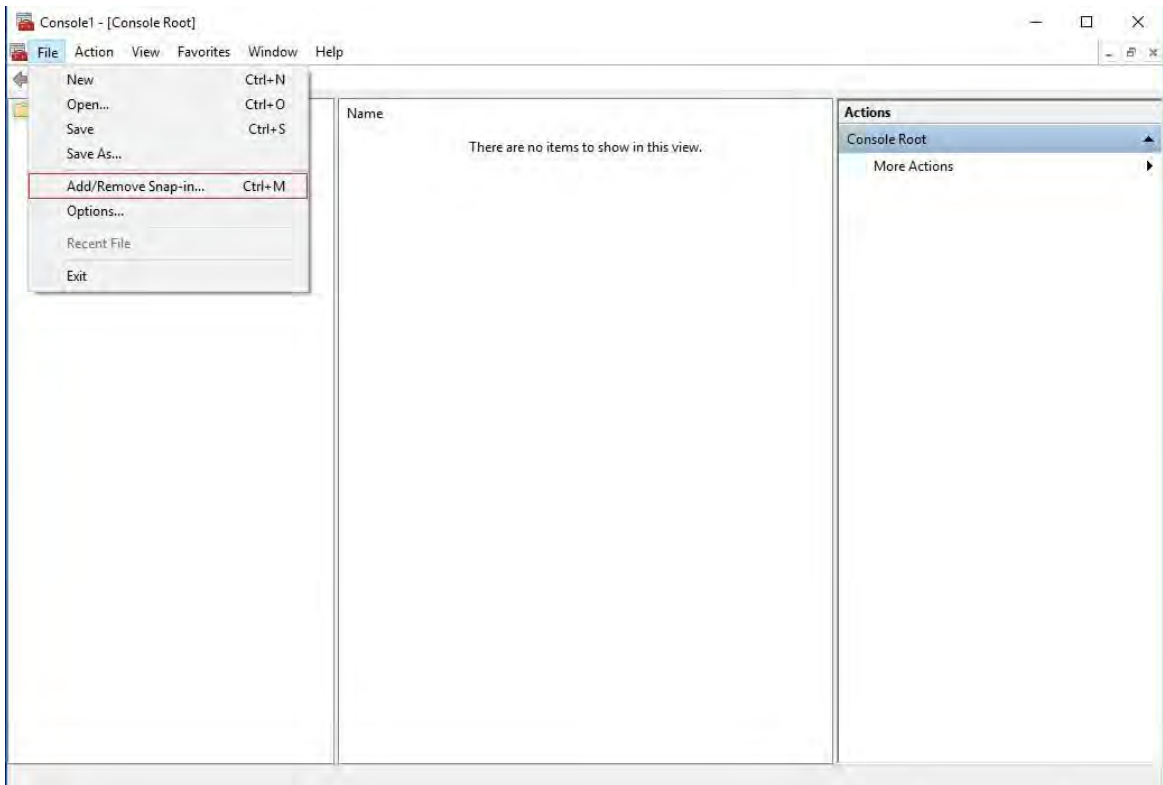
### **Agregar un certificado de CA al servidor**

Agregue el certificado de CA al servidor haciendo lo siguiente.

1. En el ordenador que aloja el servidor MOBOTIX HUB, abra la consola de administración de Microsoft.

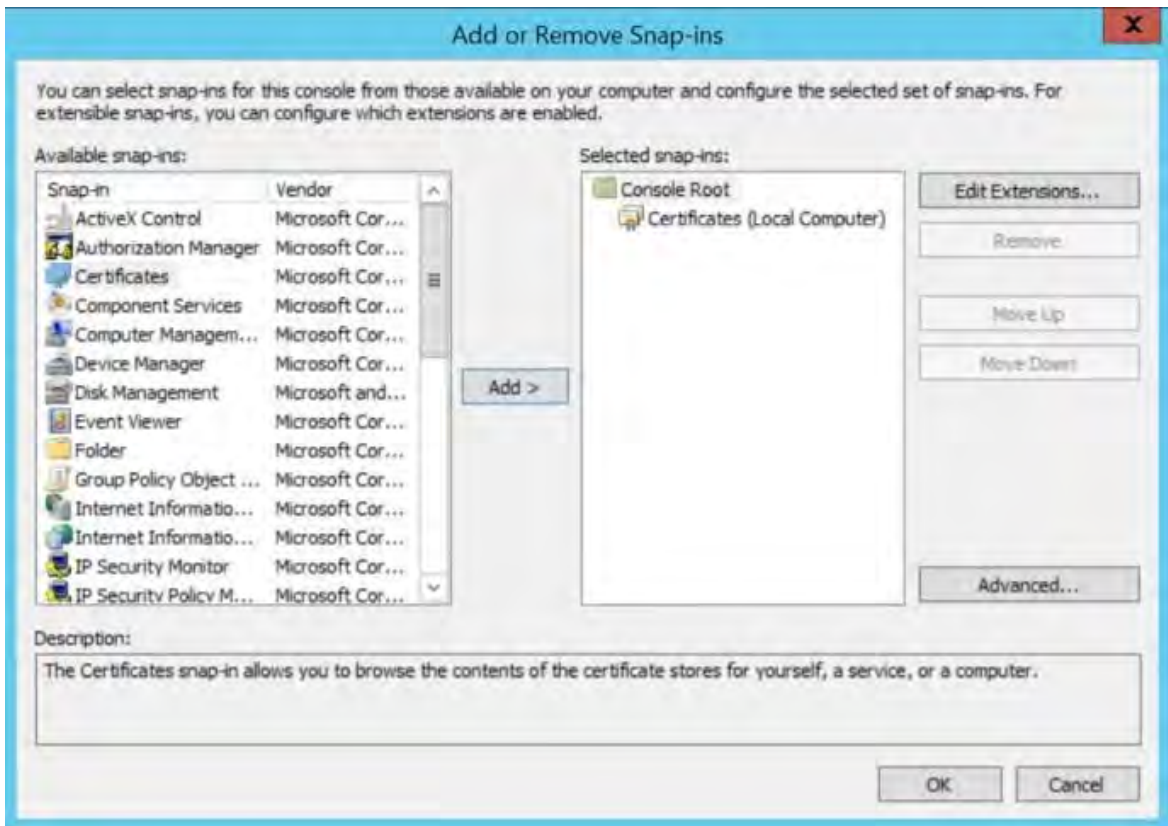


2. En Microsoft Management Console, en el menú **Archivo**, seleccione **Agregar o quitar complemento....**

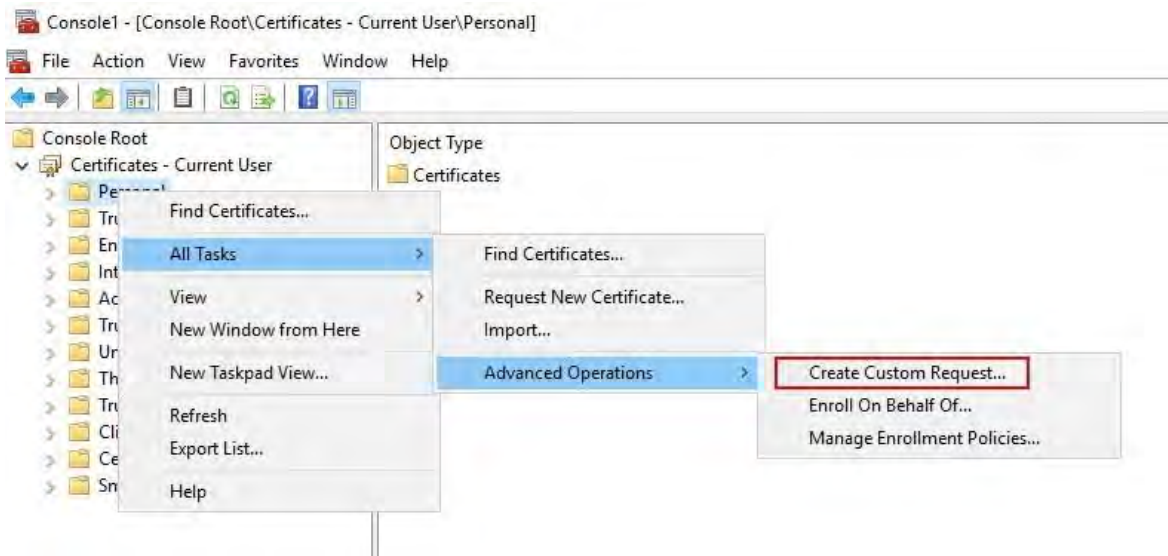


3. Seleccione el **complemento Certificados** y haga clic en **Agregar**.

Haga clic en **Aceptar**.

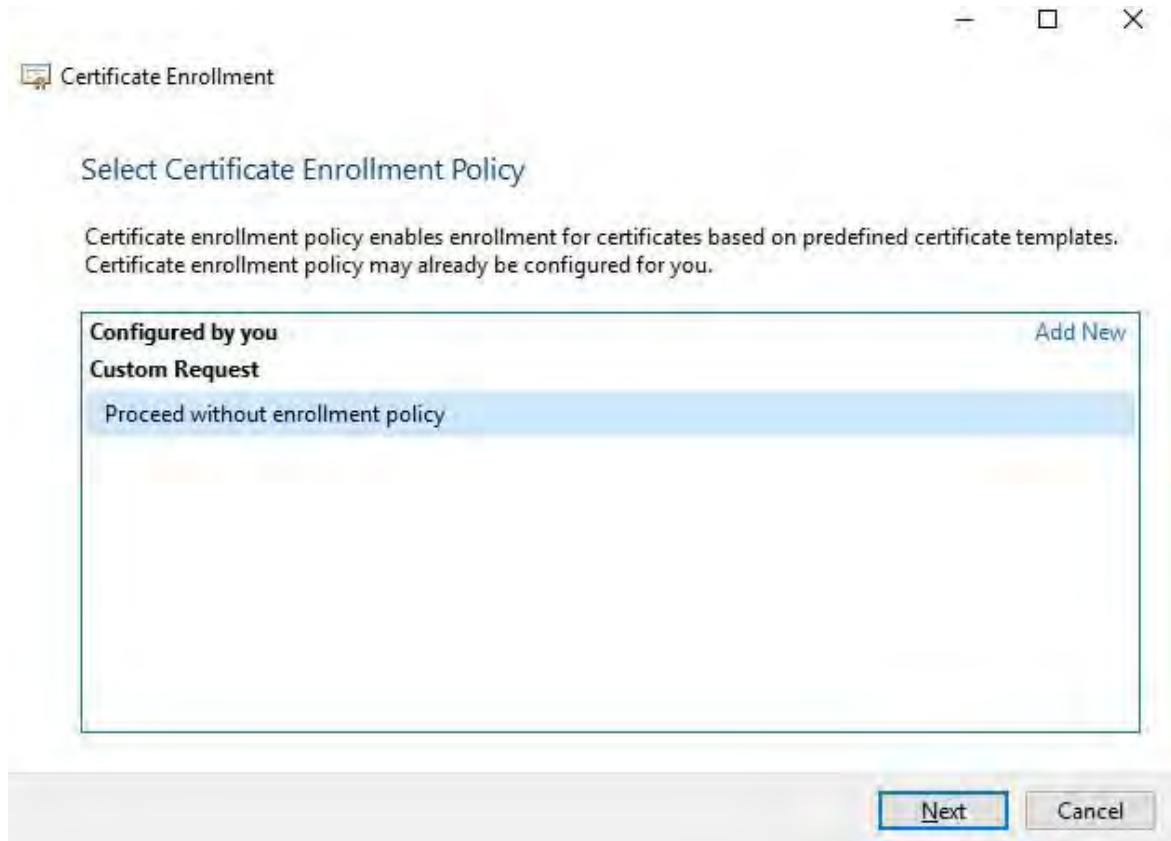


4. Expanda el objeto Certificados. Haga clic con el botón derecho en la **carpeta Personal** y seleccione **Todas las tareas > Operaciones avanzadas > Crear solicitud personalizada**.

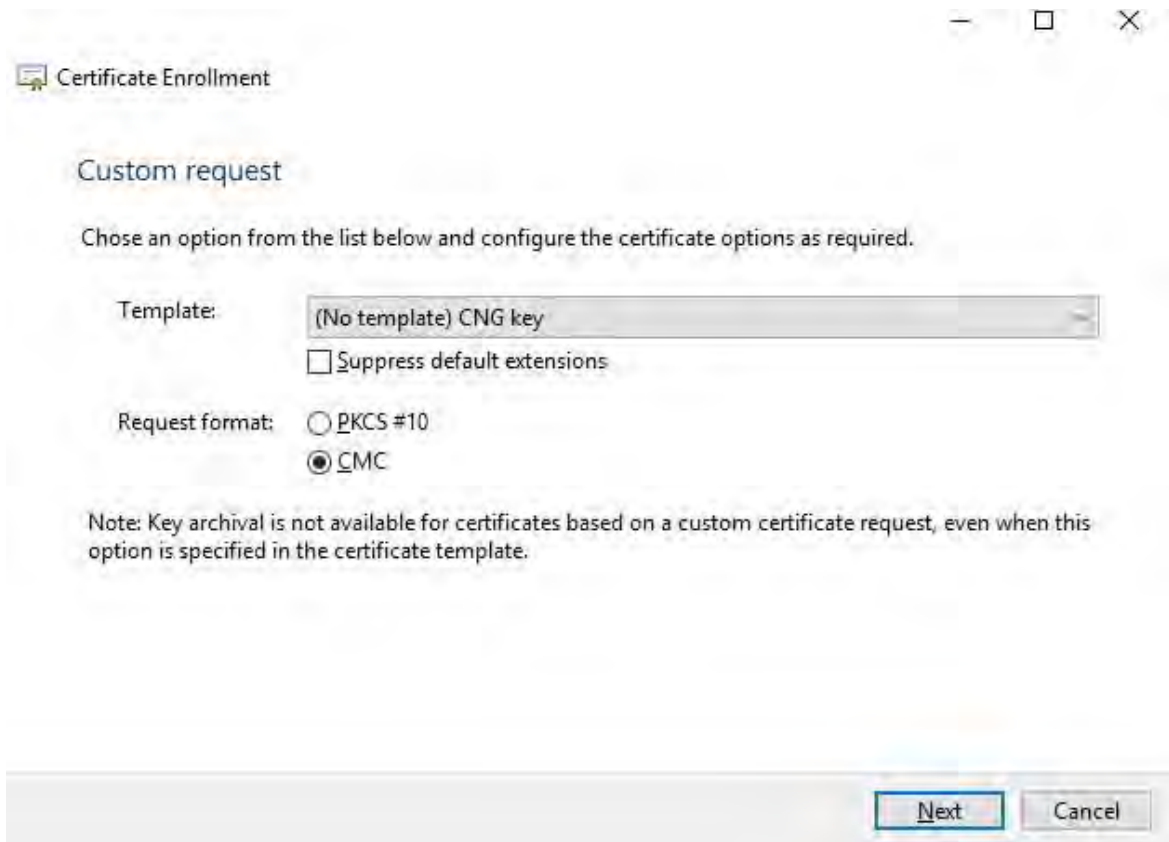


5. Haga clic en **Siguiente** en el Asistente para **inscripción de certificados** y seleccione **Continuar sin directiva de inscripción**.

Haga clic en **Siguiente**.

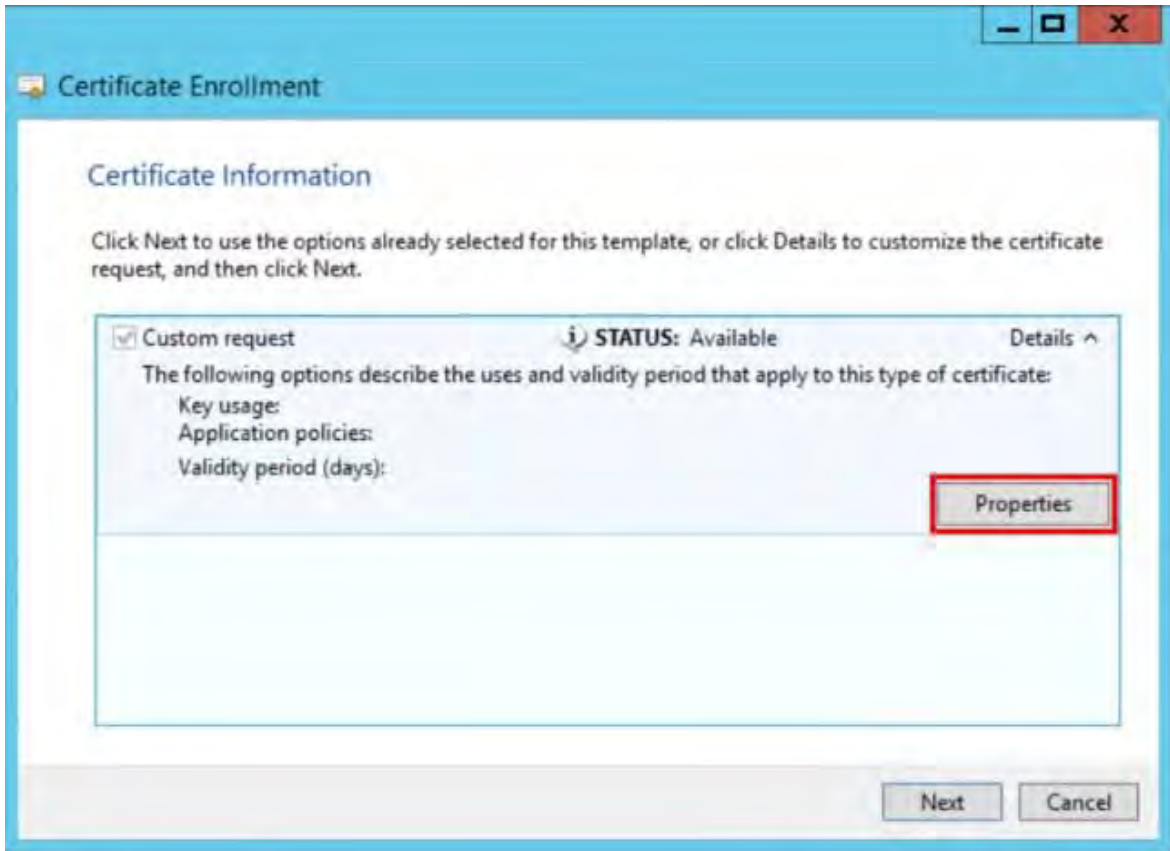


6. Seleccione la plantilla **de clave CNG (sin plantilla)** y el formato de solicitud de **CMC** y haga clic en **Siguiente**.

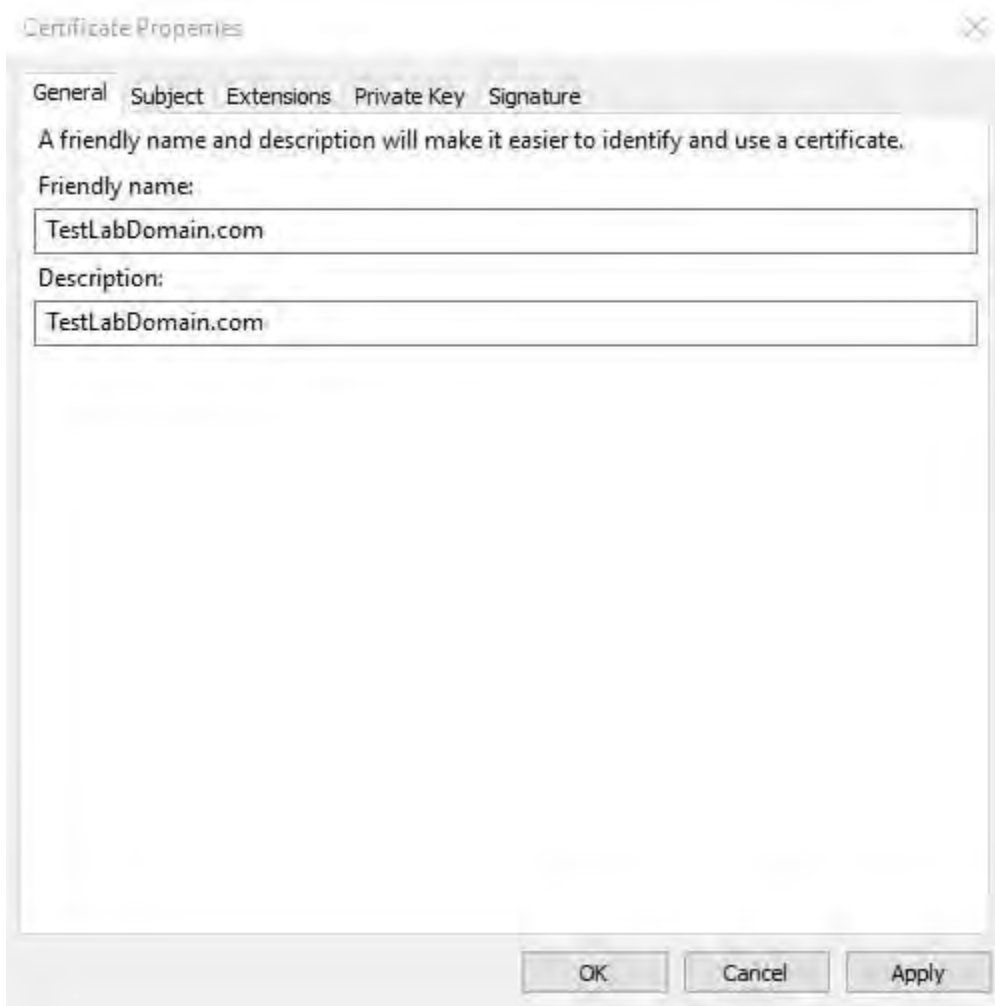




7. Expanda para ver los **detalles** de la solicitud personalizada y haga clic en **Propiedades**.



8. En la pestaña **General**, rellene los campos **Nombre descriptivo** y **Descripción** con el nombre de dominio, el nombre del equipo o la organización.

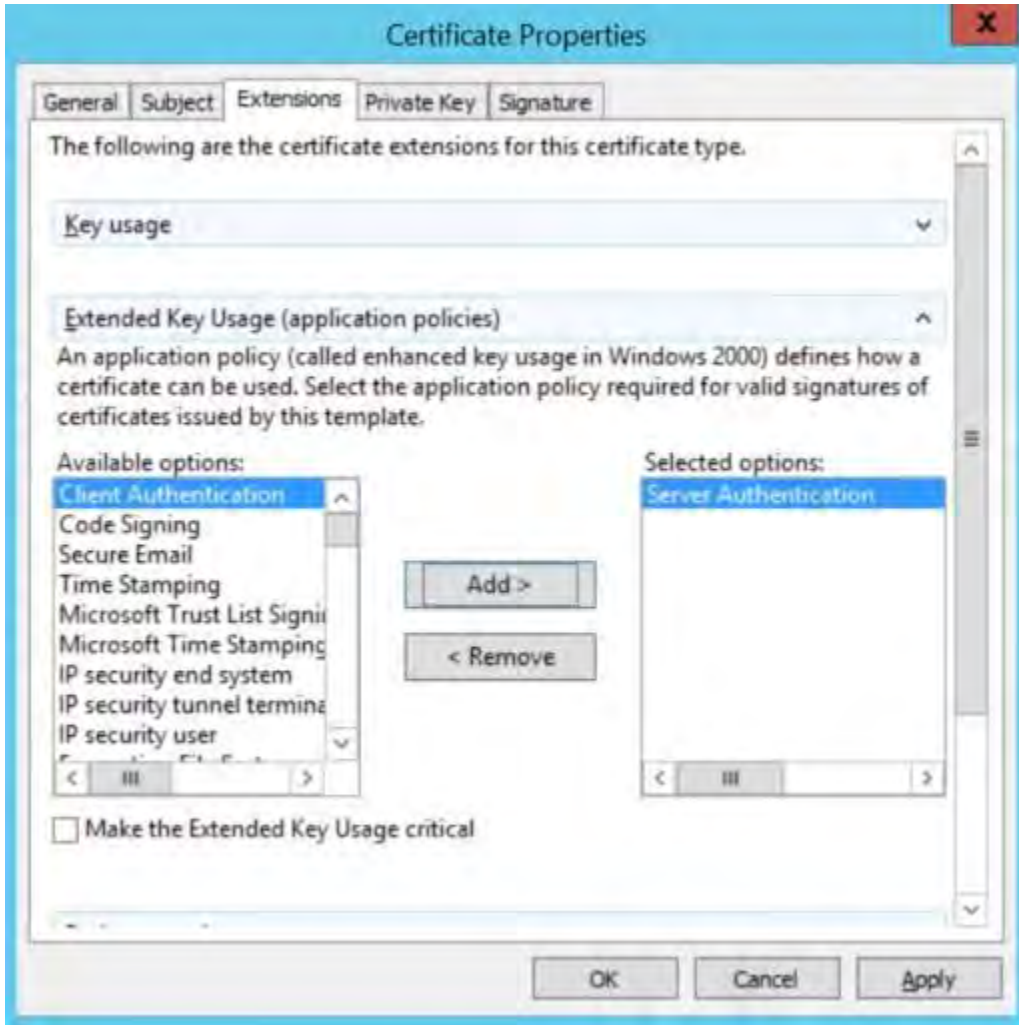


9. En la **pestaña Asunto**, introduzca los parámetros necesarios para el nombre del sujeto.

En el nombre del asunto **Tipo**, escriba en **Nombre común** el nombre de host del equipo donde se instalará el certificado.

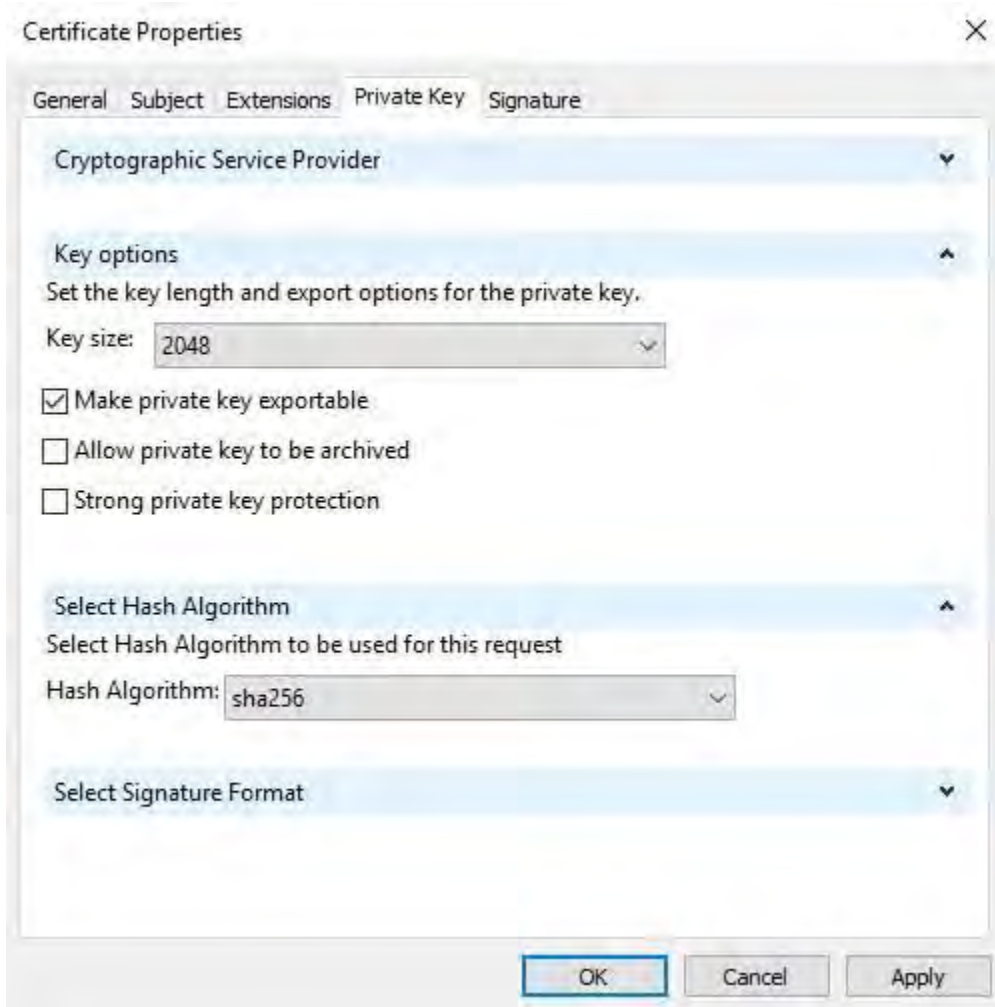


10. En la **pestaña Extensiones** y **expanda el** menú **Uso extendido de claves (directivas de aplicación)** . Agregue **la autenticación del servidor** de la lista de opciones disponibles.



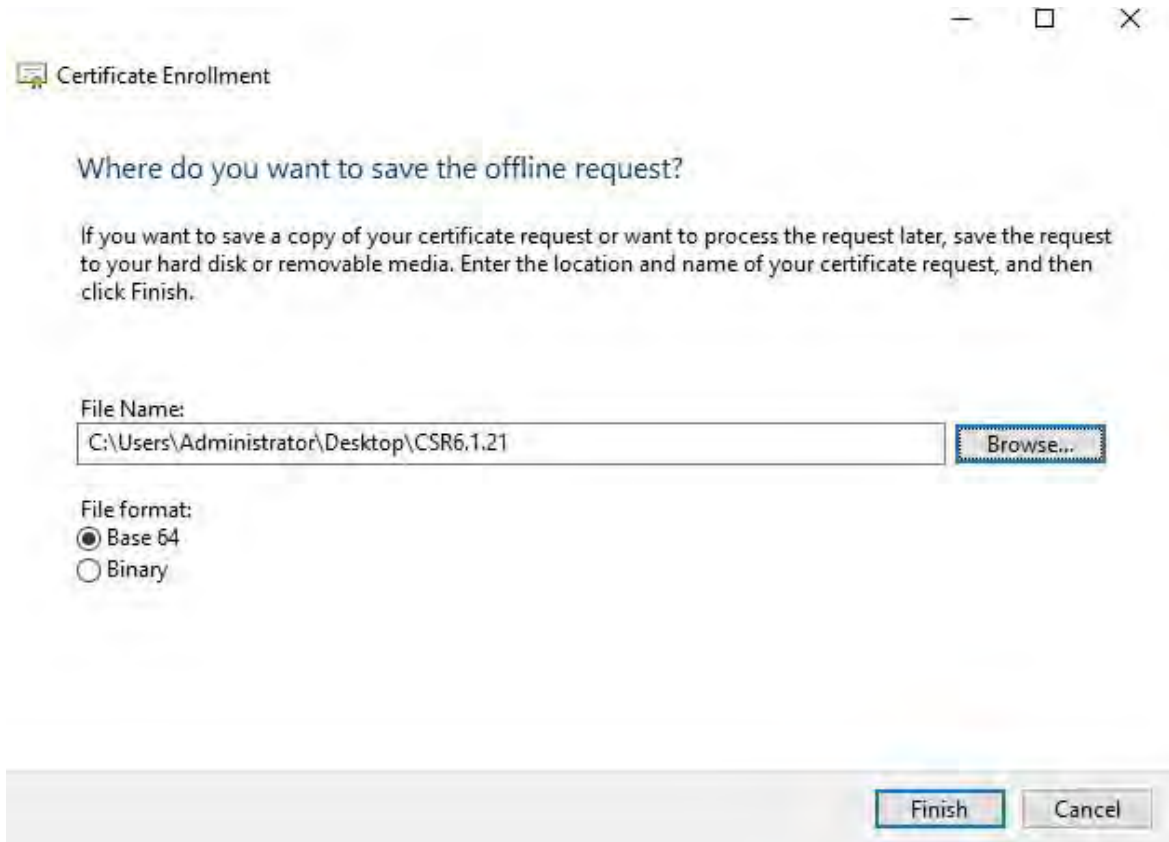
11. En la pestaña **Clave privada**, expanda el menú **Opciones de clave**.

Establezca el tamaño de la clave en 2048 y seleccione la opción para que la clave privada sea exportable. Haga clic en **Aceptar**.



12. Cuando se hayan definido todas las propiedades del certificado, haga clic **en Siguiente** en la inscripción de **certificados** hechicero.
13. Seleccione una ubicación para guardar la solicitud de certificado y un formato. Vaya a esa ubicación y especifique un nombre para el archivo .req. El formato predeterminado es base 64.

14. Haga clic en **Finalizar**.



Se genera un archivo .req, que debe utilizar para solicitar un certificado firmado.

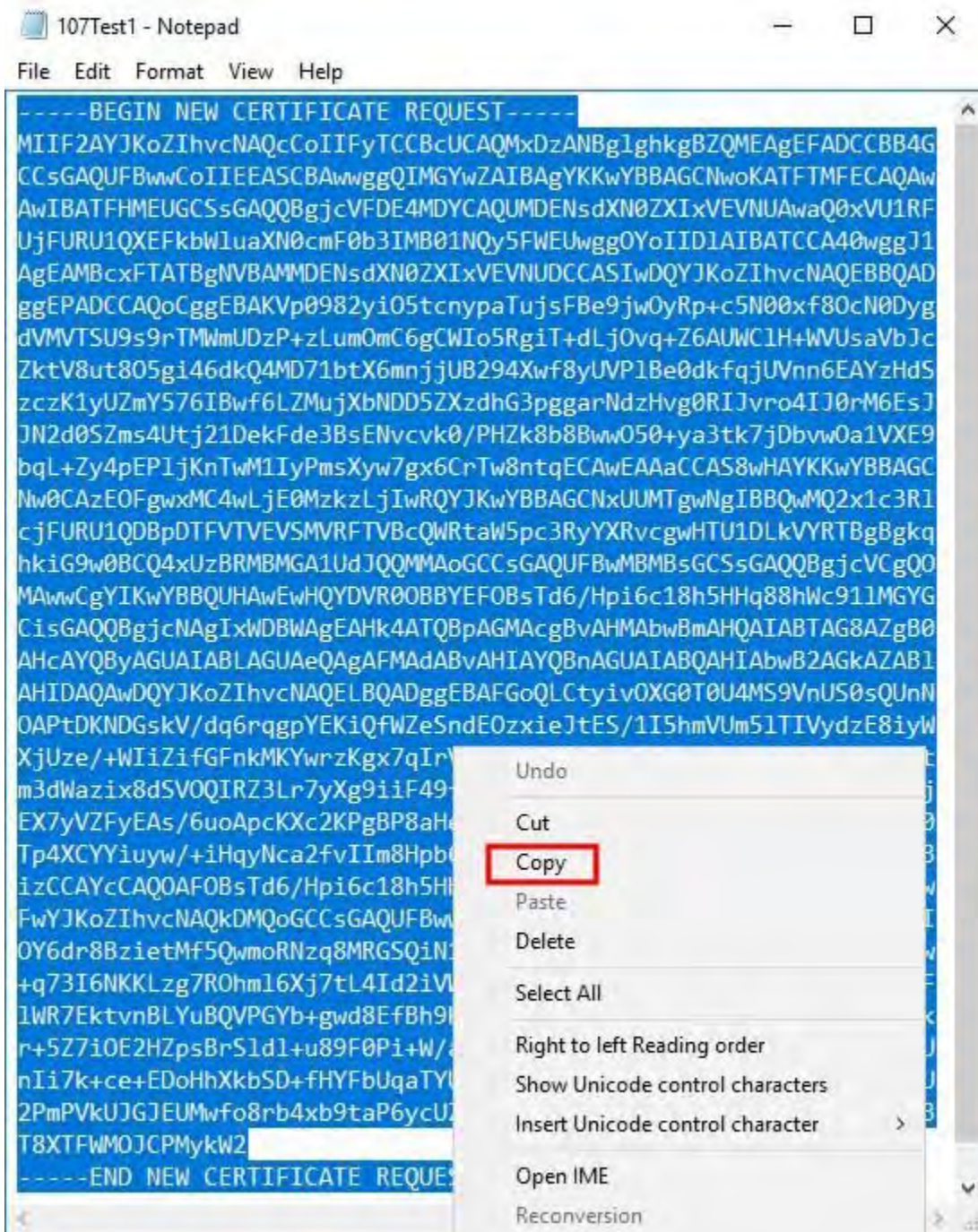
### **Cargue el archivo .req para recibir un certificado firmado a cambio**

Debe copiar todo el texto del archivo .req, incluidas las líneas inicial y final, y pegar el texto en la entidad de certificación interna de Servicios de certificados de Active Directory en la red. Consulte [Instalar Servicios de certificados de Active Directory en la página 74](#).



A menos que su dominio haya instalado recientemente los Servicios de Certificados de Active Directory, o que se haya instalado solo para este propósito, deberá enviar esta solicitud siguiendo un procedimiento separado configurado por su equipo de Administración de Dominio. Confirme este proceso con ellos antes de continuar.

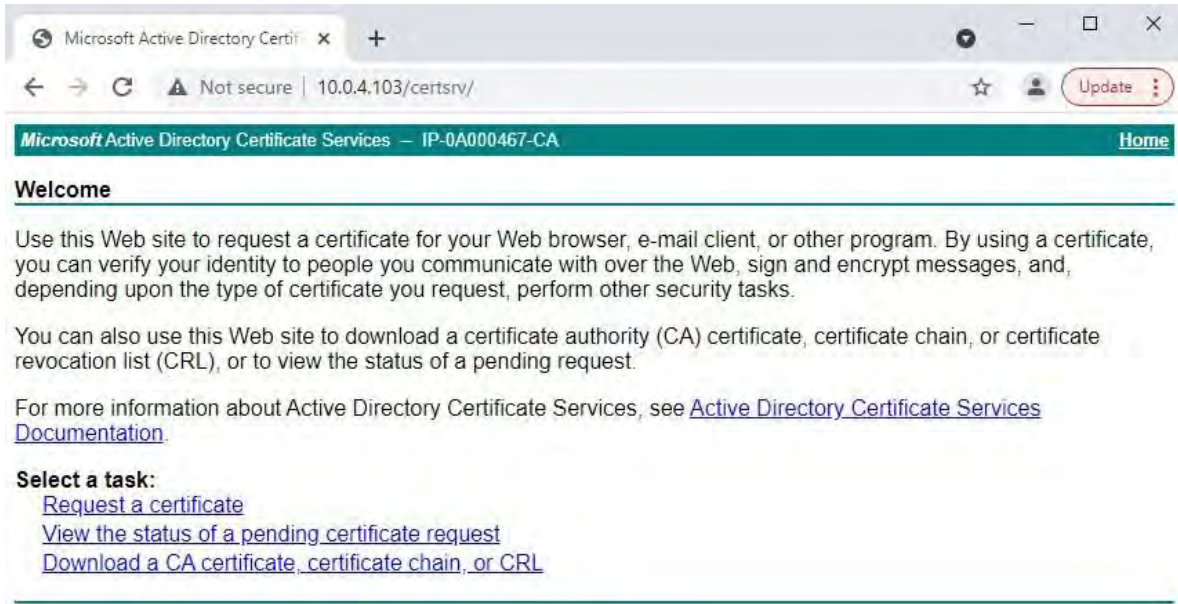
1. Busque la ubicación del archivo .req y ábralo en el Bloc de notas.



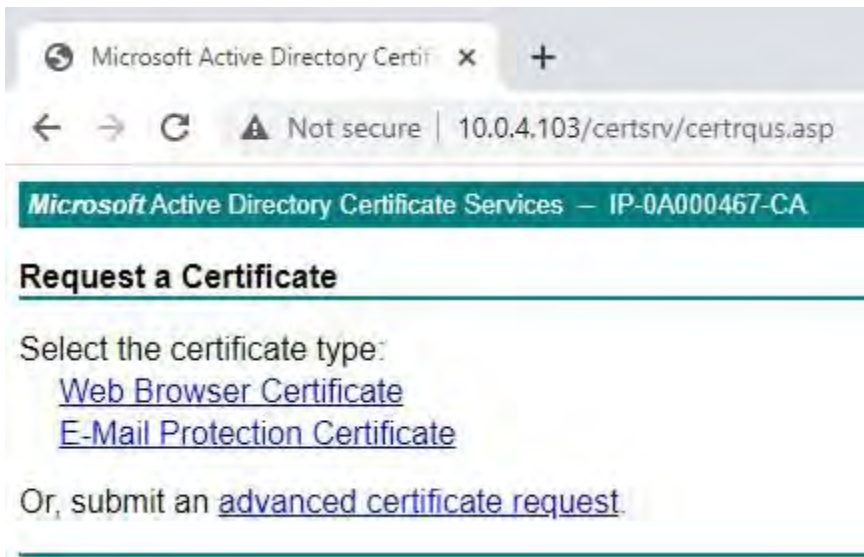
2. Copie todo el contenido del archivo. Esto incluye las líneas discontinuas que marcan el principio y el final de la solicitud de certificado.

3. Abra un navegador web e introduzca la dirección de la CA interna, que debe estar ubicada en: [ ip.ad.dr.ess/certsrv ].

Donde, ip.ad.dr.ess es la dirección IP o el nombre DNS del servidor host AD CS de la red interna.

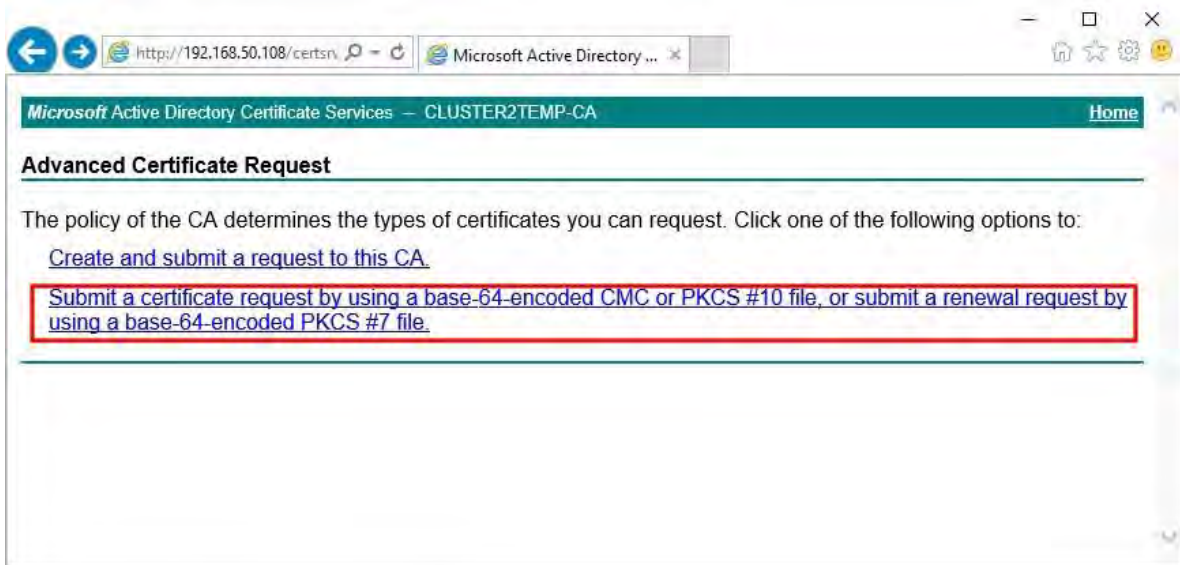


4. Haga clic en el **enlace Solicitar un certificado**.
5. Haga clic en el enlace de **solicitud de certificado avanzado**.

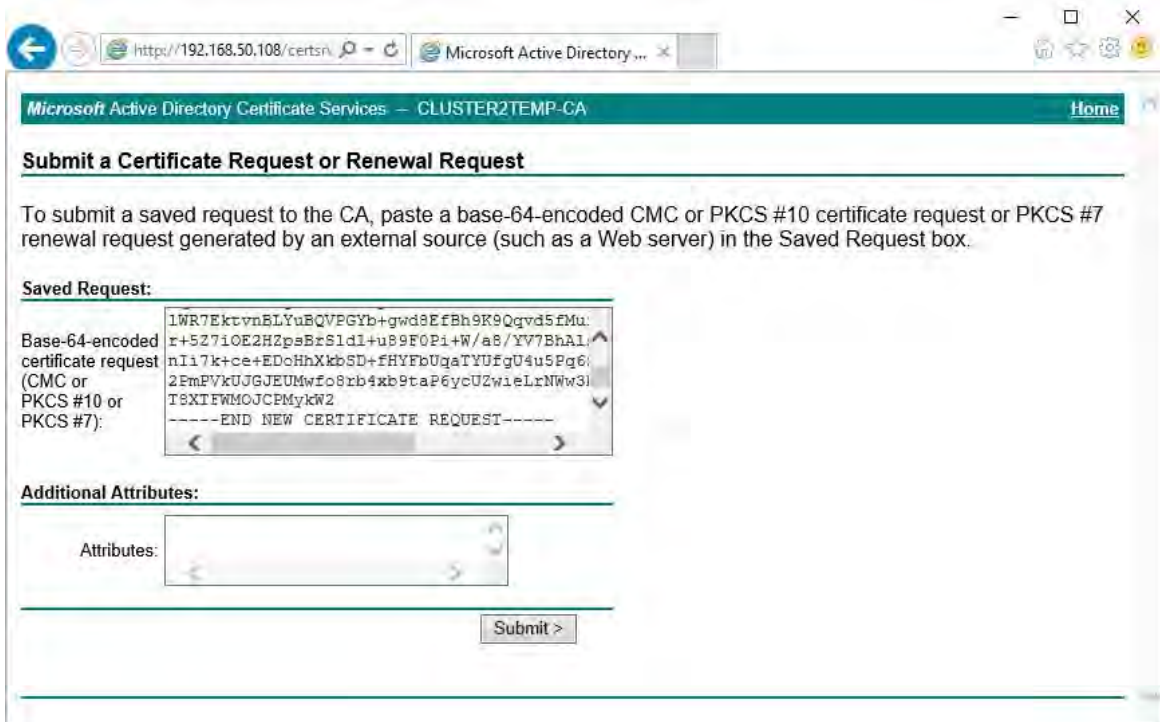




- 6. Elija Enviar una solicitud de certificado mediante un archivo CMC codificado en base 64.



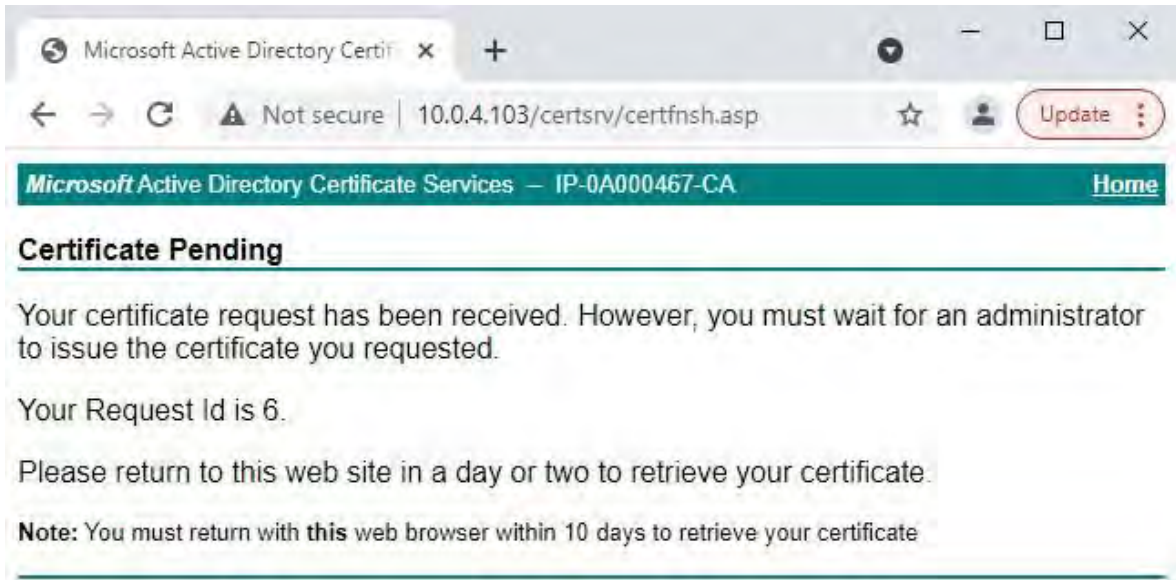
- 7. Pegue el contenido del archivo .req en el formulario. Si es necesario seleccionar una plantilla de certificado, seleccione **Servidor web** de la lista Plantilla de certificado.



8. Haga clic en **Enviar**.

El sitio muestra un mensaje que indica que el certificado se emitirá en unos días.

- Los servidores de CA internos se pueden utilizar para emitir certificados manualmente
- Anote la fecha y hora en que se presentó la solicitud de certificado

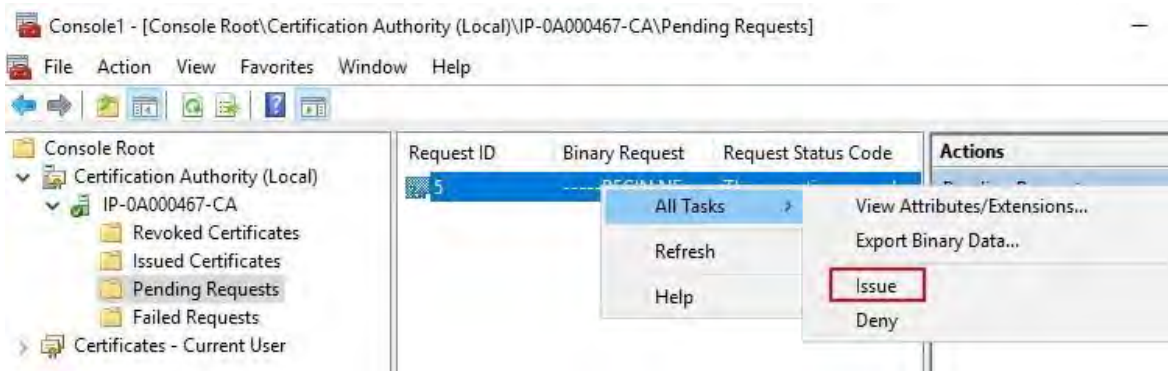


**Emisión manual de certificados**

Puede emitir certificados manualmente desde el equipo que hospeda los Servicios de certificados de Active Directory (AD CS).

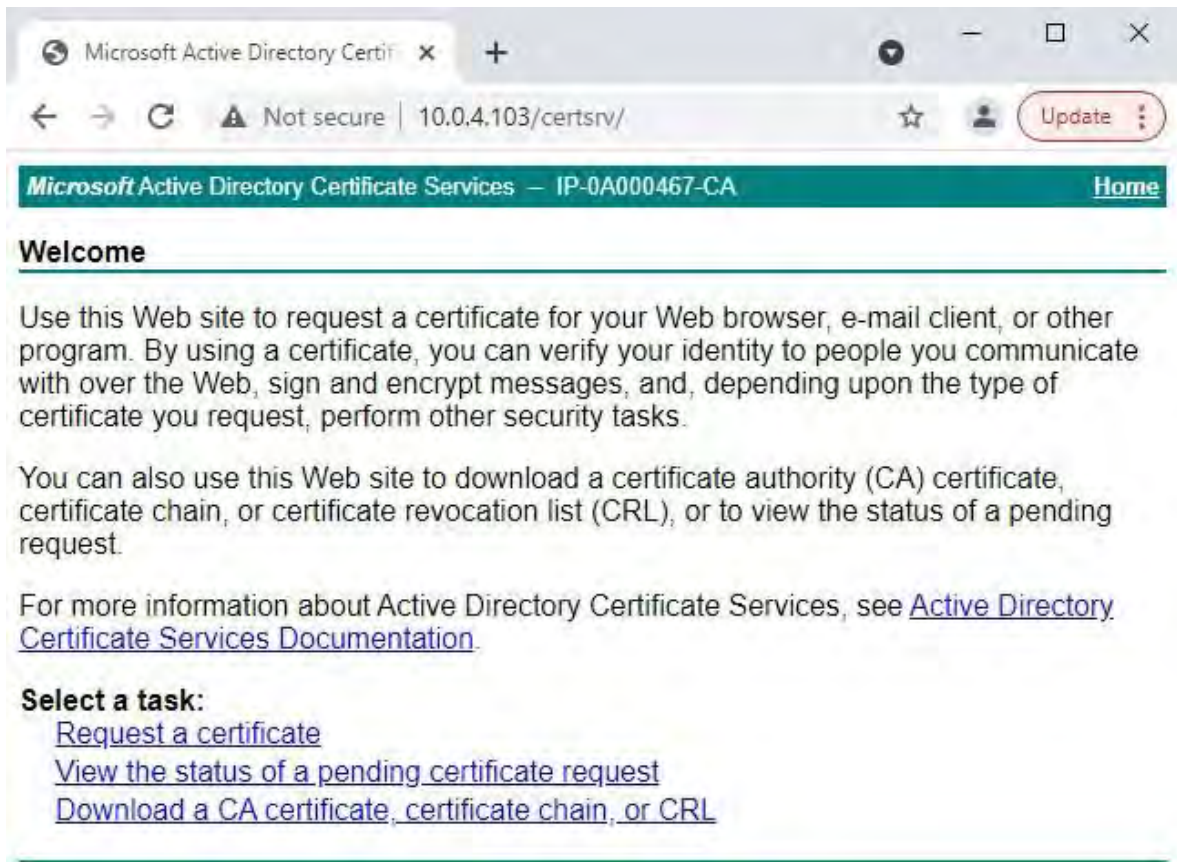
1. Abra Microsoft Management Console (MMC).
2. Vaya al **complemento Autoridad** de certificación.
3. Expanda el objeto **Autoridad de certificación**.

En la carpeta **Solicitudes pendientes**, haga clic con el botón derecho en el ID de solicitud correspondiente y, en la **lista Todas las tareas**, seleccione **Problema**.

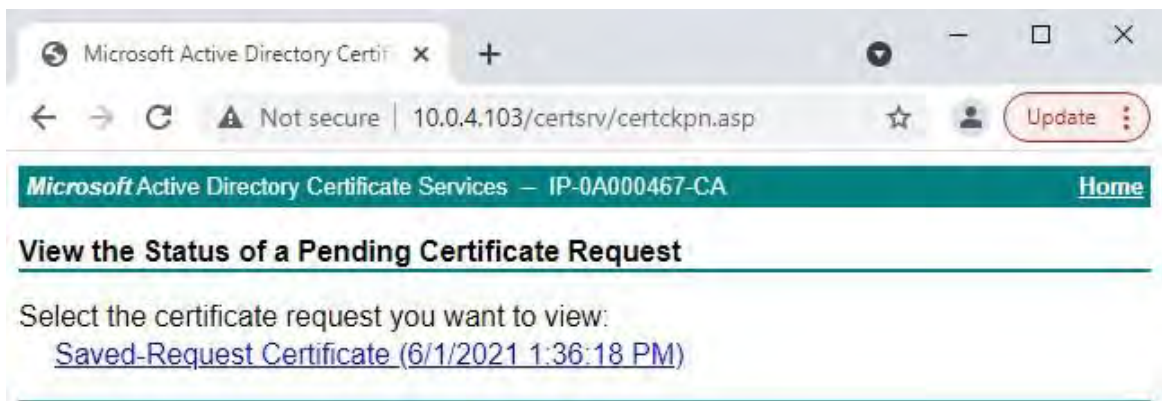


4. Abra un navegador y vaya al sitio interno de CA IIS ubicado en [ ip.ad.dr.ess/certsrv ].

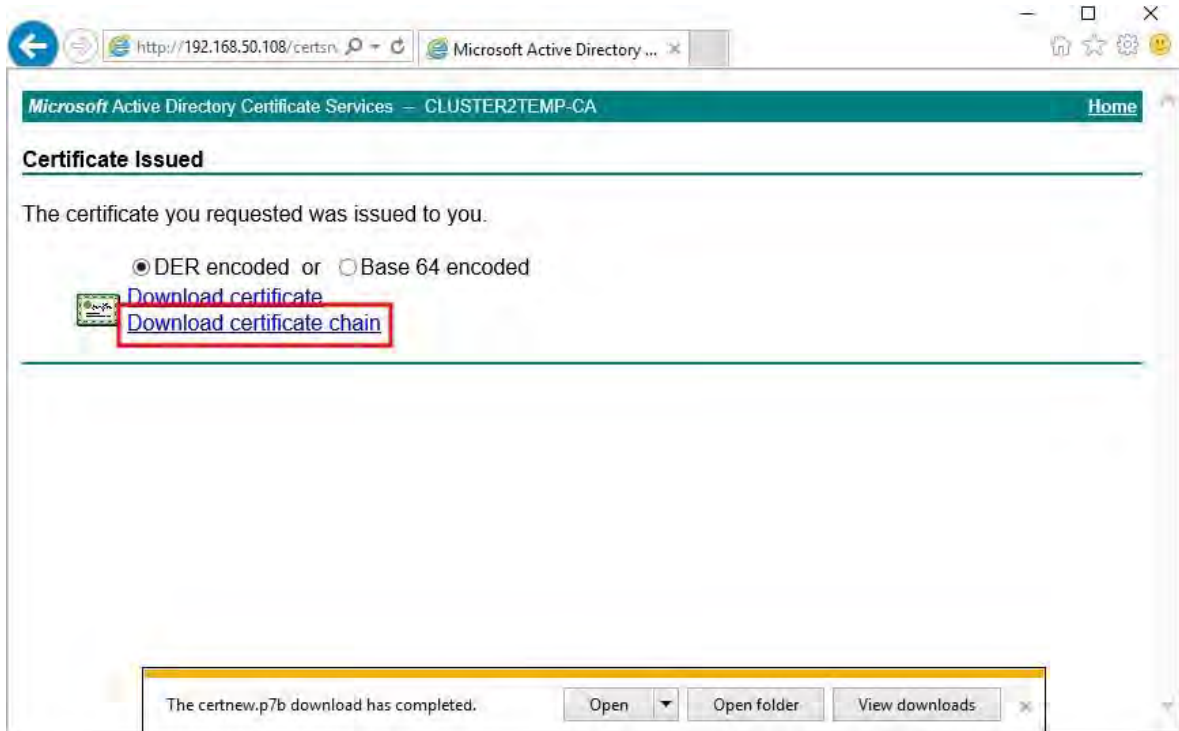
Haga clic en el enlace **Ver el estado de una solicitud de certificado pendiente**.



5. Si el certificado ha sido emitido, habrá un enlace disponible en la página resultante que contiene la fecha de la solicitud del certificado.



6. Seleccione **DER codificado** y descargue la cadena de certificados.

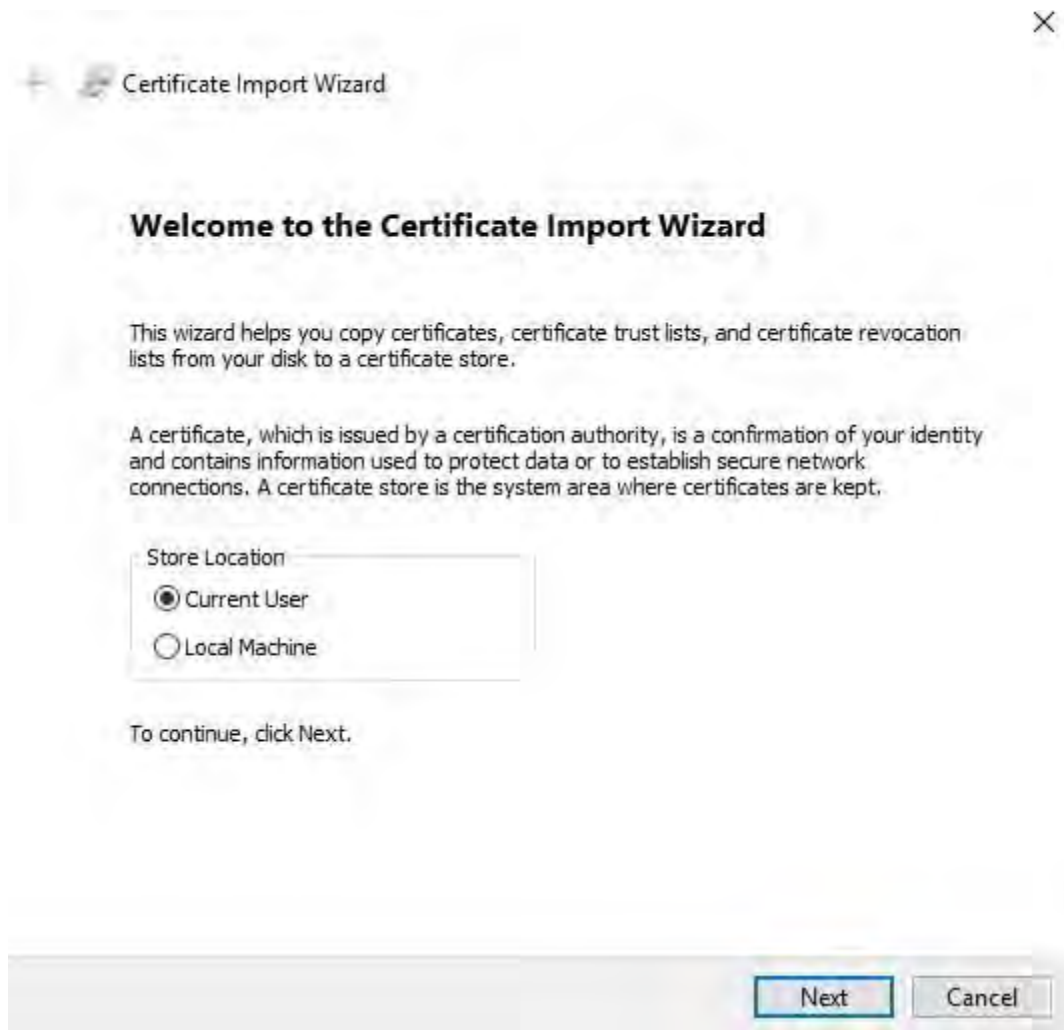


7. Vaya a la carpeta de descargas, haga clic con el botón derecho en el certificado y seleccione **Instalar certificado** en el menú contextual.



8. Acepte la advertencia de seguridad si aparece.

Seleccione esta opción para instalar el certificado para el usuario actual y haga clic en **Siguiente**.

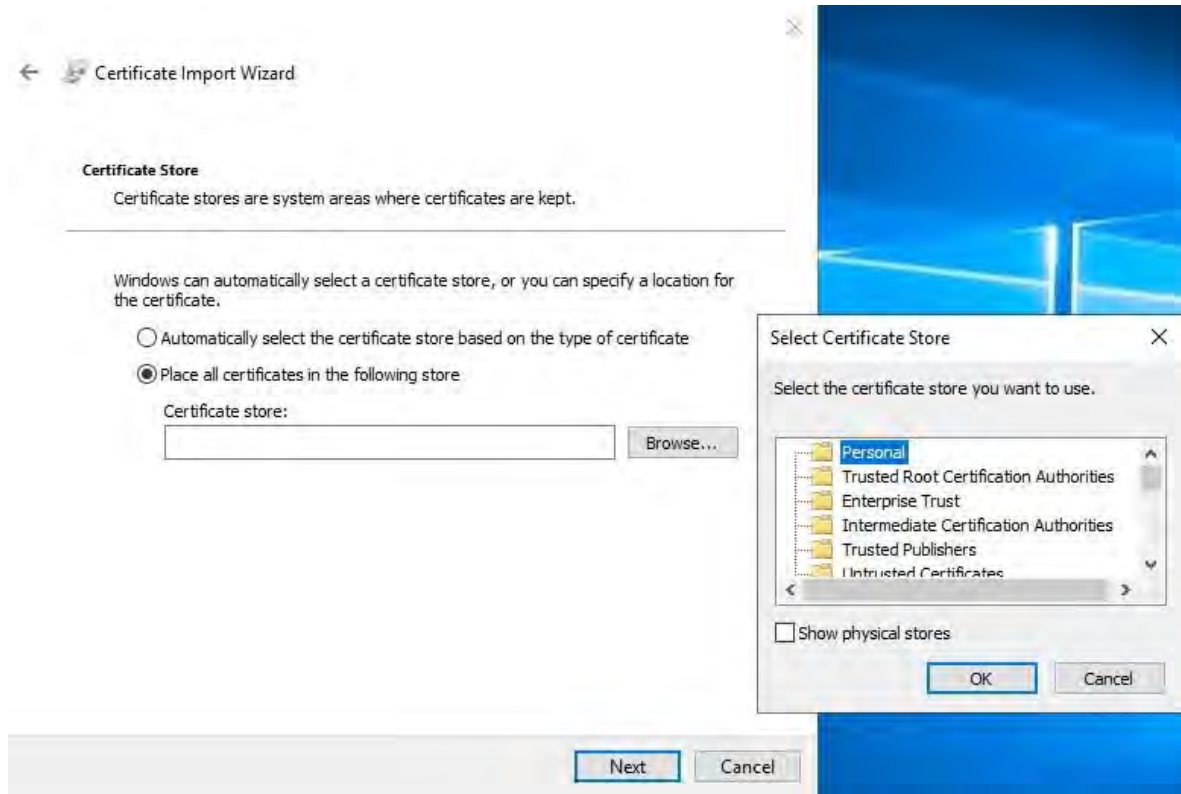


9. Elige una ubicación de tienda. Seleccione **Colocar todos los certificados en el siguiente almacén** y haga clic en el botón **Examinar** para abrir la ventana **Seleccionar almacén de certificados**.

Vaya al almacén de **certificados personales** y haga clic en

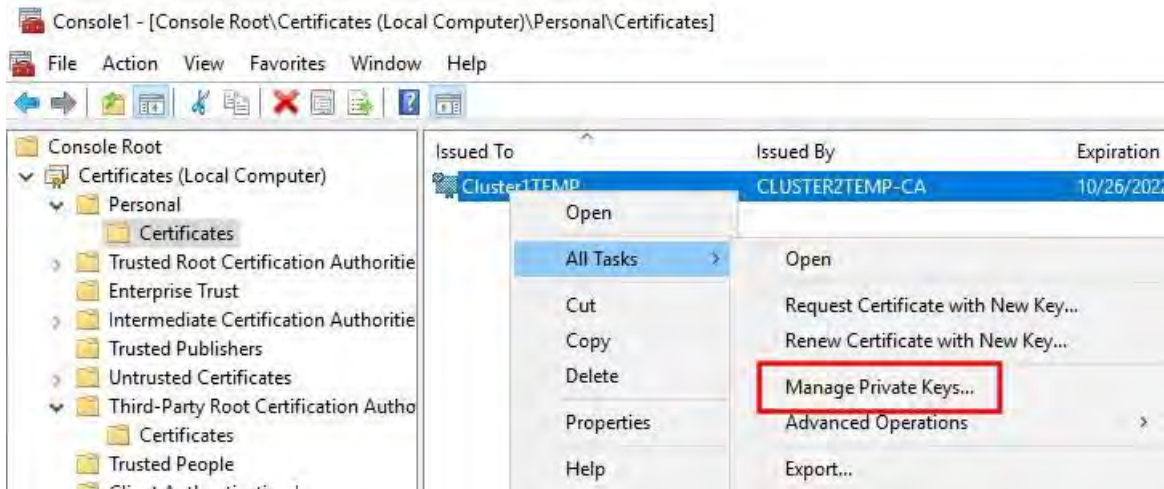
**Aceptar**.

Haga clic en **Siguiente**.



10. Finalice el **Asistente para la importación de certificados**.
11. Vaya al complemento **Certificados de Microsoft Management Console (MMC)**.

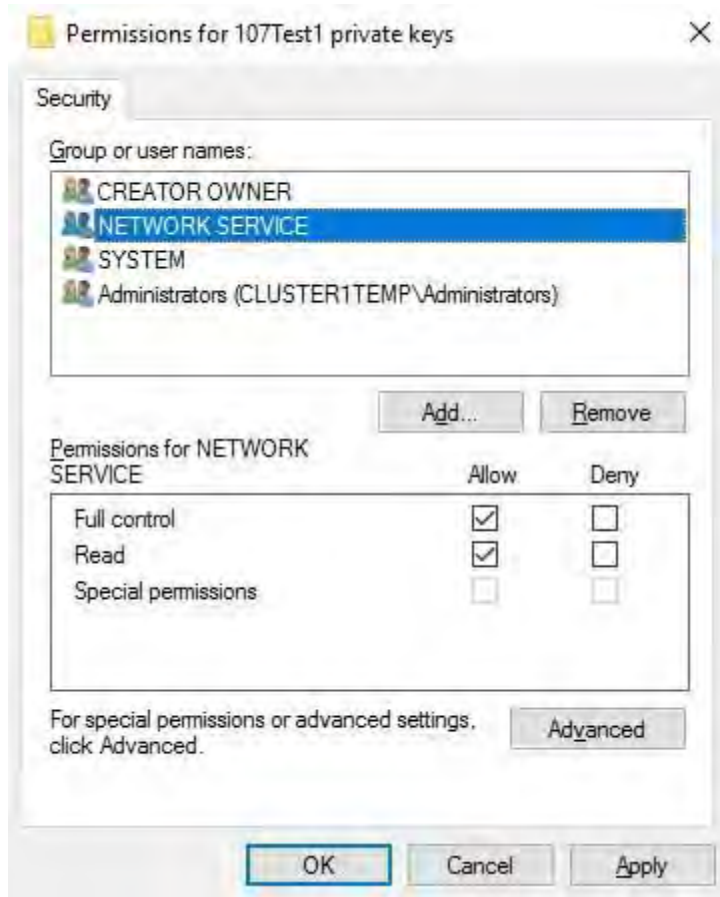
12. En la consola, vaya a la tienda personal donde está instalado el certificado. Haga clic con el botón derecho en el certificado y seleccione **Todas las tareas > Administrar claves privadas**.



13. Añada la cuenta que ejecuta el software MOBOTIX HUB Management Server, Recording Server o Mobile Server a la lista de usuarios con permiso para utilizar el certificado.

Asegúrese de que el usuario tenga habilitados los permisos Control total y Lectura.

De forma predeterminada, el software MOBOTIX HUB utiliza la cuenta NETWORK SERVICE.



### Habilitar el cifrado de servidor para servidores de administración y servidores de grabación

Una vez instalado el certificado con las propiedades y los permisos correctos, haga lo siguiente.

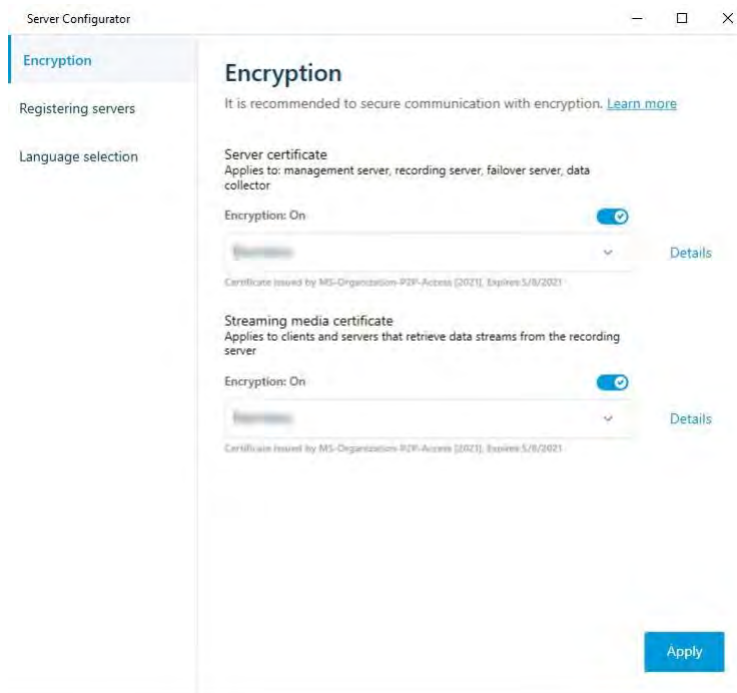
1. En un equipo con un servidor de administración o un servidor de grabación instalado, abra el **configurador de servidores**  
De:
  - El menú Inicio de Windowso
  - El administrador del servidor, haciendo clic con el botón derecho en el icono del administrador del servidor en la barra de tareas del equipo
2. En Server **Configurador**, en **Certificado de servidor**, active **Cifrado**.



3. Haga clic en **Seleccionar certificado** para abrir una lista con los nombres de los firmantes únicos de los certificados que tienen una clave privada y que están instalados en el equipo local en el Almacén de certificados de Windows.
4. Seleccione un certificado para cifrar la comunicación entre el servidor de grabación, el servidor de administración, el servidor de conmutación por error y el servidor del recopilador de datos.

Seleccione **Detalles** para ver la información del Almacén de certificados de Windows sobre el certificado seleccionado.

Al usuario del servicio del servidor de grabación se le ha dado acceso a la clave privada. Es necesario que este certificado sea de confianza en todos los clientes.



5. Haga clic en **Aplicar**.



Al aplicar certificados, el servidor de grabación se detendrá y se reiniciará. Detener el servicio del servidor de grabación significa que no puede grabar ni ver vídeo en directo mientras verifica o cambia la configuración básica del servidor de grabación.

## Instalar certificados para la comunicación con el servidor de eventos

Puede cifrar la conexión bidireccional entre el servidor de eventos y los componentes que se comunican con el servidor de eventos, incluido el servidor LPR. Cuando se habilita el cifrado en el servidor de eventos, se aplica a las conexiones de todos los componentes que se conectan al servidor de eventos. Antes de habilitar el cifrado, debe instalar certificados de seguridad en el servidor de eventos y en todos los componentes de conexión.



Cuando la comunicación del servidor de eventos está cifrada, esto se aplica a todas las comunicaciones con ese servidor de eventos. Es decir, solo se admite un modo a la vez, ya sea http o https, pero no al mismo tiempo.

El cifrado se aplica a todos los servicios hospedados en el servidor de eventos, incluidos Transact, Maps, GisMap e Intercommunication.



Antes de habilitar el cifrado en el servidor de eventos, todos los clientes (Desk Client y Management Client) y el plug-in MOBOTIX HUB LPR deben estar actualizados al menos a la versión 2022 R1.  
HTTPS solo se admite si todos los componentes se actualizan al menos a la versión 2022 R1.

La creación de los certificados es la misma que se describe en estas secciones, en función del entorno del certificado:

- [Instale certificados de CA comerciales o de terceros para la comunicación con el servidor de administración o el servidor de grabación en la página 57](#)
- [Instale certificados en un dominio para la comunicación con el servidor de administración o el servidor de grabación en la página 86](#)
- [Instale certificados en un entorno de grupo de trabajo para la comunicación con el servidor de gestión o el servidor de grabación en la página 104](#)

### Activar el cifrado del servidor de eventos de MOBOTIX HUB

Una vez instalado el certificado, puede habilitarlo para que se use con toda la comunicación con el servidor de eventos.



Una vez que todos los clientes se actualicen al menos a la versión 2022 R1, puede habilitar el cifrado en el servidor de eventos.

Puede cifrar la conexión bidireccional entre el servidor de eventos y los componentes que se comunican con el servidor de eventos, incluido el servidor LPR.



Al configurar el cifrado para un grupo de servidores, debe estar habilitado con un certificado que pertenezca al mismo certificado de CA o, si el cifrado está deshabilitado, debe estar deshabilitado en todos los equipos del grupo de servidores.

#### Prerrequisitos:

- Un certificado de autenticación de servidor es de confianza en el equipo que hospeda el

servidor de eventos En primer lugar, habilite el cifrado en el servidor de eventos.

Pasos:

1. En un equipo con un servidor de eventos instalado, abra Server **Configurator** desde:
  - El menú Inicio de Windows
  - o
  - El servidor de eventos haciendo clic con el botón derecho en el icono del servidor de eventos en la barra de tareas del equipo
2. En Server **Configurator**, en **Servidor de eventos y complementos**, active **Cifrado**.
3. Haga clic en **Seleccionar certificado** para abrir una lista con los nombres de los firmantes únicos de los certificados que tienen una clave privada y que están instalados en el equipo local en el Almacén de certificados de Windows.
4. Seleccione un certificado para cifrar la comunicación entre el servidor de eventos y los complementos relacionados.

Seleccione **Detalles** para ver la información del Almacén de certificados de Windows sobre el certificado seleccionado.



5. Haga clic en **Aplicar**.

Para completar la habilitación del cifrado, el siguiente paso es actualizar la configuración de cifrado en cada complemento relacionado en LPR Server.

## Importar certificados de cliente

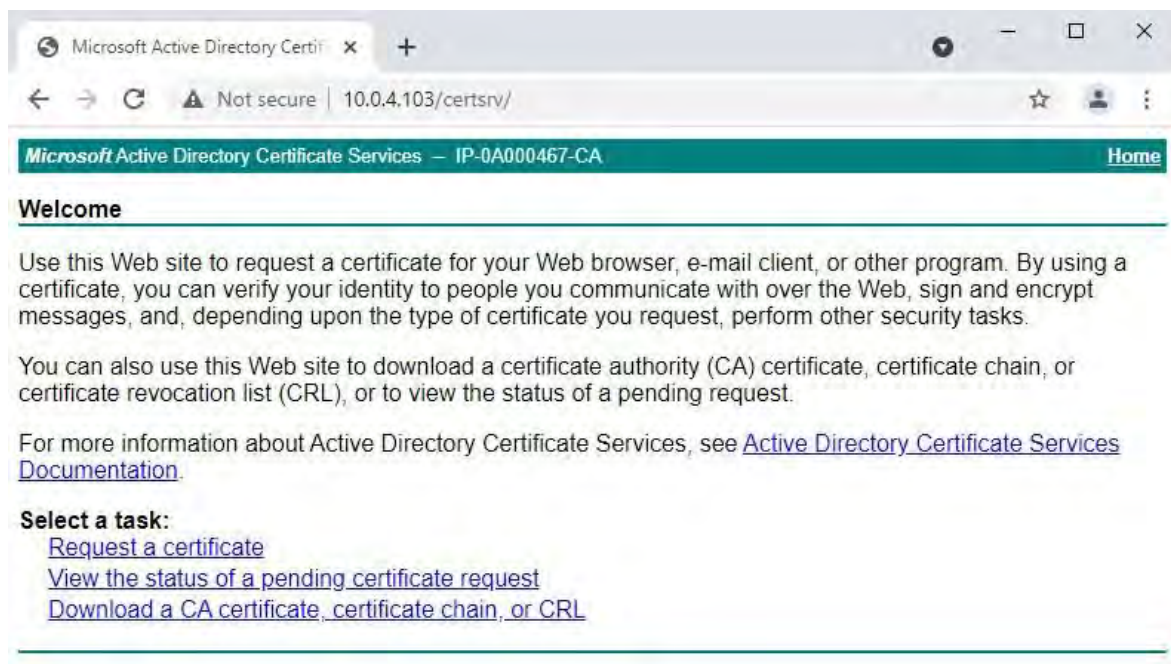
En esta sección se describe cómo importar certificados de cliente en una estación de trabajo o dispositivo cliente.

1. Después de importar un certificado de CA al servidor de administración o al servidor de grabación, puede acceder a él desde cualquier estación de trabajo o servidor de la red yendo a la siguiente dirección:

- <http://localhost/certsrv/>

Sin embargo, la dirección del servidor que contiene el certificado (clave privada) tomará el lugar de "localhost".

Por ejemplo:

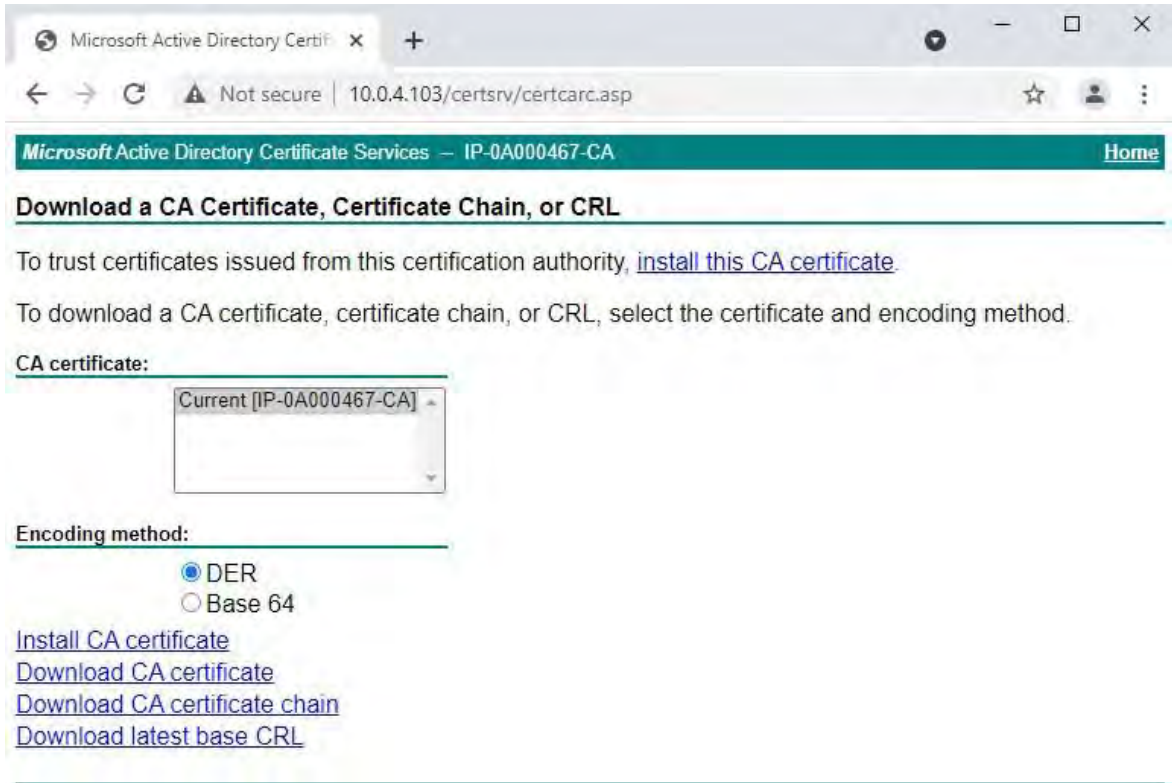


Este servidor web se hospeda en el servidor host de Servicios de certificados de Active Directory (AD CS) que contiene el certificado de CA.

2. Haga clic en **Descargar un certificado de CA, una cadena de certificados o una CRL**.

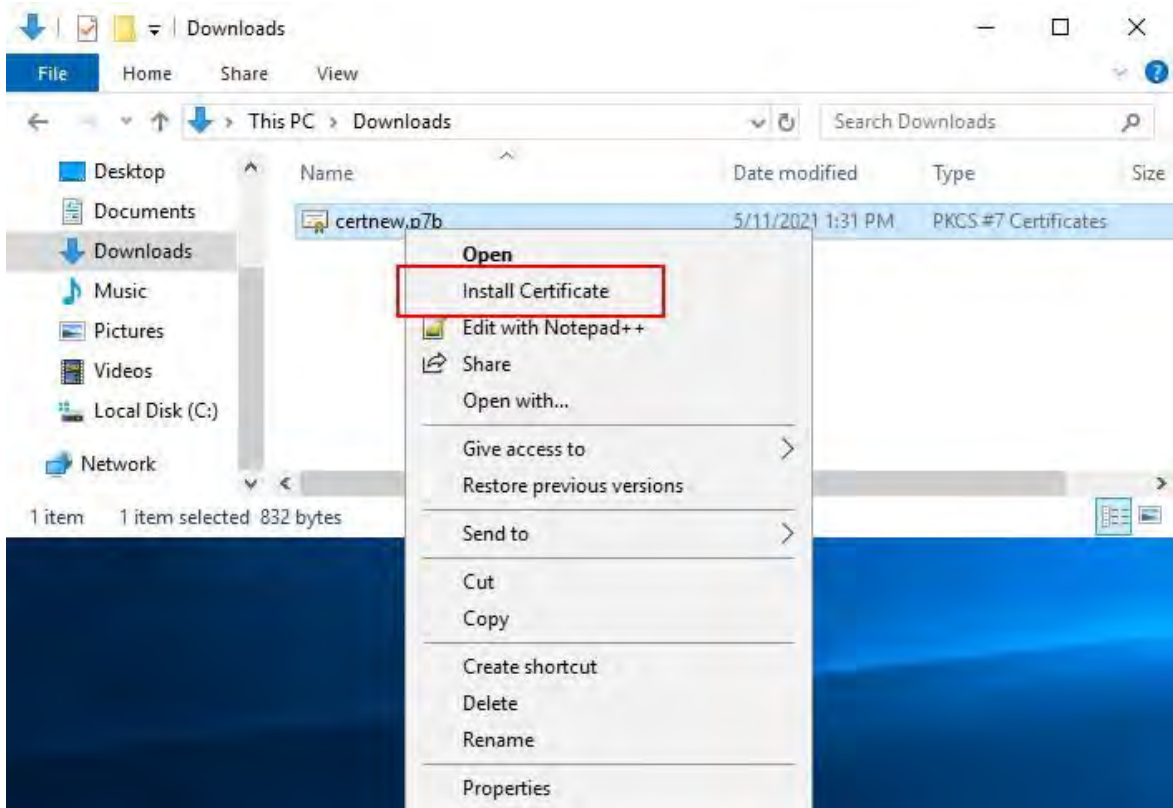
3. En el campo Certificado de **CA** , seleccione el certificado de CA que se utilizará con el sistema MOBOTIX HUB y haga clic en

**Descargue la cadena de certificados de CA.**



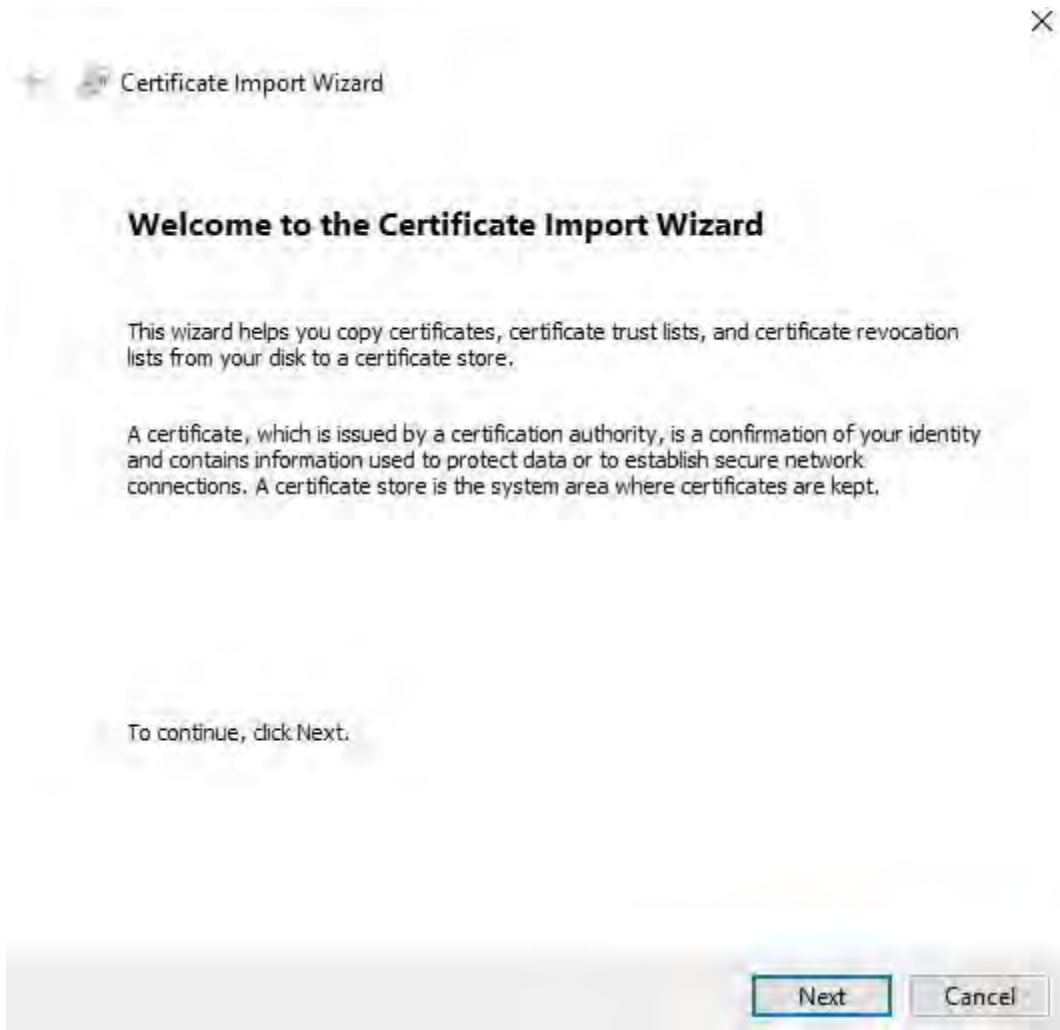
4. Seleccione **DER codificado** y descargue la cadena de certificados.

5. Vaya a la carpeta de descargas, haga clic con el botón derecho en el certificado y seleccione **Instalar certificado** en el menú contextual.



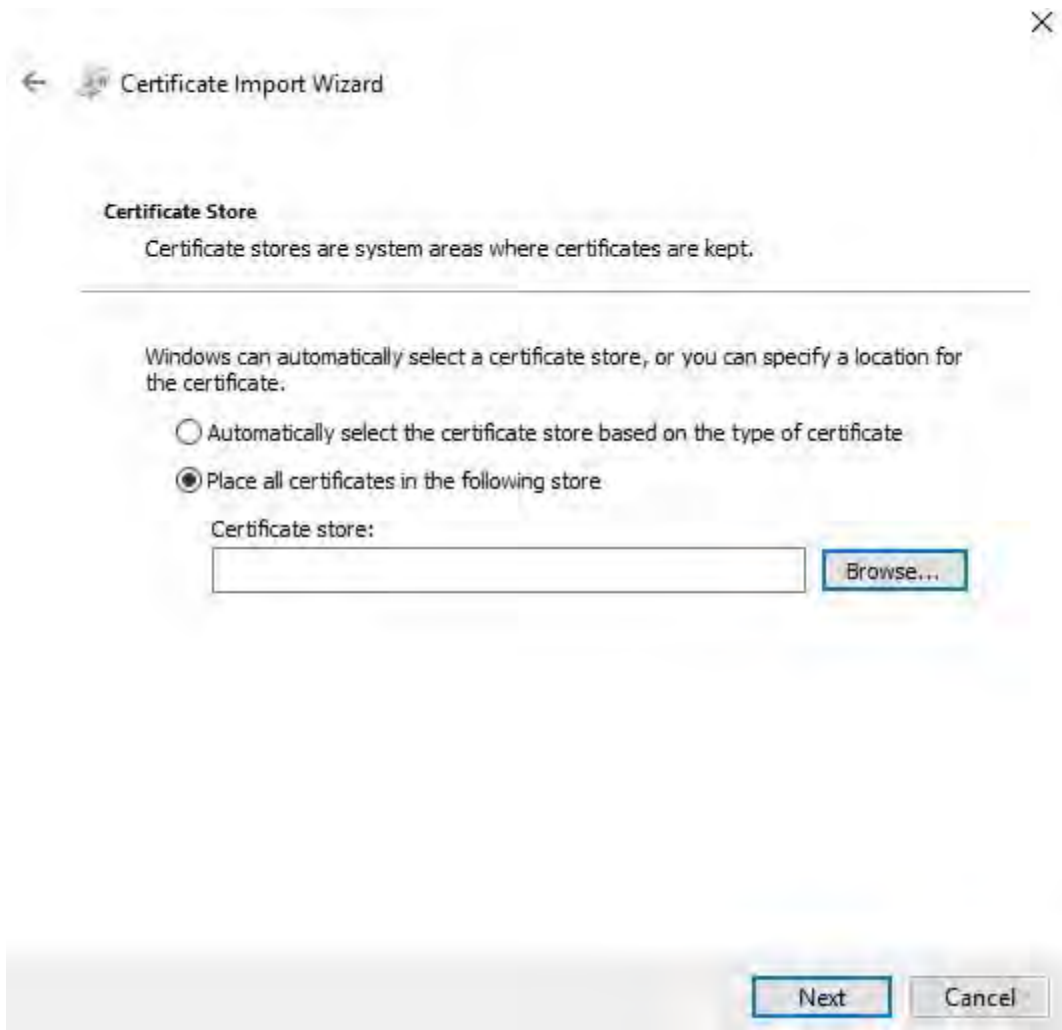
6. Se iniciará el Asistente para **la importación de certificados**.

Haga clic en **Siguiente**.

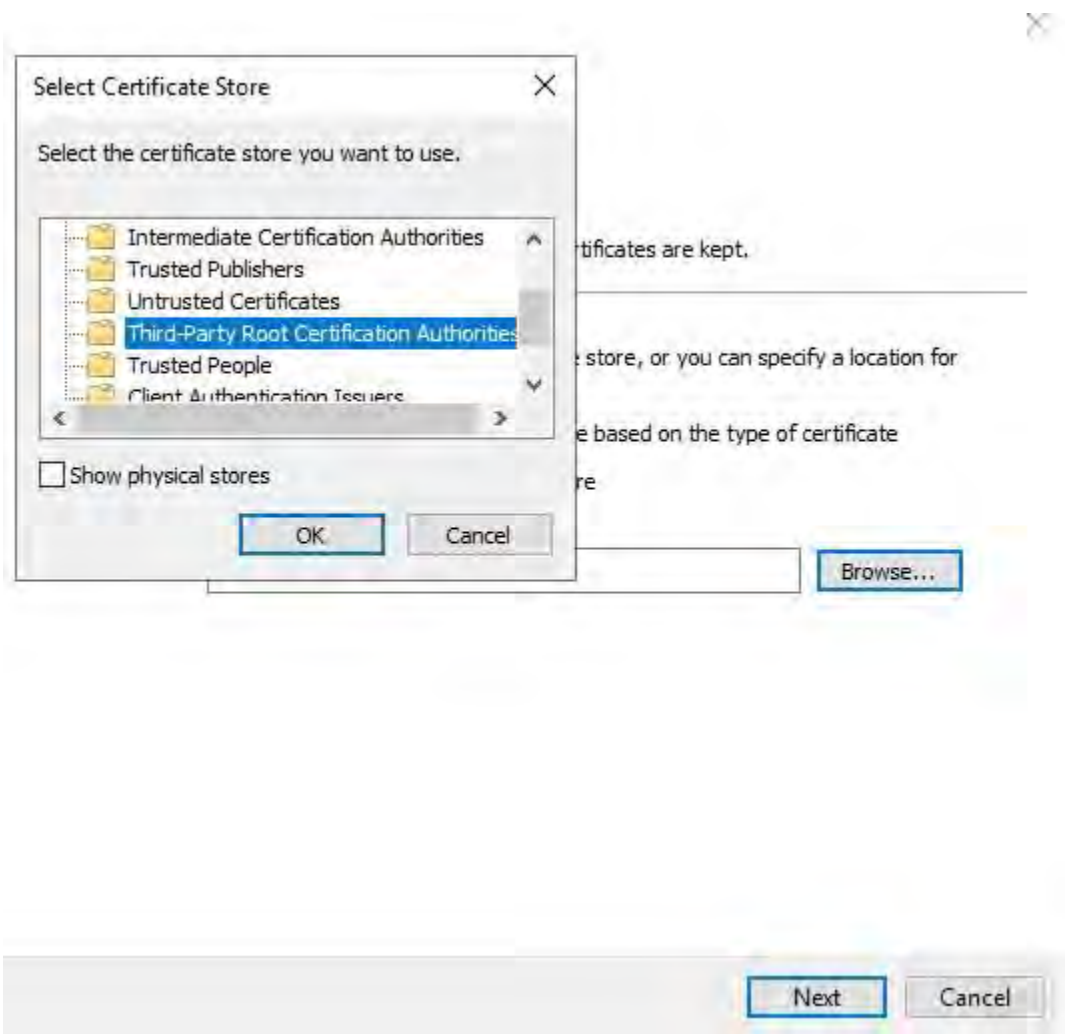




7. Elige una ubicación de tienda. Seleccione **Colocar todos los certificados en el siguiente almacén** y haga clic en el botón **Examinar** para abrir la ventana **Seleccionar almacén de** certificados.



- Vaya al almacén **de certificados de entidades de certificación raíz de terceros** y haga clic en **Aceptar**. Haga clic en **Siguiente**.



- Finalice el **Asistente para la importación de certificados**.

Ahora la estación de trabajo ha importado los componentes de certificado necesarios para establecer comunicaciones seguras con el servidor de gestión o el servidor de grabación.

## Ver el estado de cifrado de los clientes

Para verificar si el servidor de grabación cifra las conexiones:

1. Abra el cliente de administración.
2. En el panel Navegación del **sitio**, seleccione **Servidores > Servidores de grabación**. Esto abre una lista de servidores de grabación.
3. En el panel **Información general**, seleccione el servidor de grabación correspondiente y vaya a la **pestaña Información**.

Si el cifrado está habilitado para clientes y servidores que recuperan flujos de datos del servidor de grabación, aparece un icono de candado delante de la dirección del servidor web local y la dirección del servidor web opcional.

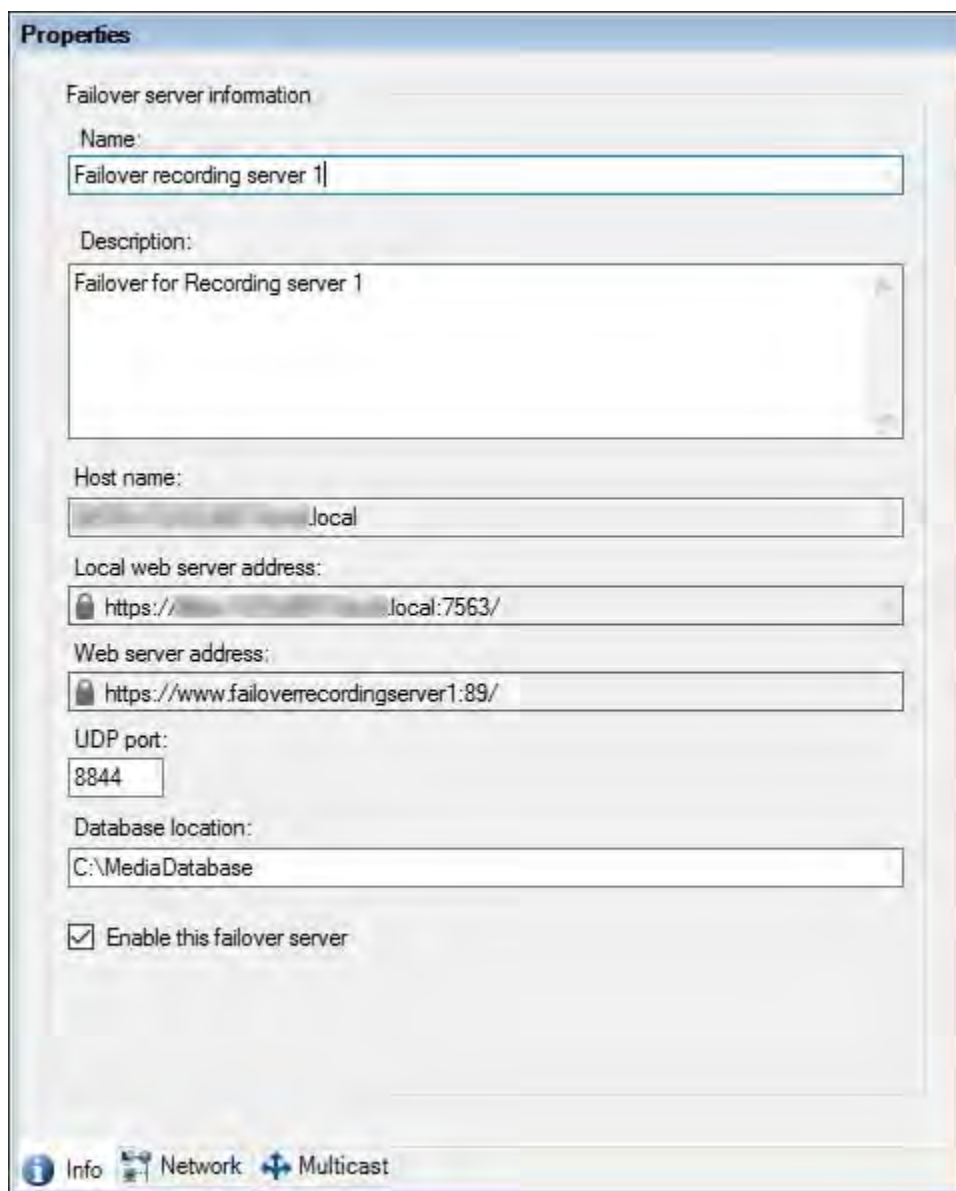


## Visualización del estado de cifrado en un servidor de grabación de conmutación por error

Para comprobar si el servidor de grabación de conmutación por error utiliza el cifrado, haga lo siguiente:

1. En el panel Navegación del **sitio**, seleccione **Servidores > Servidores de conmutación por error**. Esto abre una lista de servidores de grabación de conmutación por error.
2. En el panel **Información general**, seleccione el servidor de grabación correspondiente y vaya a la **pestaña Información**.

Si el cifrado está habilitado para clientes y servidores que recuperan flujos de datos del servidor de grabación, aparece un icono de candado delante de la dirección del servidor web local y la dirección del servidor web opcional.



# Ejecute este script una vez, para crear un certificado que pueda firmar varios certificados SSL de servidor

# Certificado privado para firmar otros certificados (en el almacén de certificados)

```
$ca_certificate = New-SelfSignedCertificate -CertStoreLocation cert:\CurrentUser\My -DnsName 'VMS Certificate Authority' -KeyusageProperty All '  
-KeyUsage CertSign, CRLSign, DigitalSignature -FriendlyName 'Certificado de CA VMS' '  
-TextExtension @"(2.5.29.19={crítico}{texto}ca=VERDADERO)"
```

# Huella digital del certificado privado utilizado para firmar otros certificados

```
set-content -path "$PSScriptRoot\ca_thumbprint.txt" -value $ca_certificate. Huella digital
```

# Certificado de CA pública en el que confiar (Autoridades de certificación raíz de terceros)

```
export-certificate -cert "cert:\CurrentUser\my\${$ca_certificate. Huella digital}" -FilePath "$PSScriptRoot\root-authority-public.cer"
```

```

# Ejecute este script una vez para cada servidor para el que se necesita un certificado SSL.
# El certificado debe ejecutarse en el único equipo donde se encuentra el certificado de CA. # El certificado SSL del servidor creado debe
moverse al servidor e importarse en el # almacén de certificados allí.
# Después de importar el certificado, permita el acceso a la clave privada del certificado para # el (los) usuario (s) del servicio de los
servicios que deben usar el certificado.

# Cargar certificado de CA desde la tienda (la huella digital debe estar en ca_thumbprint.txt)
$ca_thumbprint = get-content -path "$PSScriptRoot\ca_thumbprint.txt"
$ca_certificado = (Get-ChildItem -Path cert:\CurrentUser\My\$ca_thumbprint)

# Solicitar al usuario los nombres DNS para incluirlos en el certificado
$dnsNames = Read-Host 'Nombres DNS para el certificado SSL del servidor (delimitados por espacio - la 1ª entrada también está sujeta al certificado)'
$dnsNamesArray = @($dnsNames -split ' ' | foreach { $_. Recortar() } | donde { $_ })

if ($dnsNamesArray.Length -eq 0) {
    Write-Host -ForegroundColor Red 'Se debe especificar al menos un nombre dns' exit
}
$subjectName = $dnsNamesArray[0]
$dnsEntries = ($dnsNamesArray | foreach { "DNS=$_" }) -Unir '&'

# Opcionalmente, permitir que el usuario escriba una lista de direcciones IP para poner en el certificado
$ipAddresses = Read-Host 'Direcciones IP para el certificado SSL del servidor (defraudadas por espacio)'
$ipAddressesArray = @($ipAddresses -dividir ' ' | foreach { $_. Recortar() } | where { $_ }) if ($ipAddressesArray.Length -gt; 0)
{
    $ipEntries = ($ipAddressesArray | foreach { "IPAddress=$_" }) -Unir '&'
    $dnsEntries = "$dnsEntries&$ipEntries"
}

# Construya la cadena de entradas dns finales (por ejemplo, "2.5.29.17={texto}DNS=myhost&DNS=myhost.domain.com&IPAddress=10.0.0.103")
$dnsEntries = "2.5.29.17={texto}$dnsEntries"

# El único propósito requerido del programa es "Autenticación del servidor"
$serverAuthentication = '2.5.29.37={crítico}{texto}1.3.6.1.5.5.7.3.1'

# Ahora - crear el certificado SSL del servidor
$certificate = New-SelfSignedCertificate -CertStoreLocation cert:\CurrentUser\My -Subject $subjectName -Signer $ca_certificado '
-FriendlyName 'Certificado SSL VMS' -TextExtension @($dnsEntries, $serverAuthentication)

# Exportar certificado a disco: protéjalo con una contraseña
$password = Read-Host -AsSecureString "Contraseña del certificado SSL del servidor"
Export-PfxCertificate -cert "Cert:\CurrentUser\My\$($certificate. Huella digital)" -FilePath "$PSScriptRoot\$subjectName.pfx" -Password $password

# Eliminar el certificado SSL del servidor del almacén de certificados local
$certificate | Eliminar-Artículo

```

```

# Ejecute este script una vez para cada servidor de administración para el que se necesite un certificado.
# El certificado debe ejecutarse en el único equipo donde se encuentra el certificado de CA. # A continuación, el certificado creado debe
trasladarse a los servidores de gestión y
# importado en el almacén de certificados allí.

# Cargar certificado de CA desde la tienda (la huella digital debe estar en ca_thumbprint.txt)
$ca_thumbprint = get-content -path "$PSScriptRoot\ca_thumbprint.txt"
$ca_certificado = (Get-ChildItem -Path cert:\CurrentUser\My\$ca_thumbprint)

# Solicitar al usuario los nombres DNS para incluirlos en el certificado
$dnsNames = Read-Host 'Nombres DNS para el certificado del servidor de gestión (delimitados por comas: la 1ª entrada también está sujeta al certificado)'
$dnsNamesArray = @($dnsNames -dividir ',' | foreach { $_.Recortar() } | donde { $_ })

Si ($dnsNamesArray.Length -eq 0) {
    Write-Host -ForegroundColor Red 'Se debe especificar al menos un nombre dns' exit
}

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

# Opcionalmente, permitir que el usuario escriba una lista de direcciones IP para poner en el certificado
$ipAddresses = Read-Host 'Direcciones IP para el certificado del servidor de administración (delimitado por comas)'
$ipAddressesArray = @($ipAddresses -dividir ',' | foreach { $_.Recortar() } | donde { $_ }) if ($ipAddressesArray.Length -gt;
0) {
    $ipEntries = ($ipAddressesArray | foreach { "IPAddress=$_" }) -Unir '&'
    $dnsEntries = "$dnsEntries&$ipEntries"
}

$subjectName = $ipAddressesArray[0]

# Construya la cadena de entradas dns finales (por ejemplo, "2.5.29.17={text}DNS=myhost&DNS=myhost.domain.com&IPAddress=10.0.0.103")
$dnsEntries = "2.5.29.17={texto}$dnsEntries"

# El único propósito requerido del programa es "Autenticación del servidor"
$serverAuthentication = '2.5.29.37={crítico}{texto}1.3.6.1.5.5.7.3.1'

# Ahora: cree el certificado del servidor de administración
$certificate = New-SelfSignedCertificate -CertStoreLocation cert:\CurrentUser\My -Subject $subjectName -Signer $ca_certificate '
-FriendlyName 'Certificado de servidor VMS' -TextExtension @($dnsEntries, $serverAuthentication)

# Exportar certificado a disco: protéjalo con una contraseña
$password = Read-Host -AsSecureString "Contraseña del certificado del servidor de administración"
export-pfxCertificate -cert "cert:\CurrentUser\my\$($certificate.Huella digital)" -FilePath "$PSScriptRoot\$subjectName.pfx" -Password $password

# Eliminar el certificado del servidor de administración del almacén de certificados local
$certificate | Eliminar-Artículo

```

# MOBOTIX

BeyondHumanVision

ES\_02/25

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

MOBOTIX es una marca comercial de MOBOTIX AG registrada en la Unión Europea, EE. UU. y en otros países. Sujeto a cambios sin previo aviso. MOBOTIX no asume ninguna responsabilidad por los errores u omisiones técnicos o editoriales contenidos en este documento. Todos los derechos reservados. © MOBOTIX AG 2023