

MOBOTIX HUB – Guía de certificados

V2.03

Contenido

Derechos de autor, marcas comerciales y exención de responsabilidad	3
Acerca de esta guía	4
Introducción a los certificados	5
Información general sobre los escenarios y procedimientos utilizados con los certificados	8
¿Qué clientes necesitan certificados?	11
Configurador de servidores (explicado)	13
Scripts de PowerShell	16
Creación y distribución manual de certificados	17
Creación de un certificado de CA	17
Instalar certificados en los clientes	19
Crear certificado SSL	27
Importar certificado SSL	29
Creación de un certificado SSL para el servidor de administración de conmutación por error	38
Instalar certificados para la comunicación con el servidor móvil	40
Instale certificados de CA comerciales o de terceros para la comunicación con el servidor de administración	1, 0
Servidor de grabación	57
Instalación de Servicios de certificados de Active Directory	74
Instalación de certificados en un dominio para la comunicación con el servidor de gestión o el servidor de graba	ción 86
Instalación de certificados en un entorno de grupo de trabajo para la comunicación con el servidor de	gestión
o Servidor de Grabación	104
Instalar certificados para la comunicación con el servidor de eventos	126
Importar certificados de cliente	129
Ver el estado de cifrado de los clientes	135
Visualización del estado de cifrado en un servidor de grabación de conmutación por error	136
Apéndice A: Creación de un script de certificado de CA	137
Apéndice B: Crear script de certificado SSL de servidor	138
Apéndice C Creación de un script de certificado de servidor de administración de conmutación por error	139

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
- 5 | Introducción a Certificados

- 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.



• 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).

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).

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).

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.

J.

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 agregar 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.

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

) No Public Key Distribution Needed

Public Key Distribution Needed

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
 - 0
- 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

Milestone Server Configurator		÷	
Encryption	Encryption		
Registering servers	It is recommended to secure communication with encryption	. <u>Learn m</u>	ore
Language selection	Server certificate Applies to: management server, recording server, failover server, data collector Encryption: On		
	DocCert1 Certificate issued by mit-MJT-DC-CA, DC=mit, DC=local, Expires 4/27/2022 Mobile streaming media certificate Applies to mobile and web clients that retrieve data streams from the m server	~ nobile	Details
	Encryption: On	0	
	DocCert1	*	Details
	Certificate issued by mit-MUT-DC-CA, DC amit, DC alocal. Expires 4/27/2022		Apply

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:



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**).
- 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.

ø

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.

1	CreateCACertificate.ps1 - Notepad	×
File Edit Format View Help		
<pre># Run this script once, to creat # Private certificate for signir Sca_certificate = New-SelfSigned -KeyUsage CertSign, CRLSign, Dig # Thumbprint of private certific Set-Content -Path "SPSScriptRoot # Public CA certificate to trust xport-Certificate -Cert "Cert:</pre>	e a certificate that can sign multiple recording server certificates § other certificates (in certificate store) Certificate -CertStorelocation cert:\CurrentUser\My -DnsName 'VMS CertificateSignature -FriendlyName 'VMS CA Certificate' italSignature -FriendlyName 'VMS CA Certificate' ate used for signing other certificates (ca_thumbprint.txt" -Value \$ca_certificate.Thumbprint (Third-Party Root Certification Authorities) CurrentUser\My\\$(\$ca_certificate.Thumbprint)" -FilePath "\$PSScriptRoot\r	ficate Authority' -KeyusageProperty All ' moot-authority-public.cer"
¢		3
		Ln 8, Col 130

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.

📕 I 🔂 🖬 🗢 I			-		Cert		
File Open <u>n</u> ew window		Open Windows PowerShell	D	Open •	E Select all		
Open command prompt	•	Open Windows PowerShell as administrator	Properties	Edit History	Select none Invert selection Select		
Open Windows PowerShell							
			Da	te modified	Туре	Size	
CX Turning			04-	-02-2019 11:31	1 File folder		
O Halo			04-	-02-2019 11:31	1 File folder		
G Tielb			04-	-02-2019 11:31	1 File folder		
1			04-	-02-2019 11:31	1 File folder		
Close			04-	-02-2019 11:31	1 File folder		
			04-	-02-2019 11:31	1 File folder		
and the second sec		ReateCACertificate.ps1	31-	-01-2019 15:01	1 Windows PowerShell Script		1 KB
📕 This PC							
Destaura							

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.

 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.

	Open		F
	Install Certificate		ca -
4	Edit with Notepad++		
Ŧ	Scan with Windows Defender		
B	Share		
	Open with		
	Give access to	>	
	Restore previous versions		
	Send to	>	
	Cut		
	Сору		
	Create shortcut		
	Delete		
	Rename		

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

		×
F	🚑 Certificate Import Wizard	
	Welcome to the Certificate Import Wizard	
	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store,	
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
	Store Location	
	O <u>Current User</u>	
	To continue, click Next.	
	Sext Cance	

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

and the second se	
Certificate Store Certificate stores are system	reas where certificates are kept.
Windows can automatically set the certificate. Automatically select the Selace all certificates in t Certificate store:	ect a certificate store, or you can specify a location for certificate store based on the type of certificate re following store

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.

Certificate Import Wizard	
Completing the (Certificate Import Wizard
The certificate will be impor	rted after you dick Finish.
You have specified the follo	owing settings: by User Trusted Root Certification Authorities
Content	Certificate

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



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



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

File	nsole1 - [Console Root] Action View Favorites	Window	Help	- 🗆 X - # X
10	Open	Ctrl+N Ctrl+O	Name	Actions
	Save As	Cults	There are no items to show in this view.	Console Root
	Add/Remove Snap-in	Ctrl+M		More Actions
	Options			
	Recent File			
	Exit			

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

nap-in	Vendor	~	Console Root	Edit Extensions
ActiveX Control	Microsoft Cor	H		
Authorization Manager	Microsoft Cor			Feacle
Certificates	Microsoft Cor			
Component Services	Microsoft Cor			I Monster
Computer Managem	Microsoft Cor	r		These Devo
Device Manager	Microsoft Cor		<u>A</u> dd >	
Event Viewer	Microsoft and	4		
Folder	Microsoft Cor			
Group Policy Object	Microsoft Cor			
Internet Informatio	Microsoft Cor			
Internet Informatio	Microsoft Cor			
IP Security Monitor	Microsoft Cor	4		Advanced
		-	-	

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

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

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.

Snap-in Vendor Console Root Edit ActiveX Control Microsoft Cor Certificates (Local Computer) Edit Authorization Manager Microsoft Cor Certificates (Local Computer) Edit Component Services Microsoft Cor Computer Managem Microsoft Cor Computer Manager Microsoft Cor Microsoft Cor Device Manager Microsoft Cor Add > Event Viewer Microsoft Cor Add >

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

Eile <u>A</u> ction ⊻iew Fav <u>o</u> rites <u>W</u> indow <u>H</u> e ■ ● ▲ 〒 □ □ 0 → 1 0 ■	lp				-	£ .
Console Root	Issued To	Issued By	Ex¢ ^	Actions		_
Certificates (Local Computer)	10.5.14.40	10.5.14.40	20:	Certificates		
 Personal Personal Trusted Root Certification Authorities Certificates Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Third-Party Root Certification Authorities Trusted People Client Authentication Issuers Preview Build Roots AAD Token Issuer ESIM Certificates Remote Desktop Certificate Enrollment Requests Smart Card Trusted Roots Trusted Devices Web Hosting Windows Live ID Token Issuer 	IO.5.6.101 AddTrust External CA Root AddTrust External CA Root AddTrust External CA Root Class 3 Public Primary Certificat Copyright (c) 1997 Microsoft C DigiCett Assured ID Root CA DigiCett High Assurance EV Ro DST Root CA X3 Equifax Secure Certificate Auth Geo Trust Global CA GlobalSign GlobalSign Root CA Go Daddy Class 2 Certification Grosoft Root CA -03 Microsoft Root CA tuthenicode(tm) Ro Microsoft Root CA -03 Microsoft Root Certificate Auth Microsoft Root	10.5.6.101 AddTrust External CA Root Baltimore CyberTrust Root CKMS Class 3 Public Primary Certificatio Copyright (c) 1997 Microsoft Corp. DigiCert Assured ID Root CA DigiCert High Assurance EV Root DST Root CA X3 Equifax Secure Certificate Authority GeoTrust Global CA GlobalSign GlobalSign GlobalSign Root CA Go Daddy Class 2 Certification Au GTE CyberTrust Global Root Hotspot 2.0 Trust Root CA - 03 Microsoft Root Authority Microsoft Root Certificate Authori Microsoft Root Certificate Authori Starfield Class 2 Certification Auth Starfield Services Root Certificate Symantec Enterprise Mobile Root	20: 202 203 203 203 203 203 203 203 203 203	More Actions		

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.



Ì

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.

 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.

Open <u>n</u> ew window	*	Open Windows PowerShell		Den • 🔡 S	elect all elect none		
Open command <u>p</u> rompt	•	Open Windows PowerShell as ac	Pro	v History 🔡 Ir Open	vert selection Select		
Open Windows Powe <u>r</u> Shell							
D				Date modified	Туре	Size	
Delete history				04-02-2019 11:31	File folder		
and a second sec				04-02-2019 11:31	File folder		
Пер	1			04-02-2019 11:31	File folder		
				04-02-2019 11:31	File folder		
Liose				04-02-2019 11:53	File folder		
				04-02-2019 11:31	File folder		
Q		CreateCA	Certificate.ps1	31-01-2019 15:01	Windows PowerShell Script		11
📕 This PC		CreateSer	verCertificate.ps1	25-01-2019 15:31	Windows PowerShell Script		31

- 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**.





8. 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**.

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.

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

10. 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.

1. 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**.

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

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

ile to Import			
Specify the file you wa	ant to import.		
File name:			
C: Users\gis\Docume	nts Wy Received File	s\VMS-REC-01.pb	Browse
Note: More than one	certificate can be sto	red in a single file in t	he following formats
Personal Informatio	on Exchange-PKCS #	12 (.PFX,.P12)	
Cryptographic Mess	sage Syntax Standard	d- PKCS #7 Certificat	es (.P7B)
Microsoft Serialized	Certificate Store (.S	ST)	

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

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

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

Contificate stores are sustem areas	and the second sec	- Arreste
Cerunicate stores are system areas	where certificates an	e kept,
Windows can automatically select a	certificate store, or v	you can specify a location for
the certificate.		(
 Automatically select the cert 	ficate store based on	the type of certificate
Place all certificates in the form	llowing store	
Certificate store:		
Personal		Browse

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

The certificate will be imported after	vou dick Finish.
Certificate Store Selected by User Content File Name	Personal PFX C:\Users\gis\Desktop\VMS-REC-01.pfx

9. El certificado importado aparece en la lista.

- 🔿 🙍 💼 🗈 🖉 💼		
Certificates - Local Computer Personal Certificates Certificates Certificates Certificates Certification Authorities Certification Authorities Certification Authorities Certification Authorities Certificates Cuntrusted Publishers Cuntrusted Certification Authorities Cintrusted Publishers Cintrusted Certificates Cintrusted People Client Authentication Issuers Cintrusted People Client Authentication Issuers Cintrusted Publichers Cintrusted People Client Authentication Issuers Cintrusted People CificeScan SSL Agent CificeScan SSL A	Issued To	Issued By Iocalhost VMS Certificate Authority VMS Certificate Authority

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.

Open
Request Certificate with New Key
Renew Certificate with New Key
Manage Private Keys
Advanced Operations
Export
11. Añada permiso de lectura para el usuario que ejecuta los servicios de MOBOTIX HUB VMS y que necesita utilizar el certificado de servidor.

aroup or user names:		
SYSTEM		
Administrators (Administrator	s)	
METWORK SERVICE		
	Add	Remove
ermissions for NETWORK	1200	
ERVICE	Allow	Deny
Full control		
Read	D	
Special permissions		
A REAL PROPERTY AND A REAL PROPERTY A REAL PROPERTY AND A REAL PROPERTY A	ed settings	
or special nermissions or advance	ou sounigs,	Advanced
or special permissions or advanc lick Advanced.		

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

- 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.
- En el menú Archivo, seleccione Abrir Windows PowerShell y, a continuación, Abrir Windows PowerShell como administrador.

Open <u>n</u> ew window	*	Open Windows PowerShell		Dpen •		Select all Select none		
Open command prompt		Open Windows PowerShell as administrator	Propertie	s 🕢 History Open		Invert selection Select		
Open Windows Powe <u>r</u> Shell	*							
D				Date modifie	d	Туре	Size	
				04-02-2019 1	1:31	File folder		
Hala				04-02-2019 1	1:31	File folder		
Tich				04-02-2019 1	1:31	File folder		
·				04-02-2019 1	1:31	File folder		
Llose				04-02-2019 1	1:53	File folder		
				04-02-2019 1	1:31	File folder		
Sec. J.		CreateCACertificate.ps1	2	31-01-2019 1	5:01	Windows PowerShell Script		1.K
🜉 This PC		CreateServerCertificate.r	os1	25-01-2019 1	5:31	Windows PowerShell Script		3.K

38 | Creación de un certificado SSL para el servidor de

Guía de certificados | MOBOTIX HUB® VMS

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.



1

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 v 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....

🚡 Fil	Action View Favorites Wind	w Help	- 8 ×
	Open Ctrl+	Name	Actions
	Save Ctrl+	There are no items to show in this view.	Console Root
	Save Ctrl+ Save As Add/Remove Snap-in Ctrl+ N Options Recent File Exit	There are no items to show in this view.	Console Root Actions

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

ailable snap-ins:			Selected snap-ins:	
inap-in	Vendor	A	Console Root	Edit Extensions
ActiveX Control	Microsoft Cor.	11	Certificates - Current User	
Authorization Manager	Microsoft Cor			Remove
Certificate Templates	Microsoft Cor			
Certificates	Microsoft Cor			Uperla
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor			Marine Crewn
Computer Managem	Microsoft Cor		>	
Device Manager	Microsoft Cor			
Disk Management	Microsoft and			
Enterprise PKI	Microsoft Cor			
Event Viewer	Microsoft Cor			
Folder	Microsoft Cor			
Group Policy Object	Microsoft Cor			Advanced
San and and and		*		Advanceum
scription				

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

sole Root Certificates - Current	: User Object	t Type tificates	
Tri Find Ce	rtificates		
En All Task	s >	Find Certificates	
Ac View	ndow from Here	Request New Certificate Import	
Th New Ta	skpad View	Advanced Operations	Create Custom Request
Tri Refresh	ist		Enroll On Behalf Of Manage Enrollment Policies
Sn Help			

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

Haga clic en Siguiente.

	V
-	\sim

Certificate Enrollment

Select Certificate Enrollment Policy

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

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

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

Lo ver a F h		0.4
Certificate Enrollment		
Custom request		
Chose an option from	the list below and configure the certificate option	s as required.
Template:	(No template) CNG key	
	<u>Suppress</u> default extensions	
Request format:	○ <u>P</u> KCS #10	
	● <u>C</u> MC	
		<u>N</u> ext Cancel

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.

easier to iden	tify and use a cer	rtificate.
OF	Cristel	Apply
	ОК	OK Cancel

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:

General	Subject	Extensions	Private Key	Signature		
The sub can ent can be (oject of a er inform used in a	certificate is ation about certificate.	the user or c the types of :	omputer to w subject name	hich the certificate is and alternative nam	s issued. You e values that
Subject	of certifi	cate				
The use	r or com	puter that is	receiving the	certificate		
Subject	name:					
Type:			-		CN=Test for Doc	5
Count	rv.			Add -	O=MJT	
Value	.,				L=Maple Grove	
value			×	Remove	S=MN	
_					C=USA	
Alternat	tive name	2	-		ň.	
Туре:					1.00	
Direct	ory name					
Value:				i data		
				400		
			1	Remove		
			_			
				OK	Cancel	Apply

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**.

Seneral Subject Extensions Private Key Signature The following are the certificate extensions for this certificate type. Key usage The key usage extension describes the purpose of a certificate. Available options: CRL signing Data encipherment Decipher only Encipher only Key agreement Non repudiation Image: Constraints OK Cancel Apply	Certificat	te Propert	ties					3
The following are the certificate extensions for this certificate type. Key usage Key usage extension describes the purpose of a certificate. Available options: CRL signing Data encipherment Decipher only Add > Selected options: Digital signature Key encipherment Key agreement Non repudiation Remove Make these key usages critical Make these key usages critical Make these key usage (application policies) Make constraints OK Cancel Apply 	General	Subject	Extensions	Private Key	Signature			
Key usage The key usage extension describes the purpose of a certificate. Available options: CRL signing Data encipherment Decipher only Encipher only Key agreement Non repudiation Image: Constraints OK Cancel	The fol	lowing an	e the certific	ate extensior	ns for this co	ertificate	type.	^
The key usage extension describes the purpose of a certificate. Available options: Selected options: CRL signing Data encipherment Decipher only Add > Encipher only Add > Key agreement Non repudiation Make these key usages critical Extended Key Usage (application policies) OK Cancel	Key u	sage						*
Available options: CRL signing Data encipherment Decipher only Encipher only Key agreement Non repudiation Make these key usages critical Extended Key Usage (application policies) Basic constraints OK Cancel Apply	The ke	y usage e	extension des	cribes the pu	urpose of a	certificate	e,	
CRL signing Data encipherment Decipher only Encipher only Key agreement Non repudiation < Remove	Availal	ble option	15:			Selec	ted options:	
Decipher only Encipher only Key agreement Non repudiation < Remove	CRL si Data e	gning ncipherm	ient	11		Digit Key d	al signature certificate signi	ng
Encipher only Key agreement Non repudiation Make these key usages critical Make these key usages critical Extended Key Usage (application policies) Basic constraints	Decipł	ner only		-		Key e	encipherment	
Non repudiation Key agreement Non repudiation Key agreement Make these key usages critical Extended Key Usage (application policies) Basic constraints OK Cancel Apply	Enciph	ner only		A	dd >			
Kennepetitietten Make these key usages critical Extended Key Usage (application policies) Basic constraints	Key ag	reement		-		2		
✓ Make these key usages critical Extended Key Usage (application policies) Basic constraints OK Cancel	Non re	providuo	"	< R	emove			
Extended Key Usage (application policies)	⊠ Mał	ce these k	ey usages cr	itical				
Basic constraints	Exten	ded Key U	lsage (applic	ation policie	s)			*
OK Cancel Apply	Basic	constrain	ts					*
OK Cancel Apply								
					0	ж	Cancel	Apply

1

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.

	operti	es					×
General Sul	bject	Extensions	Private Key	Signature			
Cryptogra	aphic S	ervice Prov	ider				۲
Key option	ns						*
Set the key	/ lengt	h and expor	t options for	r the private	key.		
Key size:	2048				~		
Make pr	rivate	cey exportal	ble				
Allow p	rivate	key to be an	chived				
		tel to be at					
Strong	orivate	key protect	tion				
Strong p	private	key protect	tion				
Select Has	private sh Alg	key protect	tion				*
Select Has	private sh Algo h Algo	key protect orithm	tion used for thi	s request			*
Select Has Select Has Hash Algo	private sh Algo h Algo rithm:	key protect orithm orithm to be sha256	tion used for thi	s request		~	*
Select Has Select Has Select Hasl Hash Algo	private sh Algo h Algo rithm:	key protect orithm orithm to be sha256	tion used for thi	s request		~	*
Select Has Select Has Hash Algo	private sh Algo h Algo rithm: nature	key protect orithm orithm to be sha256 Format	tion used for thi	s request		~	*
Select Has Select Has Hash Algo Select Sign	private sh Algo h Algo rithm: nature	key protect orithm orithm to be sha256 Format	tion used for thi	s request		~	*
Select Has Select Has Hash Algo Select Sign	private sh Algo h Algo rithm: nature	key protect orithm orithm to be sha256 Format	tion used for thi	s request		~	*
Select Has Select Has Hash Algo Select Sign	private sh Algo h Algo rithm: nature	key protect orithm orithm to be sha256 Format	tion used for thi	s request		~	*

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.

-	X
	 2.02

Certificate Enrollment

Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

Custom request	U STATUS: Available	Details A
The following options	describe the uses and validity period that apply to this ty	pe of certificate:
Key usage:	Digital signature Key certificate signing Key encipherment	
Application polici	es:	
Validity period (da	ys):	
		Properties
		Next Canc

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**.

ertificate Enrollment	
Where do you want to save the offline request?	
If you want to save a copy of your certificate request or want to pro to your hard disk or removable media. Enter the location and name click Finish.	cess the request later, save the request for your certificate request, and the
File Name:	
File Name: C:\Users\Administrator\Desktop\CSR6.1.21	Browse
File Name: C:\Users\Administrator\Desktop\CSR6.1.21 File format:	Browse,,,
File Name: C:\Users\Administrator\Desktop\CSR6.1.21 File format: Base 64 Binary	Browse

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.

1

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----MIIGBAYJKoZIhvcNAQcCoIIF9TCCBfECAQMxDzANBg1ghkgBZQMEAgEFADCCBEoG CCsGAQUFBwwCoIIEPASCBDgwggQ0MGQwYgIBAgYKKwYBBAGCNwoKATFRME8CAQAw AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QLTBBMDAwNDY3DB1JUC0wQTAw MDQ2N1xBZG1pbm1zdHJhdG9yDAdNTUMuRVhFMIIDxqCCA8ICAQEwgg07MIICowIB ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAgMAk10MRQwEgYDVQQHDAtNYXBsZSBH cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UECgwDTUpUMRYwFAYDVQQDDA1U ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7G1/ 5z1YrUG0o4dW1/b3o35rpc00by0UE0K1NWjaIy4YrRPM9HjhKReThbcSnxddj6eR Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ//Zi08bEPobLv8YnWieNDuw lkaJWWRx3mbl/Yz0f1bwZrKFT3nkrXYOFYmZOR19W0J+Iin0BtziwiC8DHt+bxST nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9gC47RP9yMjyuuEtpdR9ERoR qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs18zBATRXkk/kRI+Po6cXNJp Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEAYI3DQIDMQ4WDDEwLjAuMTc3 NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/wQEAwICpDAdBgNVHQ4EFgQU vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCNxUUMTYwNAIBBQwLSVAtMEEw MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b3IMB01NQy5FWEUwZgYKKwYB BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFMAbwBmAHQAdwBh AHIAZQAgAEsAZQB5ACAAUwB0AG8AcgBhAGcAZQAgAFAAcgBvAHYAaQBkAGUAcgMB ADANBgkqhkiG9w0BAQsFAAOCAQEAqtKb5HCh2a1BD2QcKdFuhVQbNxg+G5wcVkZt 7bXdwVuzoAxd9BFd+uVy4D3TmvXtineT3GVWQbKJCcxRZeTKPBFnHG0SeaYupUrG cX4ySsKR1xGSuOhsfIVa/5NXiIYgYxMhlz3nt2CDw+RNqAp/1gLV2cLsui01y5ib 088po4/b9eiXV7A1DWFy7ecw/7Z20a07Sa0OaRbwzGJ8He1IiVEjfyAt7KLoufAq LkeSaJtjokkJuGPdr+ykjfuCmIF4hSbcOxzVkPCQbiHOwSxDG1kgYHZ8Xru665Q6 0L7QgBXCc7tcecDieqbYmp50LJPpqEQDQiYjzg57j3eYIFNYYjAAMAAxggGLMIIB hwIBA4AUvruQxeU1yku5Cem3anpu1cbMEDAwDQYJYIZIAWUDBAIBBQCgSjAXBgkq hkiG9w0BCQMxCgYIKwYBBQUHDAIwLwYJKoZIhvcNAQkEMSIEICk1SKp5MUjMa+vr DU1UXU+V05r1F8bNdM0mDgYfmjCiMA0GCSqGSIb3DQEBAQUABIIBAEjqqe4GSGE4 oZQj0vbWrAP0Ab2u8epFm7ZIMZzsJSzR0z98m+R+1R2mCoqWC0SSafybJ701Jh1y A3eqzDYxAu9p9drJft317sGAERE/i1D3BFvKZZQH0sz0JNRwDp3qByHHzVCULUEI JSOpYvI1s3S23ZYEedQLp35Xy87378zLLGLpgGKTK4teav1IitUJwVCKikL47uyF uOY4XLagwI1WWALsPF1+5ZcVNZMvsgzsbuMEXvjBkFKyhMv49oisgFcLJ1AoMtWn 7Mbg8K6ckbKkVpuvmWThkVTp1W3hIS/i/J0X7c2unA25LxAC/P/LyWhPt/Vk/ogf 06jNaHC/zBQ=

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

Windows (CRLF Ln 1, Col 1 100%

2. 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.

🛃 Certificate Import Wizard

Welcome to the Certificate Import Wizard

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

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

Store Location

O Current User

Local Machine

To continue, click Next.

Next:	Cancel
-------	--------

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

🗧 🐓 Certificate Import Wizard	
Certificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location t the certificate.	ior
 Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: 	Select Certificate Store × Select the certificate store you want to use.
Next	OK Cancel

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
 - 0
- 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 Configurator, 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.

Server Configurator			
Encryption	Encryption		
Registering servers	It is recommended to secure communi-	ication with encryption. Learn	more
anguage selection	Server certificate Applies to: management server, recording se collector	erver, failover server, data	
	Encryption: On		
	Terme	~	Details
	Cartificate insued by MS-Organization-P2P-Accent []	2023], Explore 5/8/2023	
	Mobile streaming media certificate Applies to mobile and web clients that retriev server	ve data streams from the mobile	
	Encryption: On	0	
	Name	~	Details
	Certificate (nued by	Expline 5/3/2121	
			Apply

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.

57 | Instalar certificados para la comunicación 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.

ø

1

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 v 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....

[Console Root] on View Favorites	Window	Help	- 🗆 X
	Ctrl+N Ctrl+O	Name	Actions
le.	Ctrl+S	There are no items to show in this view.	Console Root
ks kernove Snap-in ns t File	Ctrl+M	There are no items to show in this view.	Console Root
	[Console Root] in View Favorites is ternove Snap-in trike t File	[Console Root] In View Favorites Window Ctrl+N Ctrl+O Ctrl+S Is temove Snap-in Ctrl+M Ts t File	[Console Root] In View Favorites Window Help Ctrl+N Ctrl+O Ctrl+C Ctrl+S Is There are no items to show in this view.

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

ailable snap-ins:			Selected snap-ins:	
nap-in	Vendor	~	Console Root	Edit Extensions
ActiveX Control	Microsoft Cor	11	Certificates - Cu	rrent User
Authorization Manager	Microsoft Cor			Remove
Certificate Templates	Microsoft Cor			
Certificates	Microsoft Cor			No.ello.
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor	1		Manus Crown
Computer Managem	Microsoft Cor	A	a >	
Device Manager	Microsoft Cor			
Disk Management	Microsoft and			
Enterprise PKI	Microsoft Cor			
Event Viewer	Microsoft Cor			
Folder	Microsoft Cor			
Group Policy Object	Microsoft Cor			Advanced
have not in		*		Advanceant

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

sole Root Certificates - Current	: User Object	t Type tificates	
Tri Find Ce	rtificates		
En All Task	s >	Find Certificates	
Ac View	ndow from Here	Request New Certificate Import	
Th New Ta	skpad View	Advanced Operations	Create Custom Request
Tri Refresh	ist		Enroll On Behalf Of Manage Enrollment Policies
Sn Help			

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

Haga clic en Siguiente.

	V
-	\sim

Certificate Enrollment

Select Certificate Enrollment Policy

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

Configured by you	Add New
Custom Request	
Proceed without enrollment policy	
	I second second
	<u>N</u> ext Cancel

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

		- 🗆 X
🗐 Certificate Enrollm	ent	
Custom requ	est	
Chose an optior	from the list below and configure the certificate options as required	d.
Template:	(No template) CNG key	-
	Suppress default extensions	
Request for	nat: <u>P</u> KCS #10	
	● <u>c</u> MC	
		Next Cancel
El formate emitirá ur con la CA	o de la solicitud depende de la CA. Si se elige el formato inc error cuando se envíe la solicitud de firma de certificado (C para asegurarse de que elige correctamente.	orrecto, la CA SR). Consulte

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

62 | Instale certificados de CA comerciales o de terceros para la

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

easier to iden	itify and use a ce	rtificate.
OF	Control	Apply
	ОК	OK Cancel

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:

ertificate Properties			>
General Subject Extensions	Private Key	Signature	
The subject of a certificate is th can enter information about th can be used in a certificate.	ne user or c ne types of	omputer to v subject name	which the certificate is issued. You e and alternative name values that
Subject of certificate			
The user or computer that is re	ceiving the	certificate	
Subject name:			
Type:	1		CN=Test for Docs
Country		Add:	O=MJT
Value:	<	Remove	L=Maple Grove S=MN C=USA
Alternative name:	1		
Туре:	1		1
Directory name 🛛 👻			
Value:		Add>~	
		Rémove	
		OF	Cancel Apply

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**.

Certificate Properties					×
General Subject Exten	sions Private Key	Signature			
The following are the co	ertificate extension	s for this cert	tificate type.		^
Key usage				~	
The key usage extensio	n describes the pu	rpose of a ce	ertificate.		
Available options:			Selected options:		
CRL signing Data encipherment			Digital signature Key certificate signing	g	
Decipher only			Key encipherment		
Encipher only Key agreement	Ad	id >			
Non repudiation	× 0.	ultra con			
Make these key usag	ges critical				1
Extended Key Usage (a	application policies)		¥	ï
Basic constraints				٠	
					V
		1		_	

Ì

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.

	roperti	es				>
General Su	ubject	Extensions	Private Key	Signature		
Cryptogr	aphic S	Service Prov	ider			۷
Key optio	ons					*
Set the ke	y lengt	h and expo	t options for	the private key		
Key size:	2048				*	
Make p	orivate	key exportal	ble			
	orivate	key to be an	chived			
Allow	Distance	Key to be al				
Strong	private	key to be a	tion			
Strong	private	key protec	tion			
Select Ha	private	key protec	tion			*
Select Ha	private ash Alg	e key protec orithm	tion used for this	s request		*
Select Has Select Has	private ash Alg sh Algo orithm:	e key protect orithm orithm to be sha256	tion used for this	s request	×	*
Select Has Select Has	private ash Alg sh Algo orithm:	orithm orithm to be sha256	tion	s request	Ŷ	*
Select Has Select Has Hash Algo	private ash Alg sh Algo orithm: gnature	e key protect orithm prithm to be sha256	tion	s request	×	*
Select Ha Select Ha Hash Algo Select Sig	private ash Alg sh Algc orithm: gnature	e key protect orithm orithm to be sha256 Format	tion used for this	s request	~	*
Select Ha Select Ha Hash Algo Select Sig	private ash Alg sh Algo orithm: gnature	e key protect orithm orithm to be sha256 Format	tion	s request	×	*
Select Ha Select Ha Select Has Hash Algo	private ash Alg sh Algc orithm: gnature	e key protect orithm orithm to be sha256 Format	tion	s request	×	*

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.

	-	31
-		X

Certificate Enrollment

Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

Custom request	i) STATUS: Available	Details A
The following option	s describe the uses and validity period that apply to this t	ype of certificate:
Key usage:	Digital signature Key certificate signing Key encipherment	
Application polic	ies:	
Validity period (d	ays):	
		Properties
	T.	Next Cance
		INEXC Cance

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**.

ertificate enrollment	
Where do you want to save the offline request?	
If you want to save a copy of your certificate request or want to your hard disk or removable media. Enter the location and click Finish.	o process the request later, save the req name of your certificate request, and the
File Name:	
File Name: C:\Users\Administrator\Desktop\CSR6.1.21	Browse
File Name: C:\Users\Administrator\Desktop\CSR6.1.21 File format:	Browse
File Name: C:\Users\Administrator\Desktop\CSR6.1.21 File format: Base 64 Binary	Browse
File Name: C:\Users\Administrator\Desktop\CSR6.1.21 File format: Base 64 Binary	Browse
File Name: C:\Users\Administrator\Desktop\CSR6.1.21 File format: Base 64 Binary	Browse

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 . 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.

Ì

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.

68 | Instale certificados de CA comerciales o de terceros para la

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----MIIGBAYJKoZIhvcNAQcCoIIF9TCCBfECAQMxDzANBg1ghkgBZQMEAgEFADCCBEoG CCsGAQUFBwwCoIIEPASCBDgwggQ0MGQwYgIBAgYKKwYBBAGCNwoKATFRME8CAQAw AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QLTBBMDAwNDY3DB1JUC0wQTAw MDQ2N1xBZG1pbm1zdHJhdG9yDAdNTUMuRVhFMIIDxqCCA8ICAQEwgg07MIICowIB ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAgMAk10MRQwEgYDVQQHDAtNYXBsZSBH cm92ZTEQMA4GA1UECwwHTUpUIExhYjEMMAoGA1UECgwDTUpUMRYwFAYDVQQDDA1U ZXN0IGZvciBEb2NzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7G1/ 5z1YrUG0o4dW1/b3o35rpc00by0UE0K1NWjaIy4YrRPM9HjhKReThbcSnxddj6eR Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ//Zi08bEPobLv8YnWieNDuw lkaJWWRx3mbl/Yz0f1bwZrKFT3nkrXYOFYmZOR19W0J+Iin0BtziwiC8DHt+bxST nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDUzs9gC47RP9yMjyuuEtpdR9ERoR qJJoOK6CdrKLU5kZFiDTIVbs0F3mNqnHCyzs7cEEs18zBATRXkk/kRI+Po6cXNJp Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEAYI3DQIDMQ4WDDEwLjAuMTc3 NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/wQEAwICpDAdBgNVHQ4EFgQU vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCNxUUMTYwNAIBBQwLSVAtMEEw MDA0NjcMGU1QLTBBMDAwNDY3XEFkbW1uaXN0cmF0b3IMB01NQy5FWEUwZgYKKwYB BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFMAbwBmAHQAdwBh AHIAZQAgAEsAZQB5ACAAUwB0AG8AcgBhAGcAZQAgAFAAcgBvAHYAaQBkAGUAcgMB ADANBgkqhkiG9w0BAQsFAAOCAQEAqtKb5HCh2a1BD2QcKdFuhVQbNxg+G5wcVkZt 7bXdwVuzoAxd9BFd+uVy4D3TmvXtineT3GVWQbKJCcxRZeTKPBFnHG0SeaYupUrG cX4ySsKR1xGSuOhsfIVa/5NXiIYgYxMhlz3nt2CDw+RNqAp/1gLV2cLsui01y5ib 088po4/b9eiXV7A1DWFy7ecw/7Z20a07Sa00aRbwzGJ8HelIiVEjfyAt7KLoufAq LkeSaJtjokkJuGPdr+ykjfuCmIF4hSbcOxzVkPCQbiHOwSxDG1kgYHZ8Xru665Q6 0L7QgBXCc7tcecDieqbYmp50LJPpqEQDQiYjzg57j3eYIFNYYjAAMAAxggGLMIIB hwIBA4AUvruQxeU1yku5Cem3anpu1cbMEDAwDQYJYIZIAWUDBAIBBQCgSjAXBgkq hkiG9w0BCQMxCgYIKwYBBQUHDAIwLwYJKoZIhvcNAQkEMSIEICk1SKp5MUjMa+vr DU1UXU+V05r1F8bNdM0mDgYfmjCiMA0GCSqGSIb3DQEBAQUABIIBAEjqqe4GSGE4 oZQj0vbWrAP0Ab2u8epFm7ZIMZzsJSzR0z98m+R+1R2mCoqWC0SSafybJ701Jh1y A3eqzDYxAu9p9drJft317sGAERE/i1D3BFvKZZQH0sz0JNRwDp3qByHHzVCULUEI JSOpYvI1s3S23ZYEedQLp35Xy87378zLLGLpgGKTK4teav1IitUJwVCKikL47uyF uOY4XLagwI1WWALsPF1+5ZcVNZMvsgzsbuMEXvjBkFKyhMv49oisgFcLJ1AoMtWn 7Mbg8K6ckbKkVpuvmWThkVTp1W3hIS/i/J0X7c2unA25LxAC/P/LyWhPt/Vk/ogf 06jNaHC/zBQ=

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

Windows (CRLF Ln 1, Col 1 100%

2. 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.

🛃 Certificate Import Wizard

Welcome to the Certificate Import Wizard

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

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

Store Location

O Current User

Local Machine

To continue, click Next.

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

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

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

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

0

- 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.

Milestone Server Configurato	ŕ	1		×
Encryption	Encryption			
legistering servers	It is recommended to secure communication with encryption.	Learn m	ore	
Language selection	Server certificate Applies to: management server, recording server, failover server, data collector, api gateway, log server			
	Encryption: Off			
	Select certificate	~		
	No certificate selected			
	Streaming media certificate Applies to clients and servers that retrieve data streams from the recordir server	ng		
	Encryption: Off	D		
	Select certificate			
	No certificate selected			
	Mobile streaming media certificate Applies to mobile and web clients that retrieve data streams from the mo server	bile		
	Encryption: Off			
	Select certificate			
	No certificate selected			
			Apply	1

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.

Server Mana	ider • Dashboard	- @ /	Manage Tools View Help
0.0			Add Roles and Features Remove Roles and Features
Dashboard W	ELCOME TO SERVER MANAGER		Add Servers
All Servers	1 Configure th	1 Configure this local server	

- 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.

DEIECT TOTE SET V	ices	IP-0A000450
Before You Begin Installation Type	Role services	Description
Server Selection Server Roles Features AD CS	Certification Authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Certification Authority Web Enrollment Network Device Enrollment Service Online Responder	Network Device Enrollment Service makes it possible to issue and manage certificates for routers and other network devices that do not have network accounts.
Role Services Web Server Role (IIS) Role Services Confirmation		

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.

	• @ I 🏹
i,	Post-deployment Configura
	Configuration required for Active Directory Certificate Services at IP-0A000467
	Configure Active Directory Certificate Services on th
D	Feature installation
	Configuration required. Installation succeeded on IP-0A000467.
	Add Roles and Features
	Task Details

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**.

			DESTINAT	TION SER	VEF
redentials				IP-0A000)450
Credentials	Specify credentials to configure re	ole services			
Role Services					
	To install the following role services you must be	long to the local Adm	inistrators grou	p:	
	Standalone certification authority				
	Certification Authority Web Enrollment Opling Responder				
	To install the following role services you must be	long to the Enterprise	Admins aroun:		
	 Enterprise certification authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Network Device Enrollment Service 				
	Credentials: IP-0A000450\Administrator	Change	han		
	More about AD CS Server Roles				

- 13. En **Servicios de rol**, seleccione los siguientes servicios:
 - Autoridad de Certificación
 - Inscripción web de la autoridad de certificación

Haga clic en **Siguiente**.

AD CS Configuration		- 0	×
Role Services		DESTINATION SERVE IP-0A0004	ER 50
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation	Select Role Services to configure		
	More about AD CS Server Roles		

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.

AD CS Configuration		
Cryptography fo	or CA	DESTINATION SERVER
Credentials Role Services	Specify the cryptographic options	
Setup Type	Select a cryptographic provider:	Key length:
СА Туре	RSA#Microsoft Software Key Storage Provider	× 2048 ×
Private Key	Select the hash algorithm for signing certificates issued by t	his CA:
Cryptography	SHA256	+
CA Name	SHA384	
Validity Period	SHA512	
Certificate Database	SHA1	
Confirmation	MD5	
	Allow administrator interaction when the private key is a	accessed by the CA.
	More about Cryptography	

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".

AD CS Configuration	— 🗆 X
CA Name	DESTINATION SERVER IP-0A000450
Credentials Role Services Setup Type CA Type Private Key	Specify the name of the CA Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.
Cryptography	IP-0A000450-CA
Validity Period Certificate Database Confirmation	Distinguished name suffix:
	Preview of distinguished name: CN=IP-0A000450-CA
	More about CA Name
	< Previous Next > Configure Cancel

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

📥 AD CS Configuration							\overline{e}		×
Validity Period						E	DESTINAT	TION SEF	VER 0450
Credentials Role Services Setup Type	Speci Select t	ify the validity he validity period for	period	te generate	ed for this cert	tification aut	thority (C	A):	
CAType	5	Years	*						
Private Kev	CA expi	ration Date: 4/27/20	26 3:27:00 PM	N					
Cryptography CA Name	The vali certifica	dity period configure ites it will issue.	ed for this CA	A certificate	should excee	ed the validit	ty period	for the	
Validity Period									
Centificate Database									
Commaton									
	More al	bout Validity Period							
			< Pre	evious	Next >	Confi	igure	Canc	el

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:\\limu\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....

🚡 Fil	Action View Favorites Wind	w Help	- 8 ×
	Open Ctrl+	Name	Actions
	Save Ctrl+	There are no items to show in this view.	Console Root
	Save Ctrl+ Save As Add/Remove Snap-in Ctrl+ N Options Recent File Exit	There are no items to show in this view.	Console Root Actions

3. Seleccione el complemento Certificados y haga clic en Agregar

and bic bridp in bit		10.	Î	elected shap-ins.	1 August	-
inap-in	Vendor	^		Console Root	Edit Extensions	
ActiveX Control	Microsoft Cor			Certificates (Local Computer)	ison,s	
Authorization Manager	Microsoft Cor					
Certificates	Microsoft Cor				-	
Component Services	Microsoft Cor				(Morsight)	
Computer Managem	Microsoft Cor		-		diama finan	
Device Manager	Microsoft Cor		< bba		MARK DAVE	
Disk Management	Microsoft and		nuurz			
Event Viewer	Microsoft Cor					
Folder	Microsoft Cor					
Group Policy Object	Microsoft Cor					
Internet Informatio	Microsoft Cor					
IP Security Monitor	Microsoft Cor					
IP Security Policy M	Microsoft Cor	4			Advanced	
<u>0]</u>		-	1			
scription:						

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

Certificates snap-in	×
This snap-in will always manage certificates for:	
O My user account	
O Service account	
Computer account	
	Next > Cancel

-

5. En Seleccionar equipo, seleccione Equipo local.

Seleccione Finalizar y, a continuación, Aceptar.

aect computer		
Select the computer you want this snap-	in to manage.	
This snap-in will always manage:		
O Local computer: the computer the	nis console is running on)	
O Another computer:	Browne	
only applies if you save the conso	ole.	
only applies if you save the conso	ole.	

 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.

- 🗆 X

Certificate Enrollment

Select Certificate Enrollment Policy

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

Configured by you	Add New
Custom Request	
Proceed without enrollment policy	

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

lustom request		
hose an option from	n the list below and configure the certificate opti	ons as required.
Template:	(No template) CNG key	
	Suppress default extensions	
Request format:	○ <u>P</u> KCS #10	

Next Cancel

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

	30	×
🙀 Certificate Enrollment		

Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

Custom request	i) STATUS: Available	Details A
The following option	s describe the uses and validity period that apply to this	type of certificate:
Key usage:	Digital signature Key certificate signing Key encipherment	
Application polic	ies:	
Validity period (d	ays):	
		Properties

Next

Cancel

	95	Instalar	certificados	en un	dominio	para la	comunicación	con e
--	----	----------	--------------	-------	---------	---------	--------------	-------

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

Seneral Subject Extensions Private Key Signature A friendly name and description will make it easier to identify and use a certificate. Friendly name: TestLabDomain.com TestLabDomain.com	onora	and the second						
A friendly name and description will make it easier to identify and use a certificate. Friendly name: TestLabDomain.com TestLabDomain.com	JEI IEI di	Subject	Extensions	Private Key	Signature			
Friendly name: TestLabDomain.com TestLabDomain.com	A friend	lly name	and descript	tion will mak	e it easier to id	entify and u	se a certificate	e.
TestLabDomain.com TestLabDomain.com	Friendly	/ name:						
Description: TestLabDomain.com	TestLa	Domain	.com					_
TestLabDomain.com	Descrip	tion:						
OK Cancel Andy	TestLa	bDomain	.com					
OK Cantal Analy								
OK Cantal Analy								
OK Cantal Analy								
OK Cantal Anniv								
OK Cancel Anniv								
OK Cancel Apply								
OK Cantal Apply								
OK Cancel Apply								
OK Cancel Apply								
OK Cancel Apply								
OK Cancel Apply								
OK Candal Anniv								
OK Cancel Apply								

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.

Seneral Subject	Extensions	Private Key	Signature	
The subject of a c can enter informa can be used in a c Subject of certific The user or comp	ertificate is tion about ertificate. ate uter that is	the user or c the types of receiving the	omputer to w subject name certificate	hich the certificate is issued. You and alternative name values that
Subject name:		1		CN=MJT-12A
Type	-		Add >	citetari izi
Common name	,		100	
Value:			Remove	
Alternative name:		1		0
Туре:		-		
Directory name		*		
Value:		-	4dd ≥	
		C	Remove	
				1

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.

General Subject Extensions	Private Key Signature	-
The following are the certific	ate extensions for this certificate type.	^
Key usage	v	
Extended Key Usage (applic	ation policies)	
An application policy (called certificate can be used. Selec certificates issued by this ter Available options: Client Authentication Code Signing Secure Email Time Stamping Microsoft Trust List Signin Microsoft Trust List Signin Microsoft Time Stamping IP security end system IP security tunnel termina	Add > Add > Add >	
IP security user	sage critical	
-		~

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**.

Certificate Prope	ties				×
General Subject	Extensions	Private Key	Signature		
Cryptographic	Service Prov	ider			۷
Key options					*
Set the key leng	gth and expo	rt options for	the private key.		
Key size: 204	В		~		
Make private	e key exporta	ble			
Allow privat	e key to be a	chived			
Strong priva	te key protec	tion			
Select Hash Al	aorithm				*
Select Hash Alg	gorithm to be	used for this	request		
Hash Algorithm	n: sha256			~	
Select Signatu	re Format				*
				1 court	1
			UK	Cancel	Apply

- 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.

e Enrollment		
do you want to save the offline request?		
. do you want to save the online request.		
rant to save a copy of your certificate request or want to process the hard disk or removable media. Enter the location and name of your nish.	e request later, sa certificate reque	ve the re est, and th
ne: rc\Administrator\Deckton\C\$R6.1.21	T	Provisa
Is (Auministrator (Desktop (CSN0, N2)	L	browse
nat: 64		
У У		
	Finish	

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

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

Ì

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.

107Test1 - Notepad	-		×
File Edit Format View Help			
File Edit Format View Help BEGIN NEW CERTIFICATE REQUEST MIIF2AYJKoZIhvcNAQcCoIIFyTCCBcUCAQMxD CCsGAQUFBwwCoIIEEASCBAwwggQIMGYwZAIBA AwIBATFHMEUGCSsGAQQBgjcVFDE4MDYCAQUMD UjFURU1QXEFkbWluaXN0cmF0b3IMB01NQy5FW AgEAMBcxFTATBgNVBAMMDENsdXN0ZXIxVEVNL ggEPADCCAQoCggEBAKVp0982yi05tcnypaTuj dVMVTSU9s9rTMWmUDzP+zLumOmC6gCWIo5Rgi ZktV8ut805gi46dkQ4MD71btX6mnjjUB294XW zczK1yUZmY576IBwf6LZMujXbNDD5ZXzdhG3p JN2d0SZms4Utj21DekFde3BsENvcvk0/PHZk8 bqL+Zy4pEP1jKnTwM1IyPmsXyw7gx6CrTw8nt Nw0CAzE0FgwxMC4wLjE0MzkzLjIwRQYJKwYBB	 IZANBglghkgBZQMEAgEF IgYKKwYBBAGCNwoKATFT IENsdXN0ZXIxVEVNUAwa IEUwggOYoIIDIAIBATCC IDCCASIwDQYJKoZIhvcN SFBe9jwOyRp+c5N00xf T+dLjOvq+Z6AUWC1H+W If8yUVP1Be0dkfqjUVnn IggarNdzHvg0RIJvro4I Ib8Bww050+ya3tk7jDbv GECAwEAAaCCAS8wHAYK AGCNxUUMTgwNgIBBQwM	ADCCBB4 MFECAQ/ Q0xVU1 A40wgg AQEBBQ/ 80cN0Dy VUsaVb 6EAYzH0 J0rM6E W0a1VXI KwYBBA0 Q2x1c3	AW RF J1 AD JC dS sJ E9 GC R1
cjFURU1QDBpDTFVTVEVSMVRFTVBcQWRtaW5pc hkiG9w0BCQ4xUzBRMBMGA1UdJQQMMAoGCCsGA MAwwCgYIKwYBBQUHAwEwHQYDVR0OBBYEF0BsT CisGAQQBgjcNAgIxWDBWAgEAHk4ATQBpAGMAc AHcAYQByAGUAIABLAGUAeQAgAFMAdABvAHIAY AHIDAQAwDQYJKoZIhvcNAQELBQADggEBAFGoQ OAPtDKNDGskV/dq6rqgpYEKiQfWZeSndEOzxi XjUze/+WIiZifGFnkMKYwrzKgx7qIr WadWazix8d5V00TR73Lp7vXq9iiE49	3RyYXRvcgwHTU1DLkVY QUFBwMBMBsGCSsGAQQB d6/Hpi6c18h5HHq88hW gBvAHMAbwBmAHQAIABT QBnAGUAIABQAHIAbwB2 LCtyiv0XG0T0U4MS9Vn eJtES/1I5hmVUm51TIV do	RTBgBgl gjcVCg(c911MG AG8AZgl AGkAZAI USØsQU(ydzE8i)	kq QO YG BØ B1 N VW
EX7yVZFyEAs/6uoApcKXc2KPgBP8aHe Cu Tp4XCYYiuyw/+iHqyNca2fvIIm8Hpb0 izCCAYcCAQOAF0BsTd6/Hpi6c18h5He Pas FwYJKoZIhvcNAQkDMQoGCCsGAQUFBwA OY6dr8BzietMf5QwmoRNzq8MRGSQiN: Del +q73I6NKKLzg7ROhm16Xj7tL4Id2iVL Sel 1WR7EktvnBLYuBOVPGYb+gwd8EfBh9L	t py ite lete ect All		2 3 3 V I V II V
r+5Z7iOE2HZpsBrSldl+u89F0Pi+W/a Rig nIi7k+ce+EDoHhXkbSD+fHYFbUqaTYV Sho 2PmPVkUJGJEUMwfo8rb4xb9taP6ycUI Ins T8XTFWMOJCPMykW2 END NEW CERTIFICATE REQUES Op	ht to left Reading order ow Unicode control characters ert Unicode control character en IME	>)))))))))))))))))))
Rec	conversion		8 di

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.

Microsoft Active Directory Certificate Services - IP-0A000467-CA	Home
← → C ▲ Not secure 10.0.4.103/certsrv/	🖈 💄 Update 🚦
Microsoft Active Directory Certit × +	• - • ×

Welcome

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

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

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

Select a task:

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

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



E-Mail Protection Certificate

Or, submit an advanced certificate request.

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.

Microsoft Active	irectory Certificate	Services - CLUSTER2TEMP-CA	Home
Increased Picture L	Areatory Germanate	SERVICES - DEDUTENZIEMI - OM	10/16
Submit a Certif	ficate Request	or Renewal Request	
Fo submit a sav renewal request Saved Request:	ed request to the tend of	e CA, paste a base-64-encoded CMC or PKCS #10 an external source (such as a Web server) in the Sav	certificate request or PKCS #7 ed Request box.
Base-64-encoded partificate request CMC or PKCS #10 or PKCS #7):	IWR7EktvnBLYuB(r+527i0E2HZps5; nIi7k+ce+EDoHh) 2FmPVkUJGJEUMwi TSXTFWMOJCPMyki END NEW CI	2VPGYD+gwd9EfBh9K9Qgvd5fMu: cSldl+u89F0Pi+W/a8/YV7BhAl; KkbSD+fHYFDUgaTVDfgD4u5Pg6; fo8rb9xb9taP6ycUZwieLrNWw3] w2 ERTIFICATE REQUEST	
Additional Attribut	tes:		
Attributes:	÷	\$ ()	

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 .

X

- 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.

Certificate Import Wizard

Welcome t	to the Cer	tificate In	port Wizard	

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

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

Store Location

Ourrent User

O Local Machine

To continue, click Next.

Next	Cance
Land the second s	

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

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

- 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**.

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

🚰 File Action View Favorites Window	v Help			
🗢 🔿 🙍 💼 🔏 🛍 🗙 🗟 🗟 🛙				
Console Root	Issued To	^	Issued By	Expiration
Certificates (Local Computer) Personal	Cluster17	EMP Open	CLUSTERZTEMP-CA	10/26/202
 Certificates Trusted Root Certification Authoritie 		All Tasks >	Open	
 Enterprise Trust Intermediate Certification Authoritie Trusted Publishers 		Cut Copy	Request Certificate with New Key. Renew Certificate with New Key	
Untrusted Certificates		Delete	Manage Private Keys	
Certificates		Properties	Advanced Operations	>
Trusted People		Help	Export	

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:

Ì

• El menú Inicio de Windows

о

- 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.

Server Configurator		-	
Encryption	Encryption		
Registering servers	It is recommended to secure communication with encryp	tion. <u>Learn i</u>	more
Language selection	Server certificate Applies to: management server, recording server, failover server, d collector	ata	
	Encryption: On		
	(Inclusion)	4	Details
	Carolicate issued by MS-Organization-P29-Actess (2021), Expires 5/8/2021		
	Streaming media certificate Applies to clients and servers that retrieve data streams from the re server	ecording	
	Encryption: On		
	And the second s	4	Details
	Certificate instead by MS-Degarization 8(9). Access (2023). Exolem 5/8/2023		

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.

107 | Instalar certificados en un dominio para la comunicación con el

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....

File Action View Favorites	Window	Help	- □ X - 8 ×
Open	Ctrl+0	Name	Actions
Save Ar	Ctrl+S	There are no items to show in this view.	Console Root
Save As Add/Remove Snap-in Options Recent File Exit	Ctrl+M	There are no items to show in this view.	Console Root

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

Haga clic en **Aceptar**.

allable snap-lins:		-		selected snap-ins:	-	
nap-in	Vendor	1		Console Root	Edit Exter	nsions
ActiveX Control	Microsoft Cor			Certificates (Local Computer)	-	
Authorization Manager	Microsoft Cor				Kem	ove.
Certificates	Microsoft Cor	=				
Component Services	Microsoft Cor				Move	eUp
Computer Managem	Microsoft Cor					
Device Manager	Microsoft Cor		1 . II.		Monre 3	Downt
Disk Management	Microsoft and		Add >			
Event Viewer	Microsoft Cor					
Folder	Microsoft Cor					
Group Policy Object	Microsoft Cor					
Internet Informatio	Microsoft Cor					
Internet Informatio	Microsoft Cor					
IP Security Monitor	Microsoft Cor				Advan	ced.
IP Security Policy M	Microsoft Cor	-			Harbit	COMIN
scription:						
		24				

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

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

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

Haga clic en Siguiente.

	V
-	\sim

Certificate Enrollment

Select Certificate Enrollment Policy

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

Configured by you	Add New
Custom Request	
Proceed without enrollment policy	
	<u>N</u> ext Cance

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

ustom request	
hose an option fron	n the list below and configure the certificate options as required.
Template:	(No template) CNG key
	Suppress default extensions
Request format:	○ <u>P</u> KCS #10
	● ⊆MC
Note: Key archival is option is specified in	not available for certificates based on a custom certificate request, even when th the certificate template.

Cancel

Next

112 | Instale certificados en un entorno de grupo de trabajo para la

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

Certificate Information		
Click Next to use the options already request, and then click Next.	selected for this template, or click Details to cu	stomize the certifica
Custom request	j STATUS: Available	Details
The following options describe Key usage: Application policies: Validity period (days):	the uses and validity period that apply to this t	Properties

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

General g	Subject	Extensions	Private Key	Signature			
A friendly	name	and descrip	tion will make	e it easier to ider	ntify and use	a certificate	e.
Friendly r	ame:						
TestLabD	omain,	com					
Descriptio	on;						
TestLabD	omain.	com					

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.

General	Subject	Extensions	Private Key	Signature	
The sub can ent can be Subject The use	ject of a er inform used in a of certifier or com	certificate is ation about certificate. cate puter that is	the user or c the types of receiving the	omputer to w subject name certificate	hich the certificate is issued. You and alternative name values that
Subject	name:		ni i		CN-MIT-12A
Type	_		1 1		CIN=WD1-IZM
Comm	non name	E		400 *	
Value:			*	Remove	
Alternat	tive name	2	-1		
Type:			_		
Direct	ory name				
Value:				≜dd≥	
-			C	Remove	

115 | Instale certificados en un entorno de grupo de trabajo para la

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.

General Subject Extensions	Private Key Signature	
The following are the certifica	te extensions for this certificate typ	pe.
Key usage		v
Extended Key Usage (applica	tion policies)	~
An application policy (called certificate can be used. Select certificates issued by this ten Available options: Client Authentication Code Signing Secure Email Time Stamping Microsoft Trust List Signin Microsoft Time Stamping	enhanced key usage in Windows 2 t the application policy required for aplate.	2000) defines how a ir valid signatures of d options: Authenticettion
IP security end system IP security tunnel termina IP security user	< Kemove	ш >
Make the Extended Key Us	age critical	~

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**.

Certificate F	Properti	ies					×
General S	ubject	Extensions	Private Key	Signature			
Cryptog	raphic S	Service Prov	ider				۲
Key opti	ons						*
Set the ke	ey lengt	th and expo	rt options for	the private k	ey.		
Key size:	2048				~		
Make	private	key exportal	ble				
Allow	private	key to be an	chived				
Strong	private	e kev protec	tion				
Select H	ash Alo	orithm					*
Select Ha	sh Algo	prithm to be	used for this	s request			
Hash Alg	orithm	sha256				~	
Select Si	anature	= Format					*
	3						
				OK		Cancel	Apply
				-	_		- <u></u>

- 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.

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

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

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

Ì

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.

107Test1 - Notepad	-		×	
File Edit Format View Help				
BEGIN NEW CERTIFICATE REQUEST			19	~
MIIF2AYJKoZIhvcNAQcCoIIFyTCCBcUCAQMxDzANBg	glghkgBZQMEAgEFAD	CCBB4	G	
CCsGAQUFBwwCoIIEEASCBAwwggQIMGYwZAIBAgYKKw	WBBAGCNwoKATFTME	ECAQA	W	
AwIBATFHMEUGCSsGAQQBgjcVFDE4MDYCAQUMDENsd>	<pre>KN0ZXIxVEVNUAwaQ0</pre>	xVU1R	F	
UjFURU1QXEFkbWluaXN0cmF0b3IMB01NQy5FWEUwgg	gOYoIID1AIBATCCA4	lØwgg]	1	
AgEAMBcxFTATBgNVBAMMDENsdXN0ZXIxVEVNUDCCAS	SIwDQYJKoZIhvcNAQ	EBBQA	D	
ggEPADCCAQoCggEBAKVp0982yi05tcnypaTujsFBeS	jwOyRp+c5N00xf80)cN0Dy	g	
dVMVTSU9s9rTMWmUDzP+zLumOmC6gCWIo5RgiT+dL	jOvq+Z6AUWC1H+WVL	lsaVb]	c	
ZktV8ut805gi46dkQ4MD71btX6mnjjUB294Xwf8yU\	/P1Be0dkfqjUVnn6E	AYzHd	S	
zczK1yUZmY5/61Bwf6LZMujXbNDD5ZXzdhG3pggarN	IdzHvg0K1Jvro41Jk	IrM6Es	J	
JNZd0SZmS4UtjZ1UeKFde3BSENVCVK0/PHZK8D8BW	USU+ya3tK/JUDVWU	VERAC	9	
DQL+ZY4PEPIJKHIWMIIYPMSXyW7gX6CFIW6HLQECAW				
ciEURI100BpDTEVTVEVSMVRETVBc0WRtaW5pc3RvV0	(RycowHTU1DL kVVR1	RaRak		
hkiG9w0BC04xUzBRMBMGA1UdT00MMAoGCCsGA0UER	MBMBsGCSsGAOOBgi	cVC gO	0	
MAwwCgYIKwYBBOUHAwEwHOYDVR00BBYEF0BsTd6/Hp	pi6c18h5HHa88hWc9	11MGY	G	
CisGAQQBgjcNAgIxWDBWAgEAHk4ATQBpAGMAcgBvAH	MAbwBmAHQAIABTAG	8AZgB	0	
AHcAYQByAGUAIABLAGUAeQAgAFMAdABvAHIAYQBnAG	GUAIABQAHIAbwB2AG	kAZAB	1	
AHIDAQAwDQYJKoZIhvcNAQELBQADggEBAFGoQLCtyi	LVOXG0T0U4MS9VnU5	ØsQUn	N	
OAPtDKNDGskV/dq6rqgpYEKiQfWZeSndEOzxieJtES	s/1I5hmVUm51TIVyc	IzE8iy	W	
XjUze/+WIiZifGFnkMKYwrzKgx7qIr			E.	
m3dWazix8dSVOQIRZ3Lr7yXg9iiF49			j	
EX7yVZFyEAs/6uoApcKXc2KPgBP8aHe Cut			2	
Tp4XCYYiuyw/+iHqyNca2fv11m8Hpb0 Copy			ř.	
IZCCAYCCAQUAFUBST06/HP16C1805HF Paste			2	
OY6dc8BzietMf5OwmoRNzg8MRGSOiN1 Delete				
+g7316NKKLzg7R0hm16Xi7tL4Id2iV				
1WR7EktvnBLYuB0VPGYb+gwd8EfBh9l			<	
r+5Z7i0E2HZpsBrSldl+u89F0Pi+W/c Right to le	ft Reading order			
nIi7k+ce+EDoHhXkbSD+fHYFbUqaTYU Show Unic	ode control characters		J	
2PmPVkUJGJEUMwfo8rb4xb9taP6ycU2 Insert Unic	ode control character	>	3	
END NEW CERTIFICATE REQUES Open IME				
Reconvers	ion		5	4
				1.8.8

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.



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

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

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

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

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



Request a Certificate

Select the certificate type: Web Browser Certificate E-Mail Protection Certificate

Or, submit an advanced certificate request.

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.

	pg//192,168.50,108/certs	n, D = C Microsoft Active Directory ×	<u>ଲି</u> କୁ କ୍ରି
Microsoft Active	Directory Certificate	Services - CLUSTER2TEMP-CA	Home
Submit a Cer	tificate Request	or Renewal Request	
To submit a sa enewal reque Saved Request:	aved request to th est generated by a	e CA, paste a base-64-encoded CMC or PKCS #10 in external source (such as a Web server) in the Sa	0 certificate request or PKCS #7 wed Request box.
3ase-64-encodec ertificate reques CMC or PKCS #10 or PKCS #7):	IWR7EktvnBLYuBC r+52710E2H2pBE t nI17k+ce+EDcHh2 2EmFVKUJGJEUM/M TSXTFMMOJCPMykk END NEW CE	IVFGYD+gwd3EfBh9K9Qgvd5fMu Sldl+u89F0Pi+W/a8/YV7BhAl KbSD+fHYFbUqaTYUfgU4u5Pg6 S8rbfxb9taP6ycUZwieLrNWw31 IZ IRTIFICATE REQUEST	
Additional Attrib	outes:		
Attributes	:	3	
		Submit >	

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



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

Your Request Id is 6.

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

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

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**.

Console Root	Request ID	Binary Request	Request Status Code	Actions
V IP-0A000467-CA	5	All Ta	sks 🤌 View A	Attributes/Extensions
Issued Certificates		Refres	sh Export	Binary Data
Pending Requests		Help	Issue	

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.



Welcome

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

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

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

Select a task:

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

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.

Contractive Directory ×	- □ × 份☆鐙 [。]
Microsoft Active Directory Certificate Services - CLUSTER2TEMP-CA	Home
Certificate Issued	
The certificate you requested was issued to you.	
● DER encoded or ○ Base 64 encoded	
Download certificate	
The certnew.p7b download has completed. Open Open Open Vi	ew downloads

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

🕹 🛛 🔁 📒 🖛 🛛 Down	nloads			
File Home SI	hare View			
← ↑ ↓ >	This PC > Downl	oads		
1 Osidaraa	Name		Date modified	Туре
Desktop Downloads	¢ certnew.	Open Install Certificate Scan with Windows Defender	10/26/2021 2:22 PM	PKCS #7 Certificates
Pictures	*	Open with		

8. Acepte la advertencia de seguridad si aparece.

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

Certificate Import Wizard

Welcome to the Certificate Import Wizard

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

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

Store Location

Current User

O Local Machine

To continue, dick Next.

_	_
Next	Cancel

X

125 | Instale certificados en un entorno de grupo de trabajo para la

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.

Certificate Store	
Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location fo the certificate.	
O Automatically select the certificate store based on the type of certificate	Select Certificate Store
Place all certificates in the following store	
Certificate store:	Select the certificate store you want to use.
Browse	Personal
	Trusted Root Certification Authorities
	Enterprise Trust Totermediate Certification Authorities
	Trusted Publishers
	Intrusted Certificates
	OK Cancel

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.

CREATOR OWNER		
NETWORK SERVICE		
SYSTEM		
Pariministrators (CE031ER11		51
	Add	Remove
missions for NETWORK RVICE	Allow	Deny
Full control		
Read		
Special permissions		
special permissions or advance	ced settings.	Advanced

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

0

- 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.

Server Configurator		-	
Encryption	Encryption		
Registering servers	It is recommended to secure communication with encryptic	on. <u>Learn n</u>	tore
anguage selection	Server certificate Applies to: management server, recording server, failover server, data collector		
	Encryption: On	0	
	Concession 1	4	Details
	Camblicate issued by MS-Grganization-929-Acteus (2021), Explores 5/8/2021		
	Streaming media certificate Applies to clients and servers that retrieve data streams from the reco server	ording	
	Encryption: On		
	And the second s	4	Details
	Certificate instead by MS-Organization 9/09-Access (2021), Explore 5/0/2023		
		1.1	
		-	Apply

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:

1

• 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

0

- 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:



Welcome

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

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

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

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

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.

Download latest base 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.

S Microsoft Active Directory Certif × +	• - • ×
← → C ▲ Not secure 10.0.4.103/certsrv/certcarc.asp	☆ ≗ :
Microsoft Active Directory Certificate Services – IP-0A000467-CA	Home
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, install	this CA certificate.
To download a CA certificate, certificate chain, or CRL, select the	e certificate and encoding method.
CA certificate:	
Current [IP-0A000467-CA] ~	
Encoding method:	
OER	
O Base 64	
Install CA certificate	
Download CA certificate	
Download CA certificate chain	

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.

" Certificate Import Wizard

Welcome to the Certificate Import Wizard

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

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

To continue, dick Next.

Mart	Cancel
INEXL	Cancer

X

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.

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

Next	Cancel

8. Vaya al almacén de certificados de entidades de certificación raíz de terceros y haga clic en

Aceptar. Haga clic en Siguiente.

elect Certificate Store	×
elect the certificate store you want to use.	
Intermediate Certification Authorities Trusted Publishers	* tificates are kept,
Ontrusted Certificates Third-Party Root Certification Authorities Trusted People Client Authonication Issuers	store, or you can specify a location for
	e based on the type of certificate
_ Show physical stores	re
UK Caricel	Browse

9. 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.

Recording server information	
Name:	
Recording server 1	
Description:	
Covers sector 1	14
	1.90
Host name:	
Local web server address:	
https://	
Web server address:	
https://www.recordingserver1.dk:89/	
Time zone:	
(UTC+01:00) Brussels, Copenhagen, Madrid, Paris	

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.

perfies	
Failover server information	
Name	
Failover recording server 1	-
Description:	
Failover for Recording server 1	p-
	2
Host name:	
local	
Local web server address:	
https:// local:7563/	1
Web server address:	
https://www.failoverrecordingserver1:89/	
UDP port: 8844	
Database location:	
C:\MediaDatabase	
Enable this failover server	
Info 😭 Network 💠 Multicast	

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)

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"

Apéndice B | Crear script de certificado SSL de

```
# 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={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 - crear el certificado SSL del servidor

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

Apéndice C | Creación de script de

```
# 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. Longitud -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. Longitud -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
```



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