Markvision Enterprise

Versión 4.2

Guía del administrador

Septiembre de 2022 **www.lexmark.com**

Contenido

Historial de cambios....8

Descripción general....12

Descripción de Markvision Enterprise....12

Introducción....13

Mejores prácticas....13
Requisitos del sistema....15
Idiomas compatibles....16
Modelos de impresora admitidos....16
Configuración de la base de datos....19
Configuración para ejecutar como usuario....20
Instalación de MVE....20
Instalación silenciosa de MVE....21
Acceso a MVE....23
Cambio de idioma....24
Cambio de la contraseña....24

Mantenimiento de la aplicación....25

Actualización a MVE 4.2....25
Copia de seguridad y restauración de la base de datos....26
Actualización de la configuración del instalador tras la instalación....28

Configuración del acceso de usuario....29

Descripción general....29
Descripción de las funciones de usuario....29
Administración de usuarios....30
Activación de la autenticación del servidor LDAP....31
Instalación de certificados del servidor LDAP....33

Búsqueda de impresoras....34

Creación de perfiles de búsqueda....34
Administración de perfiles de búsqueda....36
Caso de ejemplo: Búsqueda de impresoras....37

Administración del panel de seguridad.....38

Descripción general.....38
Acceso al panel de seguridad.....38
Administración de Información de seguridad del dispositivo.....38
Administración de Comprobación de cumplimiento del dispositivo.....39

Visualización de impresoras.....40

Visualización de la lista de la impresora.....40
Visualización de la información de la impresora.....43
Exportación de datos de la impresora.....44
Administración de vistas.....44
Cambio de la vista de lista de impresoras.....46
Filtrado de impresoras mediante la barra de búsqueda.....46
Administración de palabras clave.....47
Utilización de las búsquedas guardadas.....47
Descripción de los estados de la vida útil de la impresora.....47
Ejecución de una búsqueda guardada.....49
Creación de una búsqueda guardada.....49
Descripción de la configuración de los criterios de búsqueda.....51
Administración de búsquedas guardadas.....53
Caso de ejemplo: Controlar los niveles de tóner de su flota.....54

Protección de las comunicaciones de la impresora.....55

Descripción de los estados de seguridad de la impresora.....55
Protección de impresoras con la configuración predeterminada.....56
Descripción de los permisos y controles de acceso a función.....58
Configuración de la seguridad de la impresora.....58
Protección de las comunicaciones de la impresora en su grupo.....59
Otras maneras de proteger sus impresoras.....60

Administración de impresoras.....61

Reinicio de la impresora.....61
Visualización de Embedded Web Server de la impresora.....61
Auditoría de impresoras.....61
Actualización del estado de la impresora.....61
Configuración del estado de la impresora.....62
Asignación de configuraciones a impresoras.....62

Desasignación de configuraciones....62
Aplicación de configuraciones....62
Comprobación de la conformidad de la impresora con una configuración....63
Implementación de archivos en impresoras....63
Actualización del firmware de la impresora....64
Desinstalación de aplicaciones de las impresoras....65
Asignación de eventos a impresoras....65
Asignar palabras clave a impresoras....66
Introducción de las credenciales para impresoras protegidas....66
Configuración de los certificados de la impresora predeterminada de forma manual....67
Eliminación de impresoras....67

Administración de configuraciones....69

Descripción general....69
Creación de una configuración....69
Creación de una configuración desde una impresora....72
Caso de ejemplo: clonación de una configuración....72
Creación de un componente de seguridad avanzada desde una impresora....73
Generación de una versión para imprimir de la configuración....73
Descripción de los ajustes dinámicos....73
Descripción de los ajustes de variables....73
Configuración de los permisos de impresión en color....74
Creación de un paquete de aplicaciones....75
Importación o exportación de una configuración....75
Importación de archivos a la biblioteca de recursos....76

Administración de certificados....77

Configuración de MVE para gestionar certificados de forma automática....77
Descripción de la función de administración automática de certificados....77
Configuración de MVE para la administración automática de certificados....79
Configuración de la CA de Microsoft Enterprise con NDES....81
Administración de certificados mediante la autoridad certificadora de Microsoft a través de SCEP....82
Descripción general....82
Instalación del servidor de la CA raíz....82
Configuración de la CA de Microsoft Enterprise con NDES....83
Configuración del servidor de la CA subordinada....84
Configuración de los ajustes de punto de distribución de certificación y acceso a la información de entidad....85

Configuración de la accesibilidad de la CRL ... 86
Configuración del servidor NDES ... 87
Configuración de NDES para MVE ... 88
Administración de certificados mediante la autoridad certificadora de Microsoft a través de MSCEWS ... 90
Requisitos del sistema ... 90
Requisitos de conectividad de red ... 90
Creación de certificados SSL para servidores CEP y CES ... 91
Creación de plantillas de certificado ... 92
Descripción de los métodos de autenticación ... 92
Requisitos de delegación ... 93
Configuración de la autenticación integrada de Windows ... 94
Configuración de la autenticación del certificado de cliente ... 97
Configuración de la autenticación nombre de usuario-contraseña ... 99
Administración de certificados mediante la autoridad certificadora de OpenXPKI a través de SCEP ... 101
Configuración de la CA de OpenXPKI ... 101
Configuración de la CA de OpenXPKI de forma manual ... 105
Generación de información de la CRL ... 110
Configuración de la accesibilidad de la CRL ... 111
Activación del servicio SCEP ... 111
Activación del certificado Firmante en nombre de un tercero (agente de inscripción) ... 112
Activación de la aprobación automática de solicitudes de certificado en la CA OpenXPKI ... 112
Creación de un segundo dominio ... 113
Activación de varios certificados activos con el mismo asunto para que estén presentes a la vez ... 116
Definición del número de puerto predeterminado para la CA OpenXPKI ... 116
Cómo rechazar solicitudes de certificado sin Contraseña de comprobación en la CA OpenXPKI ... 116
Adición de EKU de autenticación de cliente en los certificados ... 117
Obtención del asunto del certificado completo al realizar la solicitud a través de SCEP ... 117
Revocación de certificados y publicación de CRL ... 118
Administración de certificados mediante la autoridad certificadora de OpenXPKI a través de EST ... 119
Configuración de la CA de OpenXPKI ... 119
Configuración de la CA de OpenXPKI de forma manual ... 122
Creación de un segundo dominio ... 131

Administración de alertas de impresora ... 137

Descripción general ... 137
Creación de una acción ... 137
Descripción de los marcadores de posición de acción ... 138
Administración de acciones ... 139
Creación de un evento ... 139
Descripción de las alertas de impresora ... 140

Administración de eventos....144

Visualización del estado y el historial de las tareas....145

Descripción general....145
Visualización del estado de la tarea....145
Detención de tareas....145
Visualización de archivos de registro....145
Borrado de registros....145
Exportación de registros....146

Programación de tareas....147

Creación de un programa....147
Administración de tareas programadas....148

Realización de otras tareas administrativas....149

Configuración de los valores generales....149
Configuración de los valores del correo electrónico....149
Adición de una renuncia de responsabilidad de inicio de sesión....150
Firma del certificado MVE....150
Eliminación de la información de usuario y las referencias a este....151

Preguntas más frecuentes....153

Preguntas más frecuentes sobre Markvision Enterprise....153

Solución de problemas....156

El usuario ha olvidado la contraseña....156
El usuario administrador ha olvidado la contraseña....156
La página no se carga....157
No se puede encontrar una impresora de red....157
Información de la impresora incorrecta....157
MVE no reconoce una impresora como protegida....158
El uso de las configuraciones con varias aplicaciones genera un error en el primer intento, pero no se producen problemas en los intentos posteriores....158
Aplicación de configuraciones si falla la emisión del certificado de la impresora....159
Autoridad certificadora de OpenXPKI....159

Apéndice....162

Avisos..... 166

Glosario..... 168

Índice..... 169

Historial de cambios

Agosto de 2022

- Se ha añadido información sobre lo siguiente:
  - Protocolo Enrollment over Secure Transport (EST) según se define en RFC 7030
  - Panel de seguridad
  - Asignación automática de palabras clave durante el descubrimiento
  - Compatibilidad con correo electrónico a través de SSL/TLS
  - Compatibilidad con Windows Server 2022
- Se ha actualizado información sobre lo siguiente:
  - Modelos de impresora admitidos
  - Administración de certificados con la autoridad certificadora de Microsoft a través de los servicios web de inscripción de certificados de Microsoft (MSEWS)
  - Configuración del servidor de la CA de OpenXPKI
  - Administración de configuraciones MVE

Marzo de 2022

- Se ha actualizado la información sobre los modelos de impresora admitidos.
- Se ha añadido información sobre la creación de un certificado de cliente.

Mayo de 2021

- Se ha actualizado información sobre lo siguiente:
  - Modelos de impresora admitidos
  - Administración de la autoridad certificadora (CA) de Microsoft
  - Configuración de Markvision™ Enterprise (MVE) para la administración de certificados automatizados
  - Configuración de la CA de Microsoft Enterprise con el servicio de inscripción de dispositivos de red (NDES)
- Se ha añadido información sobre lo siguiente:
  - Administración de certificados con la autoridad certificadora de Microsoft a través de los servicios web de inscripción de certificados de Microsoft (MSEWS)
  - Creación de un certificado SSL para el servicio web de la política de inscripción de certificados (CEP) y los servidores del servicio web de inscripción de certificados (CES)
  - Métodos de autenticación para CEP y CES
  - Certificado de dispositivo con nombre

Noviembre de 2020

- Se ha actualizado información sobre lo siguiente:
  - Modelos de impresora admitidos
  - Bases de datos admitidas

- Se ha añadido información sobre lo siguiente:
  - Administración e implementación de configuraciones
  - Copia de seguridad y restauración de la base de datos
  - Administración de certificados mediante la autoridad certificadora de Microsoft y OpenXPKI
- Se ha añadido compatibilidad con lo siguiente:
  - Administración e implementación de configuraciones en un grupo de modelos de impresora
  - Creación de nombres de base de datos personalizados

Febrero de 2020

- Se ha actualizado información sobre lo siguiente:
  - Modelos de impresora admitidos
  - Servidores admitidos
  - Bases de datos admitidas
  - Ruta de actualización de MVE válida
- Se ha añadido información sobre lo siguiente:
  - Instrucciones de mejores prácticas
  - Instrucciones sobre la administración de certificados automatizados
  - Componentes de seguridad avanzada predeterminados y sus valores
  - Otras formas de proteger las impresoras
  - Casos de ejemplo

Junio de 2019

- Se ha actualizado información sobre lo siguiente:
  - Se han añadido notas a pie de página para los modelos de impresora que necesitan certificados
  - Asignación de derechos dbo al configurar la base de datos
  - Ruta de actualización válida al actualizar a la versión 3.4
  - Archivos necesarios para la copia de seguridad y la restauración de la base de datos
  - Configuración de la autenticación del servidor LDAP
  - Se ha añadido el estado de validez del certificado, las fechas y los parámetros de la zona horaria a los valores de criterios de búsqueda
  - Configuración de los permisos y los controles de acceso a funciones en los valores de seguridad de la impresora
  - Selección de un archivo de firmware de la biblioteca de recursos al actualizar el firmware de la impresora
  - Selección de la fecha de inicio, las horas de inicio y de pausa, y los días de la semana para actualizar el firmware de la impresora
  - Administración de configuraciones
- Se ha añadido información sobre lo siguiente:
  - Descripción de los estados de seguridad de la impresora
  - Configuración de los componentes de seguridad avanzada
  - Creación de un componente de seguridad avanzada desde una impresora
  - Generación de una versión para imprimir de la configuración
  - Carga de la autoridad certificadora de una flota de impresoras

- Eliminación de la información de usuario y las referencias a este
- Descripción de los permisos y los controles de acceso a funciones
- Pasos para la solución de problemas cuando falla la aplicación de configuraciones en varias aplicaciones
- Pasos para la solución de problemas cuando un usuario Administración ha olvidado la contraseña

Agosto de 2018

- Se ha actualizado información sobre lo siguiente:
  - Modelos de impresora admitidos
  - Configuración de la base de datos
  - Actualización a MVE 3.3
  - Preguntas más frecuentes
  - Creación de una acción
  - Creación de un programa
- Se ha añadido información sobre lo siguiente:
  - Configuración de una cuenta de ejecución como usuario de dominio
  - Exportación de registros
  - Pasos para la solución de problemas si MVE no reconoce las impresoras protegidas

Julio de 2018

- Se ha actualizado la información sobre cómo actualizar a MVE 3.2.

Abril de 2018

- Se ha actualizado información sobre lo siguiente:
  - Modelos de impresora admitidos
  - Configuración de la base de datos
  - Copia de seguridad y restauración de archivos de bases de datos
  - La URL para acceder a MVE
  - Descripción de los ajustes de variables
- Se ha añadido información sobre lo siguiente:
  - Configuración de los certificados de impresora
  - Detención de tareas
  - Actualización del firmware de la impresora

Septiembre de 2017

- Se ha actualizado información sobre lo siguiente:
  - Requisitos del sistema
  - Comunicación entre MVE y los modelos de impresora Lexmark™ Forms 2580, 2581, 2590 y 2591
  - Eliminación manual de bases de datos de Microsoft SQL Server
  - Copia de seguridad y restauración de archivos de bases de datos
  - Configuración de seguridad necesaria para el control de acceso a funciones al implementar archivos de firmware y soluciones en impresoras

- Compatibilidad con licencias al implementar aplicaciones
- Alertas de la impresora y acciones asociadas
- Recuperación automática del estado de la impresora
- Asignación de eventos y palabras clave

Junio de 2017

- Publicación del documento inicial para MVE 3.0.

Descripción general

Descripción de Markvision Enterprise

Markvision La empresa (MVE) es un software de utilidad de administración de impresoras basado en web diseñado para profesionales de TI.

Con MVE, puede gestionar un grupo grande de impresoras en un entorno de empresa de manera eficaz haciendo lo siguiente:

- Buscar, organizar y realizar un seguimiento de las impresoras. Puede realizar una auditoría de una impresora para recopilar datos de la impresora, como su estado, configuración y consumibles.
- Crear configuraciones y asignarlas a las impresoras.
- Implementar firmware, certificados de impresora, la autoridad de certificación (CA) y las aplicaciones en las impresoras.
- Supervisar los eventos y las alertas de las impresoras.

En este documento se proporcionan instrucciones sobre cómo configurar, utilizar y solucionar los problemas en la aplicación.

Este documento está dirigido a administradores.

Introducción

Mejores prácticas

En este tema se indican los pasos recomendados para utilizar MVE y gestionar su flota de forma efectiva.

1. Instale MVE en su entorno.
   a. Cree un servidor con el entorno Windows Server más reciente.

      Contenido relacionado:

      Requisitos de servidor web

   b. Cree una cuenta de usuario de dominio que no tenga acceso de administrador.

      Contenido relacionado:

      Configuración para ejecutar como usuario

   c. Cree una base de datos de Microsoft SQL Server, configure el cifrado y, a continuación, otorgue a la nueva cuenta de usuario acceso a las bases de datos.

      Contenido relacionado:

      - **Requisitos de base de datos**
      - **Configuración de la base de datos**

   d. Instale MVE con la cuenta de usuario de dominio y el servidor SQL con la autenticación de Windows.

      Contenido relacionado:

      Instalación de MVE

2. Configure MVE y, a continuación, detecte y organice su flota.
   a. Firme el certificado del servidor.

      Contenido relacionado:

      - **Firma del certificado MVE**
      - **Configuración de MVE para gestionar certificados de forma automática**

   b. Configure los valores de LDAP.

      Contenido relacionado:

      - **Activación de la autenticación del servidor LDAP**
      - **Instalación de certificados LDAP**

   c. Conéctese a un servidor de correo electrónico.

      Contenido relacionado:

      Configuración de los valores del correo electrónico

   d. Detecte su flota.

      Contenido relacionado:

      Búsqueda de impresoras

   e. Programe auditorías y actualizaciones de estado.

      Contenido relacionado:

      - **Auditoría de impresoras**
      - **Actualización del estado de la impresora**

f Configure los valores básicos, como los nombres de los contactos, las ubicaciones, las etiquetas de activos y las zonas horarias.

g Organice su flota. Utilice palabras clave, como las ubicaciones, para clasificar las impresoras.

Contenido relacionado:

- **Asignación de palabras clave a las impresoras**
- **Creación de una búsqueda guardada**

3 Proteja su flota.

a Proteja el acceso a las impresoras con los componentes de seguridad avanzada predeterminados.

Contenido relacionado:

- **Protección de impresoras con la configuración predeterminada**
- **Descripción de los permisos y controles de acceso a función**
- **Otras maneras de proteger sus impresoras**

b Cree una configuración segura en la que se incluyan certificados.

Contenido relacionado:

- **Creación de una configuración**
- **Importación de archivos a la biblioteca de recursos**

c Aplique la configuración a su flota actual.

Contenido relacionado:

- **Asignación de configuraciones a impresoras**
- **Aplicación de configuraciones**

d Programe las tareas de aplicación y las comprobaciones de cumplimiento.

Contenido relacionado:

Creación de un programa

e Añada configuraciones a los perfiles de búsqueda para proteger las nuevas impresoras.

Contenido relacionado:

Creación de perfiles de búsqueda

f Firme los certificados de la impresora.

Contenido relacionado:

Firma del certificado MVE

4 Mantenga actualizado el firmware.

Contenido relacionado:

Actualización del firmware de la impresora

5 Instale y configure las aplicaciones.

Contenido relacionado:

- **Creación de una configuración**
- **Importación de archivos a la biblioteca de recursos**

6 Supervise su flota.

Contenido relacionado:

Creación de una búsqueda guardada

Requisitos del sistema

MVE está instalado como servidor web y se puede acceder a él mediante un navegador web desde cualquier equipo de la red. MVE también utiliza una base de datos para almacenar información sobre la flota de impresoras. A continuación se enumeran los requisitos para el servidor web, para la base de datos y para el sistema de usuario:

Requisitos de servidor web

Procesador	Procesador de doble núcleo de al menos 2 GHz que utilice tecnología hyper-threading (HTT)
RAM	Al menos 4 GB
Unidad de disco duro	Al menos 60 GB

Nota: MVE, Document Distributor de Lexmark (LDD) y Device Deployment Utility (DDU) no se pueden ejecutar en el mismo servidor.

Servidores admitidos

- Windows Server 2022 Standard Edition
- Windows Server 2019
- Windows Server 2016 Standard Edition
- Windows Server 2012 Standard Edition
- Windows Server 2012 R2

  Nota: MVE es compatible con la virtualización de los servidores compatibles en un entorno local.

Requisitos de base de datos

Bases de datos admitidas

- Firebird® base de datos (integrada)
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012

  Nota: El tamaño mínimo recomendado para la base de datos es de 60 GB para asignar 20 MB a FRAMEWORK y 4,5 MB a MONITOR y QUARTZ. Para obtener más información, consulte "Configuración de la base de datos" en la página 19.

Requisitos del sistema de usuario

Navegadores web admitidos

- Microsoft Edge
- Mozilla Firefox (última versión)
- Google Chrome™ (última versión)
- Apple Safari (última versión)

Resolución de pantalla

Al menos 1280 x 768 píxeles

Idiomas compatibles

- Portugués de Brasil
- Inglés
- Francés
- Alemán
- Italiano
- Chino simplificado
- Español

Modelos de impresora admitidos

- Lexmark 6500
- Lexmark B2236[2]
- Lexmark B2338[2], B2442[2], B2546[2], B2650[2], B2865[1]
- Lexmark B3440[2], B3442[2]
- Lexmark C2132
- Lexmark C2240[2], C2325[2], C2425[2], C2535[2]
- Lexmark C2335[2]
- Lexmark C3224[2]
- Lexmark C3326[2]
- Lexmark C3426[2]
- Lexmark C4150[2], C6160[2], C9235[2]
- Lexmark C4342[2], C4352[2]
- Lexmark C746, C748
- Lexmark C792
- Lexmark C925[1], C950
- Lexmark CS310, CS410, CS510
- Lexmark CS317, CS417, CS517
- Lexmark CS331[2]
- Lexmark CS421[2], CS521[2], CS622[2]
- Lexmark CS431[2]
- Lexmark CS531[2], CS632[2]
- Lexmark CS720[2], CS725[2]
- Lexmark CS727[2], CS728[2]
- Lexmark CS730[2]
- Lexmark CS735[2]
- Lexmark CS820[2], CS827[2]
- Lexmark CS921[2], CS923[2], CS927[2]

- Lexmark CS943[2]
- Lexmark CX310, CX410, CX510
- Lexmark CX317, CX417, CX517
- Lexmark CX331[2]
- Lexmark CX421[2], CX522[2], CX622[2], CX625[2]
- Lexmark CX431[2]
- Lexmark CX532[2]
- Lexmark CX625[2]
- Lexmark CX635[2]
- Lexmark CX725[2]
- Lexmark CX728[2]
- Lexmark CX730[2]
- Lexmark CX735[2]
- Lexmark CX820[2], CX825[2], CX827[2], CX860[2]
- Lexmark CX920[2], CX921[2], CX922[2], CX923[2], CX924[2], CX927[2]
- Lexmark CX930[2], CX931[2]
- Lexmark CX942[2], CX943[2], CX944[2]
- Impresora Lexmark Forms 2580[4], 2581[4], 2590[4], 2591[4]
- Lexmark M1140, M1145, M3150
- Lexmark M1242[2], M1246[2], M3250[2], M5255[2], M5265[2], M5270[2]
- Lexmark M3350[2]
- Lexmark M5155, M5163, M5170
- Lexmark M5255[2], M5265[2], M5270[2]
- Lexmark MB2236[2]
- Lexmark MB2338[2], MB2442[2], MB2546[2], MB2650[2], MB2770[2]
- Lexmark MB3442[2]
- Lexmark MC2325[2], MC2425[2], MC2535[2], MC2640[2]
- Lexmark MC3224[2]
- Lexmark MC3326[2]
- Lexmark MC3426[2]
- Lexmark MS310, MS312, MS315, MS410, MS415, MS510, MS610
- Lexmark MS317, MS417, MS517
- Lexmark MS321[2], MS421[2], MS521[2], MS621[2], MS622[2]
- Lexmark MS331[2], MS431[2]
- Lexmark MS531[2], MS631[2], MS632[2]
- Lexmark MS617, MS817, MS818
- Lexmark MS710, MS711, MS810, MS811, MS812
- Lexmark MS725[2], MS821[2], MS822[2], MS823[2], MS824[2], MS825[2], MS826[2]
- Lexmark MS911
- Lexmark MX310, MX410, MX510, MX511, MX610, MX611
- Lexmark MX317, MX417, MX517

- Lexmark MX321[2], MX421[2], MX521[2], MX522[2], MX622[2]
- Lexmark MX331[2], MX431[2]
- Lexmark MX432[2]
- Lexmark MX532[2], MX632[2]
- Lexmark MX617, MX717, MX718
- Lexmark MX6500
- Lexmark MX710, MX711, MX810, MX811, MX812
- Lexmark MX721[2], MX722[2], MX725[2], MX822[2], MX824[2], MX826[2]
- Lexmark MX910, MX911, MX912
- Lexmark MX931[2]
- Lexmark T650[1], T652[1], T654[1], T656[1]
- Lexmark X651[1], X652[1], X654[1], X656[1], X658[1], XS651[1], XS652[1], XS654[1], XS658[1]
- Lexmark X746, X748, X792
- Lexmark X850[1], X852[1], X854[1], X860[1], X862[1], X864[1], XS864[1]
- Lexmark X925, X950, X952, X954
- Lexmark XC2130, XC2132
- Lexmark XC2235[2], XC2240[2], XC4240[2]
- Lexmark XC2335[2]
- Lexmark XC4140[2], XC4150[2], XC6152[2], XC8155[2], XC8160[2]
- Lexmark XC9225[2], XC9235[2], XC9245[2], XC9255[2], XC9265[2]
- Lexmark XC9325[2], XC9335[2]
- Lexmark XC9445[2], XC9455[2], XC9465[2]
- Lexmark XM1135, XM1140, XM1145, XM3150
- Lexmark XM1242[2], XM1246[2], XM3250[2]
- Lexmark XM3142[2]
- Lexmark XM3350[2]
- Lexmark XM5163, XM5170, XM5263, XM5270
- Lexmark XM5365[2], XM5370[2]
- Lexmark XM7155, XM7163, XM7170, XM7263, XM7270
- Lexmark XM7355[2], MX7365[2], MX7370[2]
- Lexmark XM9145, XM9155, XM9165
- Lexmark XM9335[2]
- Lexmark XC2326
- Lexmark XC2326
- Lexmark XC4342[2], XC4352[2]

[1] Es necesario actualizar el certificado de la impresora. En esta versión, las actualizaciones de seguridad y rendimiento de la plataforma Java dejan de admitir algunos algoritmos de firma de certificados, como MD5 y SHA1. Este cambio impide que MVE funcione con algunas impresoras. Para conocer más detalles, consulte la **documentación de información de ayuda.**

[2] La compatibilidad con SNMPv3 debe estar activada en la impresora.

[3] Si se establece una contraseña de seguridad avanzada en la impresora, MVE no será compatible con ella.

[4] MVE no se puede comunicar con los modelos de impresora Lexmark Forms 2580, 2581, 2590 y 2591 si se encuentran en estado No lista. La comunicación solo funciona si MVE se ha comunicado previamente con la impresora en el estado Lista. La impresora puede estar en el estado No lista cuando se producen errores o advertencias; por ejemplo, si hay consumibles vacíos. Para cambiar el estado, resuelva el error o la advertencia y pulse **Lista**.

Configuración de la base de datos

Puede utilizar Firebird o Microsoft SQL Server como base de datos back-end. La siguiente tabla le ayudará a decidir qué base de datos utilizar.

	Firebird	Microsoft SQL Server
Instalación del servidor	Debe estar instalado en el mismo servidor que MVE.	Se puede ejecutar desde cualquier servidor.
Comunicación	Limitado únicamente al host local.	Se comunica a través de un puerto estático o instancia dinámica con nombre. Se admite la comunicación SSL/TLS con Microsoft SQL Server protegido.
Rendimiento	Muestra problemas de rendimiento con grandes flotas.	Muestra el mejor rendimiento para grandes flotas.
Tamaño de la base de datos	Los tamaños predeterminados de bases de datos son de 6 MB para FRAMEWORK y de 1 MB para MONITOR y QUARTZ. La tabla de FRAMEWORK aumenta 1 KB por cada registro de impresora añadido.	Los tamaños predeterminados de bases de datos son de 20MB para FRAMEWORK y de 4,5MB para MONITOR y QUARTZ. La tabla de FRAMEWORK aumenta 1 KB por cada registro de impresora añadido.
Configuración	Configurada automáticamente durante la instalación.	Requiere ajustar la configuración antes de la instalación.

Si utiliza Firebird, el instalador de MVE instala y configura Firebird sin ningún otro tipo de configuración.

Si utiliza Microsoft SQL Server, realice las siguientes acciones antes de instalar MVE:

- Permita a la aplicación ejecutarse automáticamente.
- Configure las bibliotecas de la red para el uso de sockets TCP/IP.
- Cree las siguientes bases de datos:

  Nota: A continuación se muestran los nombres de base de datos predeterminados. También puede proporcionar nombres de base de datos personalizados.

  - FRAMEWORK
  - MONITOR
  - QUARTZ
- Si está utilizando una instancia con nombre, configure el servicio de Microsoft SQL Server Browser para que se inicie automáticamente. De lo contrario, configure un puerto estático en los sockets TCP/IP.

- Cree una cuenta de usuario con derechos de dbowner para las tres bases de datos que MVE utiliza para conectar y configurar la base de datos. Si el usuario es una cuenta de Microsoft SQL Server, active Microsoft SQL Server y los modos de autenticación de Windows en Microsoft SQL Server.

  Nota: Si MVE está configurado para utilizar Microsoft SQL Server, al desinstalarlo no se eliminarán las tablas o bases de datos que se hayan creado. Tras la instalación, las bases de datos de FRAMEWORK, MONITOR y QUARTZ se deben eliminar manualmente.
- Asigne derechos de dbo al usuario de la base de datos y, a continuación, establezca el esquema dbo como el esquema predeterminado.

Configuración para ejecutar como usuario

Durante la instalación, puede especificar que MVE se ejecute como una cuenta del sistema local o como una cuenta de usuario de dominio. Si se ejecuta MVE como una cuenta de usuario de dominio, la instalación será más segura. La cuenta de usuario de dominio tiene privilegios limitados en comparación con una cuenta del sistema local.

	Ejecutar como cuenta de usuario de dominio	Ejecutar como sistema local
Permisos locales del sistema	• Todo tipo de acceso a archivos a lo siguiente: – *$MVE_INSTALL*/tomcat/logs – *$MVE_INSTALL*/tomcat/temp – *$MVE_INSTALL*/tomcat/work – *$MVE_INSTALL*/apps/library – *$MVE_INSTALL*/apps/dm-mve/picture – *$MVE_INSTALL*/../mve_truststore* – *$MVE_INSTALL*/jre/lib/security/cacerts – *$MVE_INSTALL*/apps/dm-mve/WEB-INF/ldap – *$MVE_INSTALL*/apps/dm-mve/download Donde *$MVE_INSTALL* es el directorio de instalación. • Privilegio de Windows: LOGON_AS_A_SERVICE	Permisos de administrador
Autenticación de conexión de la base de datos	• Autenticación de Windows con Microsoft SQL Server • Autenticación SQL	Autenticación SQL
Configuración	Debe configurarse un usuario de dominio antes de la instalación.	Configurada automática-mente durante la instalación

Si configura MVE para que se ejecute como cuenta de usuario de dominio, debe crear el usuario en el mismo dominio que el servidor MVE.

Instalación de MVE

1. Descargue el archivo ejecutable en una ruta que no contenga espacios.
2. Ejecute el archivo como administrador y siga las instrucciones que aparecen en la pantalla del equipo.

Notas:

- Las contraseñas se crean y almacenan de forma segura. Asegúrese de que recuerda sus contraseñas o guárdelas en un lugar seguro, ya que las contraseñas no se pueden descifrar una vez almacenadas.
- Si se conecta a Microsoft SQL Server mediante la autenticación de Windows, no se producirá la verificación de la conexión durante la instalación. Asegúrese de que el usuario designado para ejecutar el servicio de la ventana de MVE tiene una cuenta correspondiente en la instancia de Microsoft SQL Server. El usuario designado debe tener derechos de dbowner a las bases de datos de FRAMEWORK, MONITOR y QUARTZ.

Instalación silenciosa de MVE

Configuración de la base de datos para una instalación silenciosa

Configuración	Descripción	Valor
--help	Muestra la lista de opciones válidas.	
--version	Muestra la información del producto.	
--unattendedmodeui <unattendedmodeui>	Interfaz de usuario para el modo sin atención.	Valor predeterminado: **ninguno** Permitido: • **ninguno** • **minimal** • **minimalWithDialogs**
--optionfile <optionfile>	Archivo de opciones de instalación.	Valor predeterminado:
--debuglevel <debuglevel>	Nivel de información de depuración de nivel de detalle.	Valor predeterminado: **2** Permitido: • **0** • **1** • **2** • **3** • **4**
--mode <mode>	Modo de instalación.	Valor predeterminado: **win32** Permitido: • **win32** • **unattended**
--debugtrace <debugtrace>	Nombre del archivo de depuración.	Valor predeterminado:

Configuración	Descripción	Valor
--installer-language <installer-language>	Selección de idioma.	Valor predeterminado: **es** Permitido: • **es** • **es** • **de** • **fr** • **it** • **pt_BR** • **zh_CN**
--encryptionKey <encryptionKey>	Clave de cifrado.	Clave de cifrado: Valor predeterminado:
--prefix <prefix>	Directorio de instalación	Valor predeterminado: **C:\Archivos de programa**
--mveLexmark_runas <mveLexmark_runas>	Opciones para ejecutar como usuario.	Valor predeterminado: **LOCAL_SYSTEM** Permitido: • **LOCAL_SYSTEM** • **SPECIFIC_USER**
--serviceRunAsUsername <serviceRunAsUsername>	Nombre para ejecutar como usuario.	Nombre de usuario: Valor predeterminado:
--serviceRunAsPassword <serviceRunAsPassword>	Contraseña para ejecutar como usuario.	Contraseña: Valor predeterminado:
--mveLexmark_database <mveLexmark_database>	Tipo de base de datos.	Valor predeterminado: Permitido: • **FIREBIRD** • **SQL_SERVER**
--firebirdUsername <firebirdUsername>	Nombre de usuario de la base de datos Firebird.	Nombre de usuario: Valor predeterminado:
--firebirdPassword <firebirdPassword>	Contraseña de la base de datos Firebird.	Contraseña: Valor predeterminado:
--firebirdFWDbName <firebirdFWDbName>	Nombre de la base de datos Firebird para FRAMEWORK.	Nombres de las bases de datos: Valor predeterminado: **FRAMEWORK**
--firebirdMNDbName <firebirdMNDbName>	Nombre de la base de datos Firebird para MONITOR.	Valor predeterminado: **MONITOR**
--firebirdQZDbName <firebirdQZDbName>	Nombre de la base de datos Firebird para QUARTZ.	Valor predeterminado: **QUARTZ**
--databaseIPAddress <databaseIPAddress>	Dirección IP o nombre de host de la base de datos.	Dirección IP o nombre de host: Valor predeterminado:
--databasePort <databasePort>	Número de puerto de la base de datos.	Número de puerto: Valor predeterminado:
--instanceName <instanceName>	Nombre de instancia.	Nombre de instancia: Valor predeterminado:

Configuración	Descripción	Valor
--instanceIdentifier <instanceIdentifier>	Instancia.	Valor predeterminado: **databasePort** Permitido: • **databasePort** • **instanceName**
--databaseUsername <databaseUsername>	Nombre de usuario de la base de datos.	Nombre de usuario: Valor predeterminado:
--databasePassword <databasePassword>	Contraseña de la base de datos.	Contraseña: Valor predeterminado:
--sqlServerAuthenticationMethod <sqlServerAuthenticationMethod>	Método de autenticación de Microsoft SQL Server.	Valor predeterminado: **sqlServerDbAuthentication** Permitido: • **sqlServerDbAuthentication** • **sqlServerWindowsAuthentication**
--fWDbName <fWDbName>	Nombre de la base de datos para FRAMEWORK.	Nombres de las bases de datos: Valor predeterminado: **FRAMEWORK**
--mNDbName <mNDbName>	Nombre de la base de datos para MONITOR.	Valor predeterminado: **MONITOR**
--qZDbName <qZDbName>	Nombre de la base de datos para QUARTZ.	Valor predeterminado: **QUARTZ**
--mveAdminUsername <mveAdminUsername>	Nombre de usuario del administrador.	Nombre de usuario: Valor predeterminado: **admin**
--mveAdminPassword <mveAdminPassword>	Contraseña del administrador.	Contraseña: Valor predeterminado:

Acceso a MVE

Para acceder a MVE, utilice las credenciales de inicio de sesión que ha creado durante la instalación. También puede configurar otros métodos de inicio de sesión, como los LDAP, Kerberos u otras cuentas locales. Para obtener más información, consulte "Configuración del acceso de usuario" en la página 29.

1. Abra un navegador web y escriba **https://*MVE_SERVER*/mve/**, donde ***MVE_SERVER*** es el nombre de host o la dirección IP del servidor que aloja MVE.
2. Si es necesario, acepte la renuncia de responsabilidad.
3. Introduzca sus credenciales.
4. Haga clic en **Iniciar sesión**.

Notas:

- Después de iniciar sesión, asegúrese de que cambia la contraseña de administrador predeterminada utilizada durante la instalación. Para obtener más información, consulte "Cambio de la contraseña" en la página 24.
- Si MVE está inactivo durante más de 30 minutos, se cierra la sesión de usuario automáticamente.

Cambio de idioma

1. Abra un navegador web y escriba **`https://MVE_SERVER/mve/`**, donde ***`MVE_SERVER`*** es el nombre de host o la dirección IP del servidor que aloja MVE.
2. Si es necesario, acepte la renuncia de responsabilidad.
3. En la esquina superior derecha de la página, seleccione un idioma.

Cambio de la contraseña

1. Abra un navegador web y escriba **`https://MVE_SERVER/mve/`**, donde ***`MVE_SERVER`*** es el nombre de host o la dirección IP del servidor que aloja MVE.
2. Si es necesario, acepte la renuncia de responsabilidad.
3. Introduzca sus credenciales.
4. Haga clic en **Iniciar sesión**.
5. En la esquina superior derecha de la página, haga clic en su nombre de usuario y, a continuación, haga clic en **Cambiar contraseña**.
6. Cambie la contraseña.

Mantenimiento de la aplicación

Actualización a MVE 4.2

Antes de iniciar la actualización, realice las siguientes acciones:

- Haga una copia de seguridad de los archivos de propiedades, de la aplicación y de la base de datos. Para obtener más información, consulte "Copia de seguridad y restauración de la base de datos" en la página 26.
- Si es necesario, proporcione nombres de base de datos personalizados.

Si va a actualizar desde la versión 1.x, actualice a la versión 2.0 en primer lugar, a la versión 3.3 a continuación y luego a la versión 4.0 respectivamente, antes de actualizar a la versión 4.2. El proceso de migración de políticas solo se realiza al actualizar a MVE 2.0.

Ruta de actualización válida	**3.3** a **4.0** a **4.2**
Ruta de actualización no válida	**1.6.x** a **4.2** **2.0** a **4.2**

1. Haga una copia de seguridad de los archivos de la aplicación y de la base de datos, ya que realizar una actualización o una desinstalación siempre supone un riesgo de pérdida irrecuperable de datos. Así, en caso de se produzca un fallo en la actualización, puede utilizar los archivos de la copia de seguridad para restablecer la aplicación a su estado anterior.

   Advertencia: Posibles daños: Cuando se actualiza MVE, se modifica la base de datos. No restaure una copia de seguridad de la base de datos creada a partir de una versión anterior.

   Nota: Para obtener más información, consulte "Copia de seguridad y restauración de la base de datos" en la página 26.

2. Descargue el archivo ejecutable a una ubicación temporal.

3. Ejecute el instalador como administrador y siga las instrucciones que aparecen en la pantalla del equipo.

   Notas:

   - Al actualizar a la versión 2.0 de MVE, las políticas asignadas a las impresoras se migran a una única configuración para cada modelo de impresora. Por ejemplo, si las políticas de fax, copia, papel e impresión están asignadas a una impresora X792, se consolidan en una configuración X792. Este proceso no se aplica a las políticas que no están asignadas a las impresoras. MVE genera un archivo de registro que confirma que las políticas se han migrado correctamente a una configuración. Para obtener más información, consulte "¿Dónde se encuentran los archivos de registro?" en la página 153.
   - Después de la actualización, asegúrese de borrar la caché del navegador antes de volver a acceder a la aplicación.
   - Al actualizar MVE a la versión 3.5 o posterior, los componentes de seguridad avanzada se extraen de las configuraciones en las que se encuentran. Si uno o más componentes de seguridad avanzada son iguales, se combinan en un solo componente. El componente de seguridad avanzada resultante se añade automáticamente a la biblioteca de componentes de seguridad avanzada.

Copia de seguridad y restauración de la base de datos

Nota: Hacer una copia de seguridad o una restauración supone un riesgo potencial de pérdida de datos. Asegúrese de realizar los pasos correctamente.

Copia de seguridad de los archivos de la aplicación y de la base de datos

Se recomienda que realice una copia de seguridad de la base de datos de forma periódica.

1. Detenga el servicio Firebird y el servicio Markvision Enterprise.
   a. Abra el cuadro de diálogo Ejecutar y escriba **`services.msc`**.
   b. Haga clic con el botón derecho en **Firebird Guardian - DefaultInstance** y, a continuación, en **Detener**.
   c. Haga clic con el botón derecho en **Markvision Enterprise** y, a continuación, haga clic en **Detener**.
2. Vaya a la carpeta donde se ha instalado Markvision Enterprise.

   Por ejemplo, **`C:\Archivos de programa\`**
3. Haga una copia de seguridad de los archivos de la aplicación y de la base de datos.

Copia de seguridad de los archivos de la aplicación

Copie los archivos siguientes a un repositorio seguro:

- Lexmark\mve_encryption.jceks
- Lexmark\mve_truststore.p12
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\encryption.properties
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\platform.properties
- Lexmark\Markvision Enterprise\apps\library
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\encryption.properties
- Lexmark\Markvision Enterprise\jre\lib\security\cacerts
- Lexmark\Markvision Enterprise\tomcat\conf\server.xml

Nota: Compruebe que estos archivos están almacenados de forma correcta. Sin las claves de cifrado del archivo mve_encryption.jceks, los datos almacenados en un formato cifrado en la base de datos y en el sistema de archivos no se pueden recuperar.

Copia de seguridad de los archivos de la base de datos

Para ello, realice una de las siguientes acciones:

Nota: Los siguientes archivos utilizan los nombres de base de datos predeterminados. Estas instrucciones también se aplican a los nombres de base de datos personalizados.

- Si está utilizando una base de datos Firebird, copie los siguientes archivos en un repositorio seguro. Se debe realizar una copia de seguridad de estos archivos con regularidad para evitar pérdidas de datos.
  - Lexmark\Markvision Enterprise\firebird\security2.fdb

    Si utiliza nombres de base de datos personalizados, actualice lo siguiente:
    - Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\database.properties
    - Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\database.properties

    - Lexmark\Markvision Enterprise\apps\mve-data-service/WEB-INF\classes\application.yml
    - Lexmark\Markvision Enterprise\firebird\aliases.conf
  - Lexmark\Markvision Enterprise\firebird\data\QUARTZ.FDB
  - Lexmark\Markvision Enterprise\firebird\data\MONITOR.FDB
  - Lexmark\Markvision Enterprise\firebird\data\FRAMEWORK.FDB
- Si está utilizando Microsoft SQL Server, cree una copia de seguridad de FRAMEWORK, MONITOR y QUARTZ.

  Para obtener más información, póngase en contacto con el administrador de Microsoft SQL Server.

4. Reinicie el servicio Firebird y el servicio Markvision Enterprise.
   a. Abra el cuadro de diálogo Ejecutar y escriba **`services.msc`**.
   b. Haga clic con el botón derecho en **Firebird Guardian - DefaultInstance** y, a continuación, en **Reiniciar**.
   c. Haga clic con el botón derecho en **Markvision Enterprise** y, a continuación, haga clic en **Reiniciar**.

Restauración de los archivos de la aplicación y de la base de datos

Advertencia: Posibles daños: Cuando se lleva a cabo la actualización MVE, la base de datos puede modificarse. No restaure una copia de seguridad de la base de datos creada a partir de una versión anterior.

1. Pare el dispositivo Markvision Enterprise.

   Para obtener más información, consulte paso 1 de "Copia de seguridad de los archivos de la aplicación y de la base de datos" en la página 26.

2. Vaya a la carpeta donde se ha instalado Markvision Enterprise.

   Por ejemplo, **`C:\Archivos de programa\`**

3. Restaure los archivos de la aplicación.

   Sustituya los archivos siguientes por archivos que haya guardado durante el proceso de creación de la copia de seguridad:

   - Lexmark\mve_encryption.jceks
   - Lexmark\mve_truststore.p12
   - Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\database.properties
   - Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\encryption.properties
   - Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\platform.properties
   - Lexmark\Markvision Enterprise\apps\library
   - Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\database.properties
   - Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\encryption.properties
   - Lexmark\Markvision Enterprise\jre\lib\security\cacerts
   - Lexmark\Markvision Enterprise\tomcat\conf\server.xml

   Nota: Puede restaurar una copia de seguridad de una base de datos a una nueva instalación MVE solo si la nueva instalación MVE tiene la misma versión.

4. Restaure los archivos de la base de datos.

   Para ello, realice una de las siguientes acciones:

   - Si utiliza una base de datos Firebird, sustituya los siguientes archivos que guardó durante el proceso de copia de seguridad:

Nota: Los siguientes archivos utilizan los nombres de base de datos predeterminados. Esta instrucción también se aplica a los nombres de base de datos personalizados.

- Lexmark\Markvision Enterprise\firebird\security2.fdb

  Si utiliza nombres de base de datos personalizados, también se restauran los siguientes archivos:

  - Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\database.properties
  - Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\database.properties
  - Lexmark\Markvision Enterprise\apps\mve-data-service/WEB-INF\classes\application.yml
  - Lexmark\Markvision Enterprise\firebird\aliases.conf
- Lexmark\Markvision Enterprise\firebird\data\QUARTZ.FDB
- Lexmark\Markvision Enterprise\firebird\data\MONITOR.FDB
- Lexmark\Markvision Enterprise\firebird\data\FRAMEWORK.FDB

- Si utiliza Microsoft SQL Server, póngase en contacto con su administrador de Microsoft SQL Server.

5. Reinicie el servicio Markvision Enterprise.

   Para obtener más información, consulte paso 4 de "Copia de seguridad de los archivos de la aplicación y de la base de datos" en la página 26.

Actualización de la configuración del instalador tras la instalación

La utilidad de contraseña de Markvision Enterprise le permite actualizar la configuración del servidor Microsoft SQL Server que se ha configurado durante la instalación sin necesidad de volver a instalar MVE. La utilidad también le permite actualizar las credenciales de la cuenta de dominio para ejecutar como usuario; por ejemplo, el nombre de usuario y la contraseña. También puede utilizar la utilidad para crear otro usuario Administrador si ha olvidado las credenciales de su usuario Administrador anterior.

1. Vaya a la carpeta donde se ha instalado Markvision Enterprise.

   Por ejemplo, **`C:\Archivos de programa\`**

2. Ejecute el archivo **mvepwdutility-windows.exe** en el directorio Lexmark\Markvision Enterprise\.

3. Seleccione un dispositivo y, a continuación, haga clic en **Aceptar** > **Siguiente**.

4. Siga las instrucciones que aparecen en la pantalla del equipo.

Configuración del acceso de usuario

Descripción general

MVE le permite agregar usuarios internos directamente al servidor MVE o utilizar las cuentas de usuario registradas en un servidor LDAP. Para obtener más información sobre la adición de usuarios internos, consulte "Administración de usuarios" en la página 30. Para obtener más información sobre cómo utilizar cuentas de usuario de LDAP, consulte "Activación de la autenticación del servidor LDAP" en la página 31.

Al agregar usuarios, se tienen que asignar las funciones. Para obtener más información, consulte "Descripción de las funciones de usuario" en la página 29.

Durante la autenticación, el sistema comprueba las credenciales de usuario de los usuarios internos presentes en el servidor MVE. Si MVE no puede autenticar el usuario, intenta realizar la autenticación en el servidor LDAP. Si el nombre de usuario existe tanto en el servidor MVE como LDAP, se utiliza la contraseña en el servidor MVE.

Descripción de las funciones de usuario

Los usuarios MVE se pueden asignar a una o más funciones. Según la función, los usuarios pueden realizar las siguientes tareas:

- **Administrador**: acceder y realizar tareas en todos los menús. También tienen privilegios administrativos, como agregar usuarios al sistema o configurar los ajustes del sistema. Solo los usuarios con la función de administrador pueden detener cualquier tarea en ejecución, independientemente del tipo de usuario que la haya iniciado.
- **Impresoras**
  - Administrar perfiles de búsqueda.
  - Definir el estado de la impresora.
  - Realizar una auditoría.
  - Administrar categorías y palabras clave.
  - Programar una auditoría, exportación de datos y la búsqueda de impresoras.
- **Configuraciones**
  - Administrar configuraciones, como la importación y exportación de archivos de configuración.
  - Cargar archivos en la biblioteca de recursos.
  - Asignar y aplicar las configuraciones en impresoras.
  - Programar una comprobación de conformidad y ejecución de configuraciones.
  - Implementar archivos en impresoras.
  - Actualizar el firmware de la impresora.
  - Generar solicitudes de firma de certificado de impresora.
  - Descargar solicitudes de firma de certificado de impresora.
- **Gestor de incidencias**
  - Administrar acciones y eventos.
  - Asignar eventos a impresoras.
  - Probar acciones.

- **Servicio de mantenimiento**
  - Actualizar el estado de la impresora.
  - Reiniciar impresoras.
  - Ejecutar una comprobación de conformidad.
  - Aplicar las configuraciones a impresoras.

Notas:

- Todos los usuarios en MVE pueden ver la página de información de la impresora y administrar las búsquedas guardadas y vistas.
- Para obtener más información sobre la asignación de funciones de usuario, consulte "Administración de usuarios" en la página 30.

Administración de usuarios

1. Haga clic en la esquina superior derecha de la página.
2. Haga clic en **Usuario** y, a continuación, realice una de las acciones siguientes:

Añadir un usuario

a. Haga clic en **Crear**.
b. Escriba el nombre de usuario, el ID de usuario y la contraseña.
c. Seleccione las funciones.

   Nota: Para obtener más información, consulte "Descripción de las funciones de usuario" en la página 29.

d. Haga clic en **Crear usuario**.

Edite un usuario

a. Seleccione un usuario.
b. Configure los valores.
c. Haga clic en **Guardar cambios**.

Eliminar usuarios

a. Seleccione uno o más usuarios.
b. Haga clic en **Eliminar**y, a continuación, confirme la eliminación.

Nota: La cuenta de usuario se bloquea después de tres intentos fallidos de inicio de sesión consecutivos. Sólo un usuario Administrador puede reactivar la cuenta de usuario. Si el usuario Administrador está bloqueado, el sistema lo reactiva automáticamente tras cinco minutos.

Activación de la autenticación del servidor LDAP

LDAP es un protocolo basado en estándares, multiplataforma y extensible que se ejecuta directamente sobre TCP/IP. Se utiliza para acceder a bases de datos especializadas que se denominan directorios.

Para evitar mantener varias credenciales de usuario, puede utilizar el servidor LDAP de la empresa para autenticar los ID de usuario y sus contraseñas.

Como requisito, el servidor LDAP debe contener grupos de usuarios que corresponden a las funciones requeridas del usuario. Para obtener más información, consulte "Descripción de las funciones de usuario" en la página 29.

1. Haga clic en , en la esquina superior derecha de la página.
2. Haga clic en **LDAP** y, a continuación, seleccione **Activar LDAP para la autenticación**.
3. En el campo Nombre de host del servidor LDAP, escriba la dirección IP o el nombre de host del servidor LDAP donde se llevará a cabo la autenticación.

   Nota: Si desea utilizar una comunicación cifrada entre el servidor MVE y el servidor LDAP, utilice el nombre de dominio completo (FQDN).
4. Especifique el número de puerto del servidor de acuerdo con el protocolo de cifrado seleccionado.
5. Seleccione el protocolo de cifrado.
   - **Ninguno**
   - **TLS**: un protocolo de seguridad que utiliza el cifrado de datos y la autenticación de certificados para proteger la comunicación entre un servidor y un cliente. Si se selecciona esta opción, se envía un comando START_TLS al servidor LDAP una vez establecida la conexión. Utilice esta configuración si quiere establecer una comunicación segura a través del puerto 389.
   - **SSL/TLS**: un protocolo de seguridad que utiliza la criptografía de clave pública para autenticar la comunicación entre un servidor y un cliente. Utilice esta opción si quiere establecer una comunicación segura desde el inicio del enlace LDAP. Esta opción se utiliza normalmente para el puerto 636 u otros puertos LDAP seguros.
6. Seleccione el tipo de enlace.
   - **Sencillo**: el servidor MVE proporciona las credenciales especificadas al servidor LDAP para usar la utilidad de búsqueda del servidor LDAP.
     a. Escriba el nombre de usuario del enlace.
     b. Escriba la contraseña del enlace y confírmela.
   - **Kerberos**: para configurar los valores, haga lo siguiente:
     a. Escriba el nombre de usuario del enlace.
     b. Escriba la contraseña del enlace y confírmela.
     c. Haga clic en **Elegir archivo** y, a continuación, busque el archivo krb5.conf.
   - **SPNEGO**: para configurar los valores, haga lo siguiente:
     a. Escriba el nombre principal del servicio.
     b. Haga clic en **Elegir archivo** y, a continuación, busque el archivo krb5.conf.
     c. Haga clic en **Elegir archivo** y, a continuación, busque el archivo Keytab de Kerberos.

     Esta opción solo se utiliza para la configuración del Mecanismo de negociación GSSAPI simple y protegido (SPNEGO) para admitir la funcionalidad de inicio de sesión único.

7 En la sección Opciones avanzadas, configure lo siguiente:

- **Base de búsqueda**: el nombre base distinguido (DN) del nodo raíz. En la jerarquía del servidor de comunidad de LDAP, este nodo debe ser el antecesor del nodo de usuario y del nodo de grupo. Por ejemplo, **`dc=mvetest,dc=com`**.

  Nota: Al especificar el DN raíz, asegúrese de que solo **`dc`** y **`o`** sean parte del DN raíz. Si **`ou`** o **`cn`** es el antecesor de los nodos de usuario y grupo, utilice **`ou`** o **`cn`** en las bases de búsqueda de grupo y de usuario.
- **Base de búsqueda de usuarios**: el nodo en el servidor de comunidad de LDAP en el que existe el objeto de usuario. Este nodo se encuentra bajo el DN raíz, donde se muestran todos los nodos de usuario. Por ejemplo, **`ou=people`**.
- **Filtro de búsqueda de usuarios**: el parámetro para localizar un objeto de usuario en el servidor de comunidad de LDAP. Por ejemplo, **`(uid={0})`**.

  ### Ejemplos de expresiones complejas y condiciones múltiples permitidas

Iniciar sesión con	En el campo Filtro de búsqueda de usuarios, escriba
Nombre común	**`(CN={0})`**
Nombre de inicio de sesión	**`(sAMAccountName={0})`**
Nombre principal del usuario	**`(userPrincipalName={0})`**
Número de teléfono	**`(telephoneNumber={0})`**
Nombre de inicio de sesión o nombre común	**`(|(sAMAccountName={0})(CN={0}))`**

  Nota: El único patrón válido es **`{0}`**, lo que significa que MVE busca el nombre de inicio de sesión de usuario de MVE.
- **Objeto base de búsqueda de usuarios y subárbol completo**: el sistema realiza la búsqueda en todos los nodos de la base de búsqueda de usuarios.
- **Base de búsqueda de grupo**: el nodo en el servidor de comunidad de LDAP en el que están los grupos de usuarios correspondientes a las funciones de MVE. Este nodo se encuentra bajo el DN raíz, donde se muestran todos los nodos de grupo. Por ejemplo, **`ou=group`**.
- **Filtro de búsqueda de grupo**: el parámetro para localizar a un usuario dentro de un grupo que corresponda a una función en MVE.

  Nota: Solo se pueden utilizar los patrones **`{0}`** y **`{1}`**. Si se utiliza **`{0}`**, MVE busca el DN de usuario de LDAP. Si se utiliza **`{1}`**, MVE busca el nombre de inicio de sesión de usuario de MVE.
- **Atributo de función de grupo**: escriba el atributo LDAP para el nombre completo del grupo. Un atributo LDAP tiene un significado específico y define una asignación entre un atributo y un nombre de campo. Por ejemplo, el atributo LDAP **`cn`** está asociado al campo Nombre completo. El atributo LDAP **`commonname`** también está asignado al campo Nombre completo. Por lo general, este atributo debe permanecer en su valor predeterminado: **`cn`**.
- **Objeto base de búsqueda de usuarios y subárbol completo**: el sistema realiza la búsqueda en todos los nodos de la base de búsqueda de grupo.

8 En la sección Asignación de grupos de LDAP a función de MVE, escriba los nombres de los grupos LDAP que corresponden a las funciones de MVE.

Notas:

- Para obtener más información, consulte "Descripción de las funciones de usuario" en la página 29.

- Puede asignar un grupo LDAP a varias funciones de MVE. También puede introducir más de un grupo LDAP en un campo de función utilizando el carácter de barra vertical (|) para separar varios grupos. Por ejemplo, si desea incluir los grupos **`administración`** y **`activos`** para la función Administración, escriba **`administración|activos`** en el campo de función Grupos de LDAP para Admin.
- Si solo desea utilizar la función Administración y no las otras funciones de MVE, deje los campos en blanco.

9 Haga clic en **Guardar cambios**.

Instalación de certificados del servidor LDAP

Para establecer una comunicación cifrada entre el servidor MVE y el servidor LDAP, MVE debe confiar en el certificado del servidor LDAP. En la arquitectura de MVE, cuando MVE esté autenticando con un servidor LDAP, MVE es el cliente y el servidor LDAP es del mismo nivel.

1 Haga clic en en la esquina superior derecha de la página.

2 Haga clic en **LDAP** y configure LDAP. Para obtener más información, consulte "Activación de la autenticación del servidor LDAP" en la página 31.

3 Haga clic en **Probar LDAP**.

4 Introduzca un nombre de usuario y contraseña de LDAP válidos y, a continuación, haga clic en **Iniciar prueba**.

5 Compruebe la validez del certificado y, a continuación, acéptelo.

Búsqueda de impresoras

Creación de perfiles de búsqueda

El perfil de búsqueda permite encontrar impresoras en su red y agregarlas al sistema. En un perfil de búsqueda, realice una de las siguientes acciones para incluir o excluir una lista de direcciones IP o nombres de host:

- Añadir entradas de una en una
- Importar entradas mediante un archivo TXT o CSV

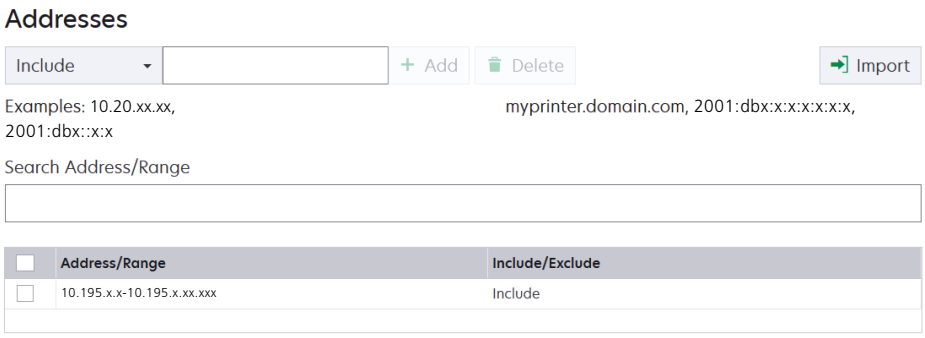
También puede asignar y aplicar una configuración automáticamente a un modelo de impresora compatible. Una configuración debe contener los valores de la impresora, aplicaciones, licencias, firmware y certificados CA que se pueden implementar para las impresoras.

1. En el menú Impresoras, haga clic en **Perfiles de búsqueda** > **Crear**.
2. En la sección General, escriba un nombre exclusivo y una descripción para el perfil de búsqueda y configure lo siguiente:
   - **Tiempo de espera**: el tiempo que espera el sistema para que responda una impresora.
   - **Reintentos**: el número de veces que el sistema intenta comunicarse con una impresora.
   - **Administrar impresoras detectadas automáticamente**: las nuevas impresoras detectadas se establecen automáticamente en un estado Administrado, y el estado Nuevo se omite durante la búsqueda.
3. En la sección Direcciones, realice una de las siguientes acciones:

Añadir las direcciones

a. Seleccione **Incluir** o **Excluir**.

b. Escriba la dirección IP, el nombre de host, la subred o el rango de direcciones IP.



No introduzca más de una entrada a la vez. Utilice los formatos siguientes para las direcciones:

- **`10.195.10.1`** (dirección IPv4 individual)
- **`miimpresora.ejemplo.com`** (nombre de host único)
- **`10.195.10.3-10.195.10.255`** (rango de direcciones IPv4)
- **`10.195.*.*`** (comodines)
- **`10.195.10.1/22`** (enrutamiento entre dominios sin clase IPv4 o notación CIDR)
- **`2001:db8:0:0:0:0:2:1`** (dirección IPv6 completa)
- **`2001:db8::2:1`** (dirección IPv6 contraída)

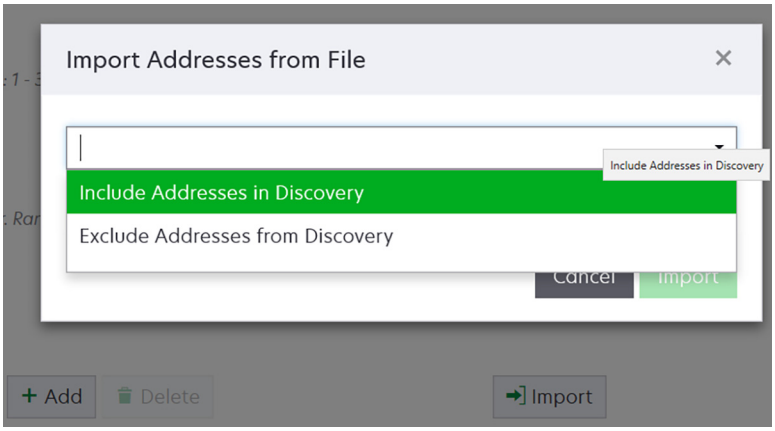
Nota: Si se crean perfiles de búsqueda independientes para las direcciones IPv6 e IPv4 de la misma impresora, se muestra la última dirección detectada. Por ejemplo, si se detecta una impresora utilizando IPv6 y se vuelve a detectar utilizando IPv4, solo se muestra la dirección IPv4 en la lista de impresoras.

c Haga clic en **Agregar**.

Importar las direcciones

a Haga clic en **Importar**.

b Seleccione si desea incluir o excluir direcciones IP durante la búsqueda.



c Busque el archivo de texto que contiene una lista de direcciones. Cada entrada de dirección debe estar en una línea distinta.

Archivo de texto de ejemplo

```
10.195.10.1
myprinter.example.com
10.195.10.3-10.195.10.255
10.195.*.*
10.195.10.1/22
2001:db8:0:0:0:0:2:1
2001:db8::2:1
```

d Haga clic en **Importar**.

4 En la sección SNMP, seleccione **Versión 1**, **Versión 2c** o **Versión 3** y configure los permisos de acceso.

Nota: Para buscar impresoras mediante la versión 3 de SNMP, cree un nombre de usuario y una contraseña en Embedded Web Server de la impresora y, a continuación, reiníciela. Si no se puede establecer una conexión, vuelva a buscar las impresoras. Para más información, consulte la *Guía del administrador de Embedded Web Server* .

5 Si fuera necesario, en la sección Introducir credenciales, seleccione el método de autenticación que utilizan las impresoras e introduzca las credenciales.

Nota: Esta función le permite establecer la comunicación con las impresoras protegidas durante la búsqueda. Se deben proporcionar las credenciales correctas para poder realizar tareas en las impresoras protegidas, como auditorías, actualizaciones de estado y actualizaciones de firmware.

6 Si fuera necesario, en la sección Asignar configuraciones, asocie una configuración a un modelo de impresora. Para obtener más información sobre la creación de configuraciones, consulte “Creación de una configuración” en la página 69.

7 Si fuera necesario, en la sección Asignar palabras clave, asocie una configuración a un modelo durante el descubrimiento. Para obtener información sobre la asignación de palabras clave a impresoras, consulte "Asignar palabras clave a impresoras" en la página 66.

Notas:

- Todas las impresoras detectadas a través de este perfil se asignan con las nuevas palabras clave.
- Las nuevas palabras clave se añaden a la lista existente de palabras clave que ya están asignadas a una impresora.

8 Haga clic en **Guardar perfil** o **Guardar y ejecutar perfil**.

Nota: Se puede programar una tarea de búsqueda para que se realice con regularidad. Para obtener más información, consulte "Creación de un programa" en la página 147.

Administración de perfiles de búsqueda

1 En el menú Impresoras, haga clic en **Perfiles de búsqueda**.

2 Haga lo siguiente:

Edite un perfil

a Seleccione un perfil y haga clic en **Editar**.

b Configure los valores.

c Haga clic en **Guardar perfil** o **Guardar y ejecutar perfil**.

Copiar un perfil

a Seleccione un perfil y haga clic en **Copiar**.

b Configure los valores.

c Agregar las direcciones IP. Para obtener más información, consulte "Añadir las direcciones" en la página 34.

d Haga clic en **Guardar perfil** o **Guardar y ejecutar perfil**.

Eliminar un perfil

a Seleccione uno o más perfiles.

b Haga clic en **Eliminar**y, a continuación, confirme la eliminación.

Ejecutar un perfil

a Seleccione uno o más perfiles.

b Haga clic en **Ejecutar**. Compruebe el estado de búsqueda desde el menú Tareas.

Caso de ejemplo: Búsqueda de impresoras

ABC es una gran empresa de fabricación que ocupa un edificio de nueve plantas. La empresa acaba de comprar 30 nuevas impresoras Lexmark y las ha distribuido en las nueve plantas. Como personal del equipo de TI, debe añadir estas nuevas impresoras a MVE. Las impresoras ya están conectadas a la red, pero desconoce todas las direcciones IP.

Quiere proteger estas impresoras nuevas del departamento de contabilidad:

10.194.55.60
10.194.56.77
10.194.55.71
10.194.63.27
10.194.63.10

Implementación de ejemplo

1. Cree un perfil de búsqueda para las impresoras del departamento de contabilidad.
2. Agregue las cinco direcciones IP.
3. Cree una configuración que proteja las impresoras en cuestión.
4. Incluya las configuraciones en el perfil de búsqueda.
5. Guarde y ejecute el perfil.
6. Cree otro perfil de búsqueda para el resto de las impresoras.
7. Incluya las direcciones IP con un comodín. Utilice lo siguiente: **10.194.*.***
8. Excluya las cinco direcciones IP de las impresoras del departamento de contabilidad.
9. Guarde y ejecute el perfil.

Administración del panel de seguridad

Descripción general

El panel de control de seguridad le permite ver el estado de la configuración de seguridad del dispositivo. Es una representación visual de varias configuraciones de seguridad, como puertos, protocolos, estado de cifrado de disco, cuentas de administrador de dispositivos y estado de certificado predeterminado. Proporciona visibilidad de la situación de seguridad de su flota, lo que ayuda a los administradores a identificar y corregir los ajustes que no cumplen las normativas.

Acceso al panel de seguridad

1. En el portal web de MVE, haga clic en **Panel**.

   Nota: El panel de seguridad es la página de inicio predeterminada para los administradores.

2. Haga clic en uno de los siguientes widgets:
   - **Información de seguridad del dispositivo**
   - **Comprobación de cumplimiento del dispositivo**

Administración de Información de seguridad del dispositivo

Este widget resume la vista de seguridad de la flota.

1. Haga clic en cualquier barra del gráfico para ir a la ventana Información de seguridad del dispositivo.
2. Pase el ratón sobre las barras para ver los siguientes detalles:
   - Número de puerto
   - Número de impresoras asociadas
   - Si la configuración de la impresora está abierta o activada
3. Haga clic en **Imprimir** para obtener un formato imprimible de la vista detallada.

Notas:

- La ventana Información de seguridad del dispositivo proporciona al usuario una función de desglose.
- Al hacer clic en cualquier elemento de la barra del gráfico, el usuario puede navegar a una vista filtrada de la página de listado de impresoras. Para obtener más información, consulte “Visualización de la lista de la impresora” en la página 40.

Administración de Comprobación de cumplimiento del dispositivo

Este widget resume la vista detallada de la comprobación de cumplimiento de la flota.

1. Haga clic en cualquier sección del gráfico circular para ir a la ventana Comprobación de cumplimiento del dispositivo.
2. En el panel izquierdo, aplique el filtro Intervalo de fechas.

   Nota: El intervalo predeterminado es de siete días.
3. Haga clic en **Imprimir** para obtener un formato imprimible de la vista detallada.

Notas:

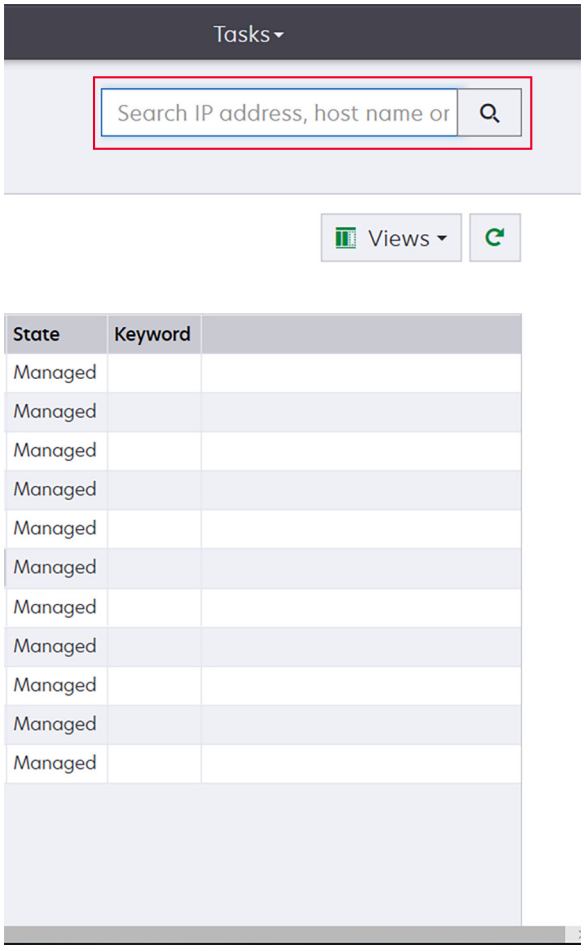
- La ventana Comprobación de cumplimiento del dispositivo proporciona al usuario una función de desglose.
- Al hacer clic en cualquier sección del gráfico circular, el usuario puede desplazarse a una vista filtrada de la página de lista de impresoras. Para obtener más información, consulte “Visualización de la lista de la impresora” en la página 40.

Visualización de impresoras

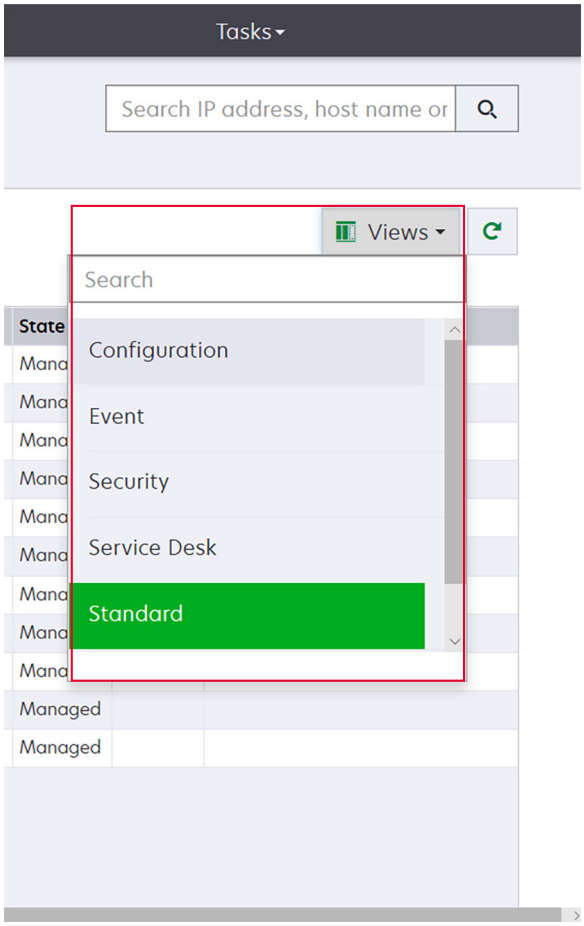
Visualización de la lista de la impresora

La página Lista de impresoras es la página de aterrizaje predeterminada al acceder a MVE. La tabla muestra la lista de las impresoras agregadas a MVE.

1. En el menú Impresoras, haga clic en **Listado de impresoras**.
2. En la página de Listado de impresoras, realice las siguientes acciones:
   - Para buscar impresoras específicas, haga lo siguiente:
     - Utilice el cuadro de búsqueda para buscar una dirección IP, un nombre de host, un nombre de sistema o el número de serie.

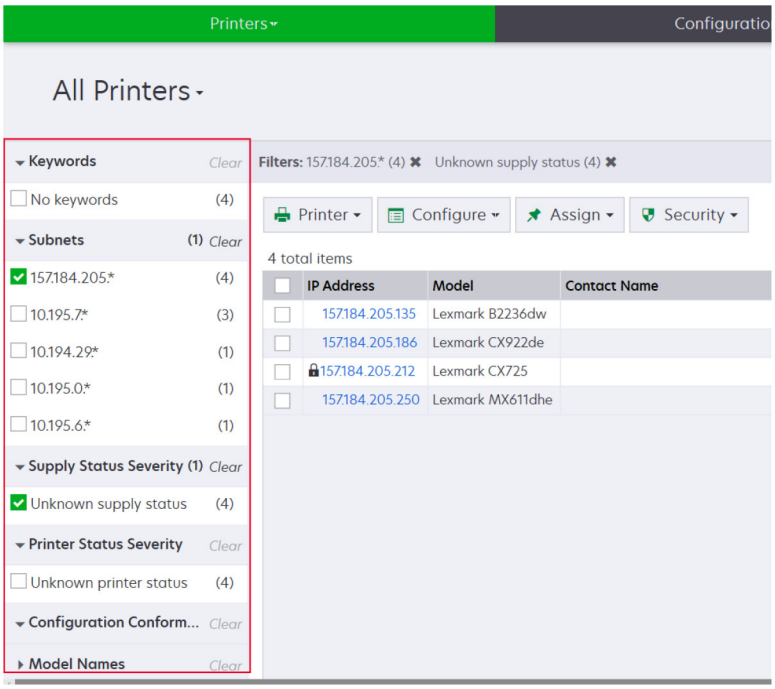


– Cambie la vista de la lista de impresoras. Para obtener más información, consulte “Cambio de la vista de lista de impresoras” en la página 46.

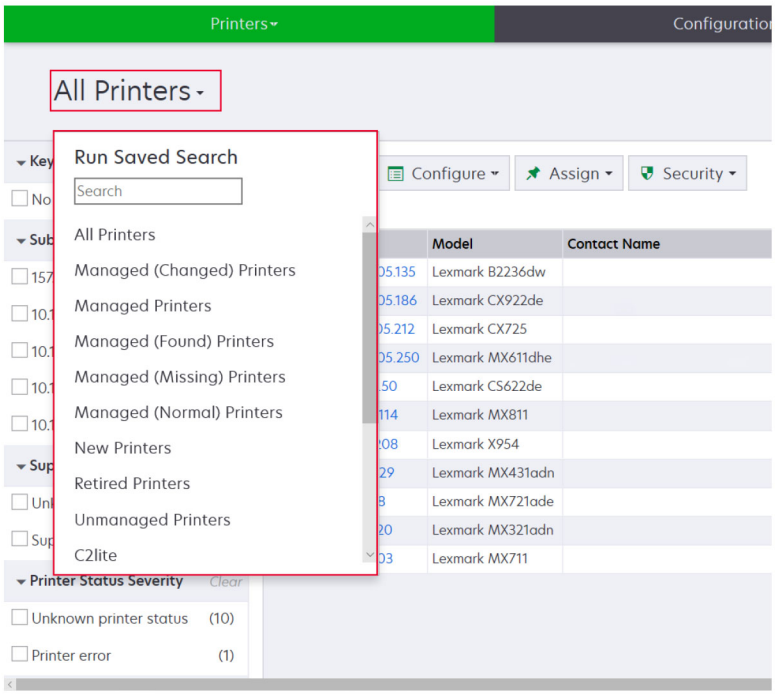


Nota: Si utiliza el cuadro de búsqueda, la aplicación busca todas las impresoras en el sistema. Los filtros seleccionados y las búsquedas guardadas se ignoran. Si ejecuta una búsqueda guardada, se utilizan los criterios especificados en la búsqueda guardada. Los filtros seleccionados y la dirección IP o el nombre de host introducido en el cuadro de búsqueda se ignoran. También puede utilizar los filtros para limitar la búsqueda actual resultados.

– Utilice los filtros.



– Ejecute una búsqueda guardada. Para obtener más información, consulte “Ejecución de una búsqueda guardada” en la página 49.



- Para ordenar las impresoras, en la tabla de la lista de impresoras, haga clic en el encabezado de cualquier columna. Las impresoras se ordenarán en función de la columna seleccionada.

- Para ver más información sobre las impresoras, cambie el tamaño de las columnas. Coloque el cursor sobre el borde vertical del encabezado de la columna y, a continuación, arrastre el borde hacia la izquierda o hacia la derecha.

Visualización de la información de la impresora

Para ver la lista completa de información, asegúrese de que se realiza una auditoría a la impresora. Para obtener más información, consulte "Auditoría de impresoras" en la página 61.

1. En el menú Impresoras, haga clic en **Listado de impresoras**.
2. Haga clic en la dirección IP de la impresora.
3. Vea la siguiente información:
   - **Estado**: el estado de la impresora.
   - **Consumibles**: los detalles de los consumibles y el porcentaje de suministro restante.
   - **Identificación**: la información de identificación de la red de la impresora.

     Nota: La información de la zona horaria solo está disponible en determinados modelos de impresora.
   - **Fechas**: la fecha en que la impresora se añade al sistema, la fecha de detección y la fecha de la auditoría más reciente.
   - **Firmware**: las propiedades del firmware de la impresora y los niveles de código.
   - **Funciones**: características de la impresora.
   - **Opciones de memoria**: el tamaño del disco duro y el espacio libre del usuario flash.
   - **Opciones de entrada**: la configuración de las bandejas disponibles.
   - **Opciones de salida**: la configuración de las salidas disponibles.
   - **Aplicaciones eSF**: la información sobre las aplicaciones Embedded Solutions Framework (eSF) instaladas en la impresora.
   - **Estadísticas de la impresora**: los valores específicos de todas las propiedades de la impresora.
   - **Cambiar detalles**: la información sobre los cambios en la impresora.

     Nota: Esta información solo se está disponible en impresoras en estado Administradas (modificadas). Para obtener más información, consulte "Descripción de los estados de la vida útil de la impresora" en la página 47.
   - **Credenciales de la impresora**: las credenciales utilizadas en la configuración asignadas a la impresora.
   - **Certificado de impresora**: propiedades del certificado de la impresora:
     - **Predeterminado**
     - **HTTPS**
     - **802.1x**
     - **IPSec**

     Notas:

     - Esta información está disponible únicamente en algunos modelos de impresora.
     - Un estado de validez Caducará pronto indica la fecha de caducidad definida en Autoridad certificadora, en Configuración del sistema.
   - **Propiedades de configuración**: las propiedades de la configuración asignadas a la impresora.

- **Alertas activas**: las alertas de la impresora que están a la espera de ser eliminadas.
- **Eventos asignados**: los eventos asignados a la impresora.

Exportación de datos de la impresora

MVE le permite exportar la información de la impresora disponible en su vista actual.

1. En el menú Impresoras , haga clic en **Listado de impresoras**.
2. Seleccione una o más impresoras.
3. Haga clic en **Impresora** > **Exportar datos**.

   Notas:

   - Los datos exportados se guardan en un archivo CSV.
   - Se puede programar una tarea de exportación de datos para que se realice con regularidad. Para obtener más información, consulte “Creación de un programa” en la página 147.

Administración de vistas

La función Vistas le permite personalizar la información que se muestra en la página de lista de impresoras.

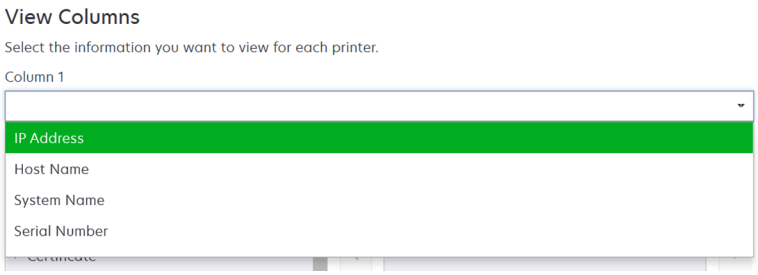
1. En el menú Impresoras, haga clic en **Vistas**.
2. Haga lo siguiente:

Crear una vista

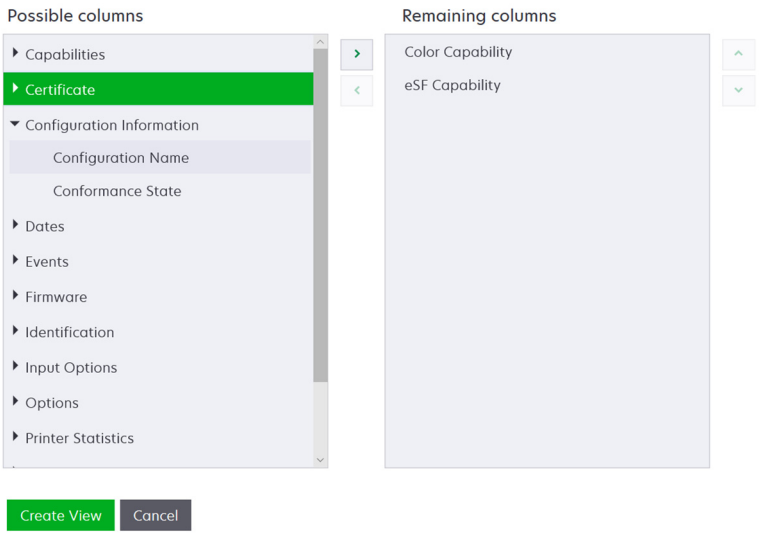
a. Haga clic en **Crear**.

b. Introduzca un nombre exclusivo para la vista y su descripción.

c. Diríjase a la pestaña Ver columnas y luego al menú Columna 1; a continuación, seleccione la columna del identificador.



d En la sección Posibles columnas , seleccione la información que desea mostrar como una columna y, a continuación, haga clic en **>**.



- **Capacidades**: muestra si las funciones seleccionadas están disponibles en la impresora.
- **Certificado**: muestra la fecha de creación del certificado de la impresora, el estado de inscripción, la fecha de caducidad, la fecha de renovación, el número de revisión, el asunto del certificado, la validez y el estado de firma.
- **Información de configuración**: muestra la información de la impresora relacionada con la configuración, como la conformidad, el nombre de la configuración y el estado.
- **Fechas**: muestra la última auditoría, la última comprobación de conformidad, la última detección y la fecha en que la impresora se añadió al sistema.
- **Eventos**: muestra información de la impresora relacionada con los eventos.
- **Firmware**: muestra información relacionada con el firmware, como la versión.
- **Identificación**: muestra información sobre la impresora, como la dirección IP, el nombre de host y el número de serie.
- **Opciones de entrada**: muestra información sobre las opciones de entrada, como el tamaño de la bandeja y el tipo de papel.
- **Opciones**: muestra información sobre las opciones de la impresora, como el disco duro y la unidad flash.
- **Estadísticas de la impresora**: muestra información sobre el uso de la impresora, como el número de páginas impresas o escaneadas y el número total de trabajos de fax.
- **Soluciones**: muestra las aplicaciones eSF instaladas en la impresora y sus números de versión.
- **Estado**: muestra el estado de los consumibles y de la impresora.
- **Consumibles**: muestra información relacionada con los consumibles.
- **Puertos de la impresora**: muestra información relacionada con los puertos.

  Nota: La opción **Desconocido** en el valor de puerto puede significar que el puerto no existe en la impresora o que MVE no puede recuperar el puerto.
- **Opciones de seguridad de la impresora**: muestra la información TLS y de cifrado.

e Haga clic en **Crear vista**.

Editar una vista

a Seleccione una vista.

b Haga clic en **Editar** y, a continuación, modifique los valores.

c Haga clic en **Guardar cambios**.

Copiar una vista

a Seleccione una vista.

b Haga clic en **Copiar** y configure los valores.

c Haga clic en **Crear vista**.

Eliminar vistas

a Seleccione una o más vistas.

b Haga clic en **Eliminar**y, a continuación, confirme la eliminación.

Establecer una vista predeterminada

a Seleccione una vista.

b Haga clic en **Establecer como predeterminada**.

El sistema genera las siguientes vistas, que no se pueden modificar ni eliminar:

- Configuración
- Lista de impresoras
- Evento
- Seguridad
- Servicio de mantenimiento
- Estándar

Cambio de la vista de lista de impresoras

Para obtener más información, consulte “Administración de vistas” en la página 44.

1. En el menú Impresoras, haga clic en **Lista de impresoras**.
2. Haga clic en **Vistas** y seleccione una vista.

Filtrado de impresoras mediante la barra de búsqueda

Tenga en cuenta lo siguiente al utilizar la barra de búsqueda para buscar impresoras.

- Si desea buscar una dirección IP, asegúrese de escribir la dirección IP o rango completos.

  Por ejemplo:

  - `10.195.10.1`
  - `10.195.10.3-10.195.10.255`
  - `10.195.*.*`
  - `2001:db8:0:0:0:0:2:1`

- Si la cadena de búsqueda no es una dirección IP completa, las impresoras se buscan según su nombre de host, nombre de sistema o número de serie.
- El carácter de guion bajo (_) se puede utilizar como un carácter comodín.

Administración de palabras clave

Las palabras clave permiten crear etiquetas personalizadas y asignarlas a las impresoras.

1. En el menú Impresoras, haga clic en **Palabras clave**.
2. Para ello, realice una de las siguientes acciones:
   - Añada, edite o elimine una categoría.

     Nota: Las categorías agrupan las palabras.
   - Añada, edite o elimine una palabra clave.

Para obtener información sobre la asignación de palabras clave a impresoras, consulte "Asignar palabras clave a impresoras" en la página 66.

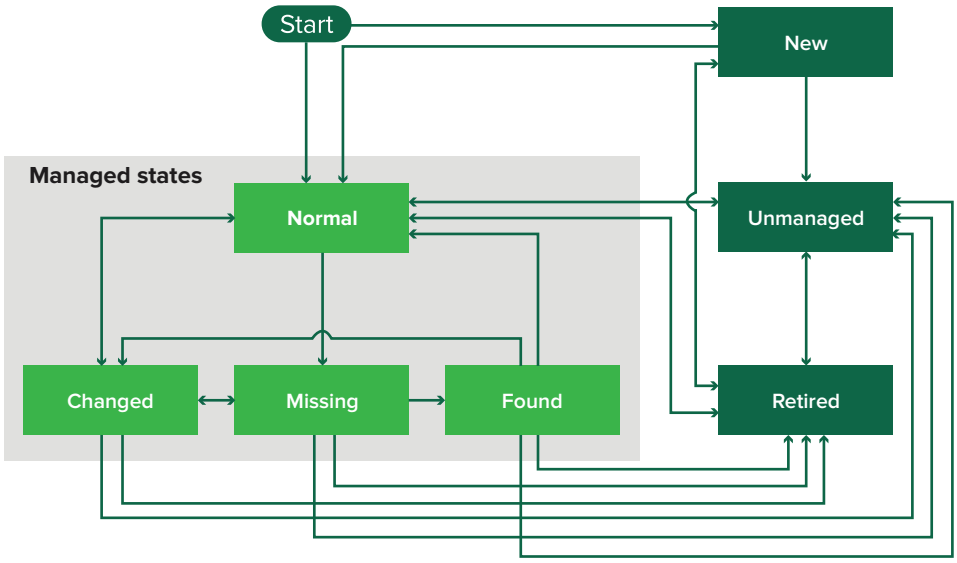
Utilización de las búsquedas guardadas

Descripción de los estados de la vida útil de la impresora

Las búsquedas guardadas generadas por el sistema muestran las impresoras en los siguientes estados de vida útil:

- **Todas las impresoras**: todas las impresoras del sistema.
- **Impresoras administradas**: las impresoras que aparecen pueden estar en cualquiera de los siguientes estados:
  - Administrada (normal)
  - Administrada (modificada)
  - Administrada (desaparecida)
  - Administrada (encontrada)
- **Impresoras administradas (modificadas)**: las impresoras en el sistema cuyas propiedades siguientes han cambiado desde la última auditoría:
  - Etiqueta de propiedad
  - Nombre de host
  - Nombre de contacto
  - Ubicación de contacto
  - Tamaño de la memoria
  - Doble cara
  - Consumibles (excluyendo los niveles)
  - Opciones de entrada
  - Opciones de salida
  - Aplicaciones eSF
  - Certificado de la impresora predeterminada

- **Impresoras administradas (encontradas)**: las impresoras que estaban declaradas como desaparecidas, pero que ahora se han encontrado.
- **Impresoras administradas (desaparecidas)**: las impresoras con las que el sistema no ha podido comunicarse.
- **Impresoras administradas (normales)**: las impresoras en el sistema cuyas propiedades han permanecido iguales desde la última auditoría.
- **Nuevas impresoras**: las impresoras recién encontradas y que no se han ajustado automáticamente al estado Administradas.
- **Impresoras retiradas**: las impresoras marcadas como que ya no están activas en el sistema.
- **Impresoras no administradas**: las impresoras que se han marcado para excluirlas de las actividades llevadas a cabo en el sistema.



Estado inicial	Estado de final	Transición
Empezar	Normal	Detectado.[1]
Empezar	Nueva	Detectado.[2]
Cualquiera	Normal, no administrada o retirada	Manual (Desaparecida no cambia a normal).
Retirada	Normal	Detectado.[1]
Retirada	Nueva	Detectado.[2]
Normal, desaparecida o encontrada	Modificada	Nueva dirección al encontrarla.
Normal	Modificada	Las propiedades de auditoría no coinciden con las de la base de datos.
Normal, cambiada o encontrada	Desaparecida	No se ha encontrado en la auditoría o en la actualización de estado.
Modificada	Normal	Las propiedades de auditoría coinciden con las de la base de datos.

[1] El ajuste "Impresoras detectadas gestionadas automáticamente" está activado en el perfil de búsqueda.

[2] El ajuste "Impresoras detectadas gestionadas automáticamente" está desactivado en el perfil de búsqueda.

Estado inicial	Estado de final	Transición
Desaparecida	Encontrada	Estado de descubierto, auditoría o actualización.
Encontrada	Normal	Estado de descubierto, auditoría o actualización.

[1] El ajuste "Impresoras detectadas gestionadas automáticamente" está activado en el perfil de búsqueda.

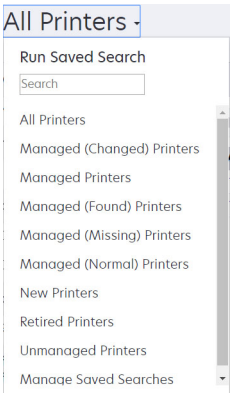
[2] El ajuste "Impresoras detectadas gestionadas automáticamente" está desactivado en el perfil de búsqueda.

Ejecución de una búsqueda guardada

Una búsqueda guardada es un conjunto guardado de parámetros que devuelve la información más reciente de la impresora que coincide con dichos parámetros.

Puede crear y ejecutar una búsqueda guardada personalizada o bien utilizar las búsquedas guardadas predeterminadas generadas por el sistema. Las búsquedas guardadas generadas por el sistema muestran las impresoras en sus estados de vida útil. Para obtener más información, consulte "Descripción de los estados de la vida útil de la impresora" en la página 47.

1. En el menú Impresoras, haga clic en **Listado de impresoras**.
2. En el menú desplegable, seleccione una búsqueda guardada.



Creación de una búsqueda guardada

Uso de filtros

1. En el menú Impresoras, haga clic en **Listado de impresoras**.
2. En el lado izquierdo de la página, seleccione los filtros.

   Nota: Los filtros seleccionados se enumeran encima del encabezado de resultados de búsqueda.
3. Haga clic en **Guardar** e introduzca un nombre exclusivo para su búsqueda guardada y su descripción.
4. Haga clic en **Crear búsqueda guardada**.

Uso de la página de búsqueda guardada

1. En el menú Impresoras, haga clic en **Búsquedas guardadas** > **Crear**.
2. En la sección General, escriba un nombre exclusivo para su búsqueda guardada y su descripción.

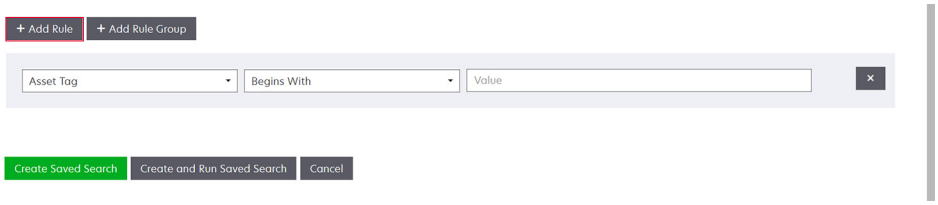
3 En la sección Reglas y grupos de reglas, en el menú Coincidencia, especifique si los resultados de búsqueda deben coincidir con todas o con alguna de las reglas.

4 Para ello, realice una de las siguientes acciones:

Agregar una regla

a Haga clic en **Agregar regla**.

b Especifique el parámetro, la operación y el valor de su criterio de búsqueda. Para obtener más información, consulte "Descripción de la configuración de los criterios de búsqueda" en la página 51.



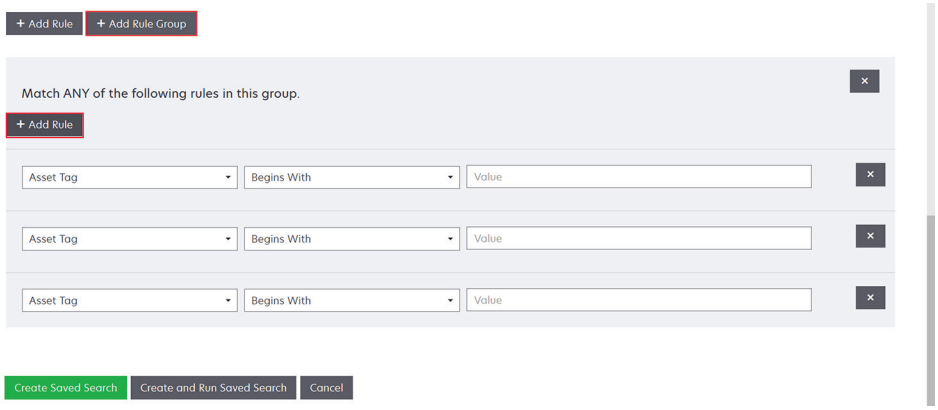
Agregar un grupo de reglas

Un grupo de reglas puede contener una combinación de reglas. Si el menú Coincidencia está definido en **CUALQUIER regla y grupo de reglas**, el sistema busca impresoras que coincidan con todas las reglas en el grupo de reglas. Si el menú Coincidencia está definido en **TODAS las reglas y grupos de reglas**, el sistema busca impresoras que coincidan con todas las reglas en el grupo de reglas.

a Haga clic en **Añadir grupo de reglas**.

b Especifique el parámetro, la operación y el valor de su criterio de búsqueda. Para obtener más información, consulte "Descripción de la configuración de los criterios de búsqueda" en la página 51.

c Para agregar otra regla, haga clic en **Agregar regla**.



5 Haga clic en **Crear búsqueda guardada** o **Crear y ejecutar búsqueda guardada**.

Descripción de la configuración de los criterios de búsqueda

Puede buscar impresoras utilizando uno o varios de los siguientes parámetros:

Parámetro	Descripción
Etiqueta de activo	El valor de la configuración de la etiqueta de activo en la impresora.
Fecha de creación del certificado[1]	La fecha en que se creó el certificado.
Estado de inscripción del certificado[1]	El estado de inscripción del certificado.
Fecha de caducidad del certificado[1]	La fecha en que caduca el certificado.
Fecha de renovación del certificado[1]	La fecha en que se renueva el certificado.
Número de revisión del certificado[1]	El número de revisión del certificado.
Estado de firma de certificado[1]	El estado del certificado.
Estado de validez del certificado[1]	La validez del certificado. **Nota:** El estado Caducará pronto indica que el certificado caducará en menos de 30 días.
Capacidad de color	La impresora imprime en color o en blanco y negro.
Configuración	El nombre de configuración asignado a la impresora.
Cumplimiento de configuración	El estado de conformidad de la impresora en relación con la configuración asignada.
Ubicación de contacto	El valor de configuración de la ubicación del contacto en la impresora.
Nombre de contacto	El valor de la configuración de nombre de la persona de contacto en la impresora.
Copia	La impresora admite la función de copia.
Fecha: adición al sistema	La fecha en que se añadió la impresora al sistema.
Fecha: última auditoría	La fecha en que la impresora se auditó por última vez.
Fecha: última comprobación de cumplimiento	La fecha en que se comprobó el cumplimiento de la configuración de la impresora por última vez.
Fecha: última detección	La fecha en que se detectó la impresora por última vez.
Codificación de disco	La impresora está configurada para la codificación de discos.
Borrado de disco	La impresora está configurada para el borrado del disco.
A dos caras	La impresora es compatible con impresión a doble cara.
Capacidad de eSF	La impresora es compatible con la administración de aplicaciones eSF.
Información de eSF	Información sobre la aplicación eSF instalada en la impresora, como el nombre, el estado y la versión.
Nombre del evento	El nombre de los eventos asignados.
Nombre de fax	El valor de la configuración de nombre de fax en la impresora.
Número de fax	El valor de la configuración de número de fax en la impresora.

Parámetro	Descripción
Recepción de fax	La impresora admite la recepción de fax.
Información de firmware	La información sobre el firmware instalado en la impresora. • **Nombre**: el nombre del firmware. Por ejemplo, **Base** o **Kernel**. • **Versión**: la versión del firmware de la impresora.
Nombre de host	El nombre de host de la impresora.
Dirección IP	La dirección IP de la impresora. **Nota:** Puede utilizar un asterisco en los tres últimos octetos para buscar varias entradas. Por ejemplo, **123.123.123.***, **123.123.*.***, **123.*.*.***, **2001:db8::2:1** y **2001:db8:0:0:0:0:2:1**.
Palabra clave	Las palabras clave asignadas.
Número total de páginas impresas	El valor del número total de páginas impresas de la impresora.
Dirección MAC	La dirección MAC de la impresora.
Contador de mantenimiento	El valor del contador de mantenimiento de la impresora.
Fabricante	El nombre del fabricante de la impresora.
Tecnología de marca	La tecnología de marca compatible con la impresora.
Capacidad de impresora mutifunción	La impresora es un producto multifuncional (MFP).
Modelo	El nombre de modelo de la impresora.
Número de serie modular	El número de serie modular.
Estado de la impresora	El estado de la impresora. Por ejemplo, **Listo**, **Atasco de papel**, **Falta bandeja 1**.
Gravedad del estado de la impresora	El valor del estado más grave presente en la impresora. Por ejemplo, **Desconocido**, **Listo**, **Advertencia** o **Error**.
Perfil	La impresora admite perfiles.
Escanear a correo electrónico	La impresora admite la digitalización a correo electrónico.
Digitalizar a fax	La impresora admite la digitalización a fax.
Digitalizar a red	La impresora admite la digitalización a red.
Estado de comunicación segura	El estado de autenticación o la seguridad de la impresora.
Número de serie	El número de serie de la impresora.
Estado	El estado actual de la impresora en la base de datos.
Estado de consumible	El estado de consumibles de la impresora.
Gravedad del estado de los consumibles	El valor del estado de los consumibles más grave presente en la impresora. Por ejemplo, **Desconocido**, **Correcto**, **Advertencia** o **Error**.
Nombre del sistema	El nombre del sistema de la impresora.
Zona horaria	La zona horaria de la región en la que se encuentra la impresora.
TLI	El valor de la configuración de TLI en la impresora.

[1]Los parámetros relacionados con el certificado se aplican a los siguientes certificados de dispositivo:

- **Predeterminado**
- **HTTPS**
- **802.1x**
- **IPSec**

Utilice los siguientes operadores cuando busque impresoras:

- **Coincide exactamente**: un parámetro es equivalente a un valor especificado.
- **No es**: un parámetro no es equivalente a un valor especificado.
- **Contiene**: un parámetro contiene un valor especificado.
- **No contiene**: un parámetro no contiene un valor especificado.
- **Comienza con**: un parámetro comienza con un valor especificado.
- **Finaliza con**: un parámetro finaliza con un valor especificado.
- **Fecha**
  - **Anterior a**: un parámetro para buscar días antes de los días especificados.
  - **Dentro del último**: un parámetro para buscar dentro de los días especificados antes del día de hoy.
  - **Dentro del siguiente**: un parámetro para buscar dentro de los días especificados después de hoy.

Nota: Para buscar impresoras que tienen parámetros con valores vacíos, utilice **`_EMPTY_O_NULL_`**. Por ejemplo, para buscar impresoras que tienen vacío el Nombre de fax en el campo Valor, escriba **`_EMPTY_O_NULL_`**.

Administración de búsquedas guardadas

1. En el menú Impresoras, haga clic en **Búsquedas guardadas**.
2. Haga lo siguiente:

Edite una búsqueda guardada

a. Seleccione una búsqueda guardada y haga clic en **Editar**.

Nota: Las búsquedas guardadas generadas por el sistema no se pueden editar. Para obtener más información, consulte “Descripción de los estados de la vida útil de la impresora” en la página 47.

b. Configure los valores.

c. Haga clic en **Guardar cambios** o **Guardar y ejecutar**.

Copiar una búsqueda guardada

a. Seleccione una búsqueda guardada y haga clic en **Copiar**.

b. Configure los valores.

c. Haga clic en **Crear búsqueda guardada** o **Crear y ejecutar búsqueda guardada**.

Eliminar búsquedas guardadas

a. Seleccionar una o más búsquedas guardadas.

Nota: Las búsquedas guardadas generadas por el sistema no se pueden eliminar. Para obtener más información, consulte “Descripción de los estados de la vida útil de la impresora” en la página 47.

b. Haga clic en **Eliminar**y, a continuación, confirme la eliminación.

Caso de ejemplo: Controlar los niveles de tóner de su flota

Como personal del equipo de TI de la empresa ABC, debe organizar la flota de impresoras para poder controlarlas fácilmente. Quiere controlar el uso de tóner de las impresoras para determinar si es necesario sustituir los consumibles.

Implementación de ejemplo

1. Cree una búsqueda guardada que recupere las impresoras cuyos consumibles tengan errores o advertencias.

   Regla de ejemplo para la búsqueda guardada

   Parámetro: **Gravedad del estado de los suministros**

   Operación: **No es**

   Valor: **Consumibles correctos**

2. Cree una vista que muestre el estado de los consumibles, la capacidad y el nivel para cada impresora.

   Columnas de ejemplo que se mostrarán en la vista de consumibles

   Estado de suministro
   Capacidad de cartucho negro
   Nivel de cartucho negro
   Capacidad de cartucho cian
   Nivel de cartucho cian
   Capacidad de cartucho magenta
   Nivel de cartucho magenta
   Capacidad de cartucho amarillo
   Nivel de cartucho amarillo

3. Ejecute la búsqueda guardada mientras utiliza la vista.

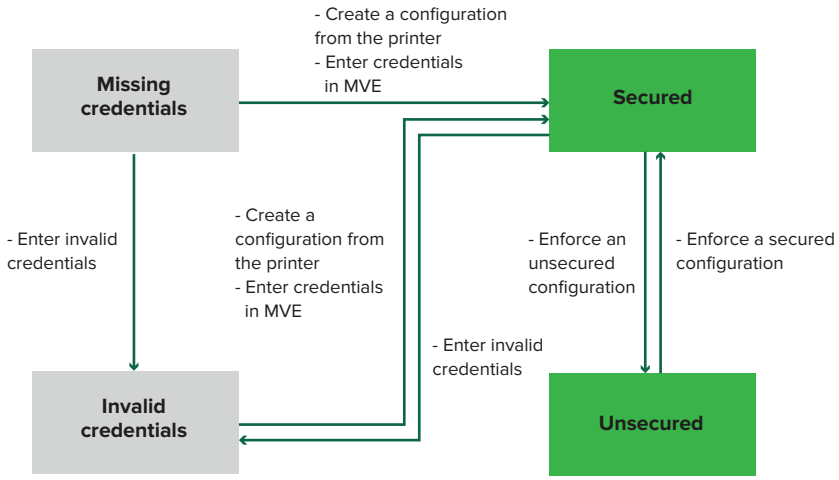
   Nota: La información que se muestra en la vista de listado de impresoras se basa en la última auditoría. Realice una auditoría y una actualización de estado para obtener el estado actual de la impresora.

Protección de las comunicaciones de la impresora

Descripción de los estados de seguridad de la impresora

Durante la detección, la impresora puede estar en cualquiera de los siguientes estados de seguridad:

- **Desprotegidas**: MVE no requiere credenciales para comunicarse con el dispositivo.
- **Protegidas**: MVE requiere credenciales y se le han proporcionado.
- **Faltan credenciales**: MVE requiere credenciales pero no se le han proporcionado.
- **Credenciales no válidas**: MVE requiere credenciales pero se le han proporcionado credenciales incorrectas.



Una impresora tiene el estado Credenciales no válidas cuando presenta credenciales no válidas durante la detección, la auditoría, la actualización del estado, la comprobación de conformidad o la aplicación de la configuración.

La impresora tiene el estado Desprotegidas únicamente cuando no requiere credenciales durante la detección.

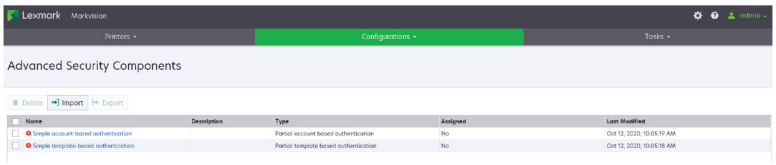
Para cambiar el estado de Desprotegidas a Protegidas, aplique una configuración protegida.

Para cambiar el estado de la impresora Faltan credenciales o Credenciales no válidas, introduzca las credenciales en MVE de forma manual o cree una configuración desde la impresora.

Protección de impresoras con la configuración predeterminada

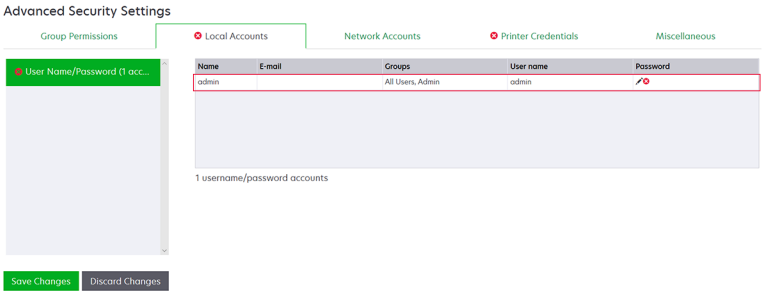
Algunos modelos de impresora no disponen de un usuario administrador predeterminado. El usuario invitado tiene acceso abierto y no tiene que iniciar sesión. Esta configuración otorga acceso al usuario a todos los permisos de la impresora y a los controles de acceso. MVE gestiona este riesgo a través de configuraciones predeterminadas. Después de una nueva instalación, se crean dos componentes de seguridad avanzada de forma automática. Cada componente contiene los valores de seguridad predeterminados y la cuenta de administrador local preconfigurada. Puede utilizar estos componentes de seguridad cuando cree una configuración y, a continuación, implementar y aplicar dicha configuración a las nuevas impresoras.

En el menú Configuraciones, haga clic en **Todos los componentes de seguridad avanzada**.

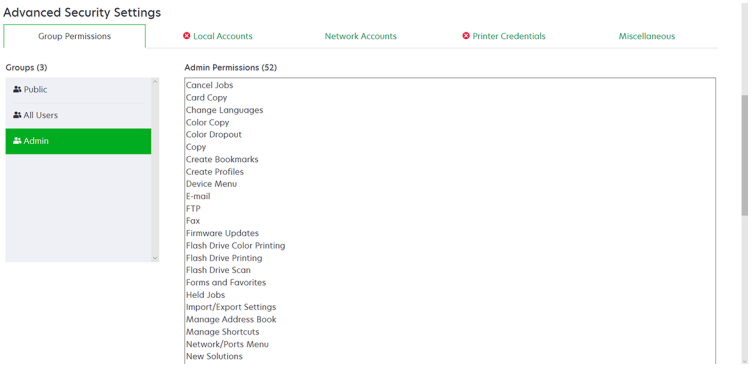


Autenticación basada en una cuenta simple

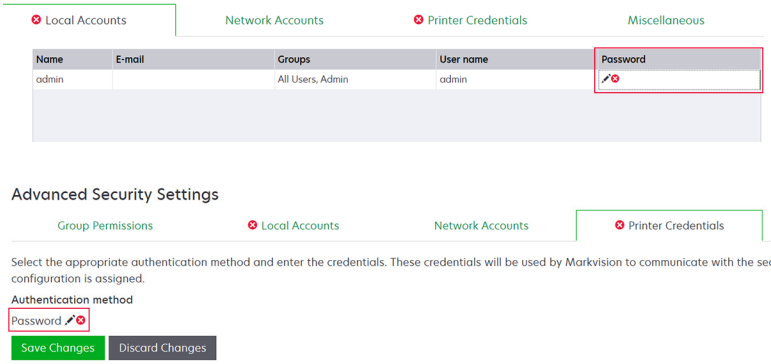
Este componente de seguridad contiene una Cuenta local Nombre de usuario/Contraseña denominada **administración**.



La cuenta **administración** es miembro del Grupo de administración, entre cuyos permisos se incluyen los controles de acceso a función, así como permisos para proteger la impresora y restringir el acceso público. Para obtener más información, consulte “Descripción de los permisos y controles de acceso a función” en la página 58.

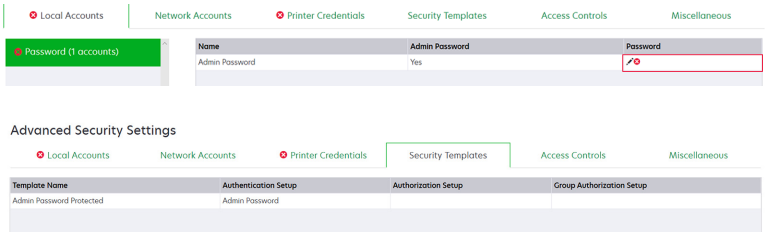


Antes de añadir este componente a una configuración, asegúrese de establecer la contraseña de **administración** y las credenciales de la impresora.



Autenticación basada en plantilla sencilla

Este componente de seguridad contiene una plantilla de seguridad denominada Proteg. con PIN admin, configurada con una Contraseña de cuenta local.

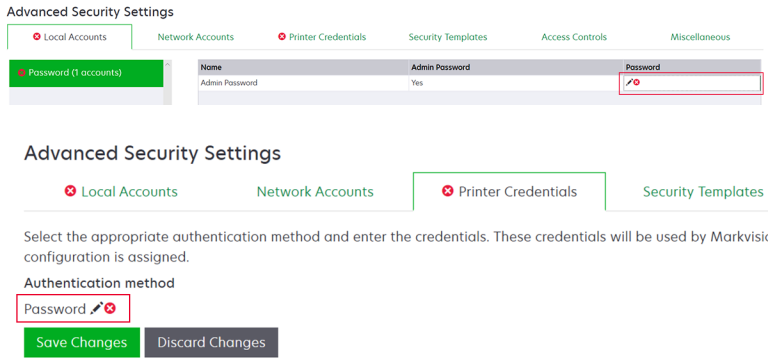


Esta plantilla de seguridad se aplica a los siguientes controles de acceso:

- Actualizaciones de firmware
- Administración remota
- Menú de seguridad de forma remota

Los controles de acceso restantes se han establecido como **Sin seguridad**. Sin embargo, siempre puede establecer los demás menús administrativos de la impresora para que utilicen la plantilla de seguridad para obtener más protección. Para obtener más información sobre los controles de acceso, consulte “Descripción de los permisos y controles de acceso a función” en la página 58.

Antes de añadir este componente a una configuración, asegúrese de establecer la contraseña y las credenciales de la impresora.



Descripción de los permisos y controles de acceso a función

Es posible configurar las impresoras para restringir el acceso público a los menús administrativos y las funciones de gestión de dispositivos. En los modelos de impresora más recientes, se pueden proteger los permisos para acceder a las funciones de la impresora mediante diferentes tipos de métodos de autenticación. En modelos de impresora anteriores, es posible aplicar una plantilla de seguridad al control de acceso a función (FAC).

Para comunicarse con estas impresoras protegidas y gestionarlas, MVE requiere determinados permisos o FAC, en función del modelo de impresora.

La siguiente tabla explica qué funciones de gestión de impresora se pueden gestionar en MVE y qué permisos o FAC se requieren.

Tenga en cuenta que MVE requiere las credenciales de autenticación cuando la Administración remota está protegida. Si otros menús administrativos y permisos de gestión de dispositivos o FAC están protegidos, entonces Administración remota también deberá estarlo. De lo contrario, MVE no podrá ejecutar las funciones.

Estos permisos y controles de acceso a funciones están predefinidos en MVE como componentes de seguridad avanzada predeterminados y se pueden utilizar fácilmente en una configuración. Para obtener más información, consulte “Protección de impresoras con la configuración predeterminada” en la página 56.

Si no utiliza los componentes de seguridad avanzada predeterminados, compruebe que estos permisos y controles de acceso a funciones se configuran manualmente en la impresora. Para obtener más información, consulte “Configuración de la seguridad de la impresora” en la página 58.

Permisos o FAC	Descripción
Administración remota	La capacidad de leer y escribir valores de forma remota. Si cualquier otro permiso o FAC incluido en esta tabla está protegido, entonces Administración remota también debe estarlo.
Actualizaciones de firmware	La capacidad de actualizar firmware utilizando cualquier método.
Configuración de aplicaciones	La capacidad de instalar o eliminar aplicaciones de la impresora y enviar los archivos de valores de la aplicación a la impresora.
Importar/Exportar todos los valores o **Importación/exportación de archivo de configuración**	La capacidad de enviar archivos de configuración a la impresora.
Menú de seguridad o **Menú de seguridad de forma remota**	La capacidad de gestionar métodos de inicio de sesión y configurar opciones de seguridad de la impresora.

Para proteger nuevos modelos de impresora en MVE, desactive el acceso público a Administración remota y los permisos del Menú de seguridad. Para modelos de impresora anteriores, aplique una plantilla de seguridad al FAC de Administración remota.

Configuración de la seguridad de la impresora

1. En el menú Impresoras, haga clic en **Lista de impresoras**.
2. Haga clic en la dirección IP de la impresora y, a continuación, haga clic en **Abrir servidor web incorporado**.

3 Haga clic en **Ajustes** o **Configuración**.

4 En función del modelo de impresora, realice una de las siguientes acciones:

- Haga clic en **Seguridad** > **Métodos de inicio de sesión** y proceda de la siguiente manera:

  ### Para los modelos de impresora más recientes

  a En la sección Seguridad, cree un método de inicio de sesión.
  b Haga clic en **Administrar grupo/permisos** o **Administrar permisos** al lado del método de inicio de sesión.
  c Expanda los **Menús administrativos** y seleccione **Menú de seguridad**.
  d Expanda **Administración de dispositivos** y, a continuación, seleccione las siguientes opciones:
  - **Administración remota**
  - **Actualizaciones de firmware**
  - **Configuración de aplicaciones**
  - **Importar/Exportar todos los valores**

  e Haga clic en **Guardar**.
  f En la sección Público, haga clic en **Administrar permisos**.
  g Despliegue los **Menús administrativos** y elimine el **Menú de seguridad**.
  h Despliegue la **Administración de dispositivos** y, a continuación, elimine la **Administración remota**.
  i Haga clic en **Guardar**.

- Haga clic en **Seguridad** > **Configuración de seguridad** o **Editar configuración de seguridad**y, a continuación, haga lo siguiente:

  ### Para los modelos de impresora anteriores

  a En la sección de Configuración de seguridad avanzada, cree un componente y una plantilla de seguridad.
  b Haga clic en **Controles de acceso** y, a continuación, expanda los **Menús administrativos**.
  c En el Menú de seguridad remota, seleccione la plantilla de seguridad.
  d Expanda **Administración** y, a continuación, seleccione la plantilla de seguridad para los siguientes controles de acceso a función:
  - **Configuración de aplicaciones**
  - **Administración remota**
  - **Actualizaciones de firmware**
  - **Importación/exportación de archivo de configuración**

  e Haga clic en **Enviar**.

Protección de las comunicaciones de la impresora en su grupo

1 Encuentre una impresora segura. Para obtener más información, consulte “Búsqueda de impresoras” en la página 34.

Notas:

- Una impresora es segura cuando aparece un junto a ella. Para obtener información sobre la protección de una impresora, consulte el **documento de ayuda**.
- Para obtener más información sobre los estados de seguridad de la impresora, consulte "Descripción de los estados de seguridad de la impresora" en la página 55.

2. Crear una configuración desde una impresora. Para obtener más información, consulte "Creación de una configuración desde una impresora" en la página 72.
3. Asigne la configuración a su flota. Para obtener más información, consulte "Asignación de configuraciones a impresoras" en la página 62.
4. Aplicar dicha configuración. Para obtener más información, consulte "Aplicación de configuraciones" en la página 62. Aparece un símbolo de candado junto a la impresora segura.

Otras maneras de proteger sus impresoras

Para obtener más información sobre la configuración de los valores de seguridad de la impresora, consulte la *Guía del administrador de Embedded Web Server* de la impresora.

En la impresora, compruebe los siguientes valores:

- Compruebe que la codificación de disco esté activada.
- Compruebe que los siguientes puertos estén restringidos:
  - TCP 79 (Finger)
  - TCP 21 (FTP)
  - UDP 69 (TFTP)
  - TCP 5001 (IPDS)
  - TCP 9600 (IPDS)
  - TCP 10000 (Telnet)
- La lista de cifrado predeterminada es la cadena de cifrado "B" de OWASP.

Administración de impresoras

Reinicio de la impresora

1 En el menú Impresoras , haga clic en **Listado de impresoras**.

2 Haga clic en la dirección IP de la impresora.

3 Haga clic en **Reiniciar impresora**.

Visualización de Embedded Web Server de la impresora

Embedded Web Server es un software integrado en la impresora que proporciona un panel de control para la configuración de la impresora desde cualquier navegador web.

1 En el menú Impresoras , haga clic en **Listado de impresoras**.

2 Haga clic en la dirección IP de la impresora.

3 Haga clic en **Abrir Embedded Web Server**.

Auditoría de impresoras

Una auditoría recopila información de cualquier impresora en estado Administrada y la almacena en el sistema. Para asegurarse de que la información del sistema es actual, realice una auditoría regularmente.

1 En el menú Impresoras, haga clic en **Lista de impresoras**.

2 Seleccione una o más impresoras.

3 Haga clic en **Impresora** > **Auditoría**.

Nota: Se puede programar una auditoría para que se realice con regularidad. Para obtener más información, consulte “Creación de un programa” en la página 147.

Actualización del estado de la impresora

La función Actualizar estado le permite actualizar el estado de la impresora y proporciona información. Para comprobar que el estado de la impresora y la información de suministros están actualizados, actualice el estado con regularidad.

1 En el menú Impresoras, haga clic en **Listado de impresoras**.

2 Seleccione una o más impresoras.

3 Haga clic en **Impresora** > **Actualizar estado**.

Nota: Se puede programar una tarea de actualización de estado para que se realice con regularidad. Para obtener más información, consulte “Creación de un programa” en la página 147.

Configuración del estado de la impresora

Para obtener más información sobre los estados de la impresora, consulte “Descripción de los estados de la vida útil de la impresora” en la página 47.

1. En el menú Impresoras, haga clic en **Lista de impresoras**.
2. Seleccione una o más impresoras.
3. Haga clic en **Impresora** y, a continuación, seleccione una de las siguientes opciones:
   - **Establecer estado en administrado**: la impresora se incluye en todas las actividades que se pueden realizar en el sistema.
   - **Establecer estado en no administrado**: la impresora se excluye de todas las actividades que se pueden realizar en el sistema.
   - **Establecer estado en retirado**: la impresora se ha eliminado de la red. El sistema conserva la información de la impresora, pero no pretende volver a ver a la impresora en la red.

Asignación de configuraciones a impresoras

Antes de comenzar, asegúrese de que se ha creado una configuración para la impresora. La asignación de una configuración a una impresora permite que el sistema ejecute comprobaciones de conformidad y de aplicación. Para obtener más información, consulte “Creación de una configuración” en la página 69.

1. En el menú Impresoras, haga clic en **Listado de impresoras**.
2. Seleccione una o más impresoras.
3. Haga clic en **Configurar** > **Asignar configuraciones**.
4. En la sección Configuración, seleccione una configuración.

   Nota: Si se ha establecido el sistema en **Utilizar Markvision para gestionar los certificados de dispositivo**, seleccione **Confiar en los dispositivos seleccionados**. Con esta confirmación, el usuario puede verificar que las impresoras son dispositivos reales y no están suplantados.
5. Haga clic en **Asignar configuraciones**.

Desasignación de configuraciones

1. En el menú Impresoras, haga clic en **Lista de impresoras**.
2. Seleccione una o más impresoras.
3. Haga clic en **Configurar** > **Desasignar configuraciones**.
4. Haga clic en **Desasignar configuraciones**.

Aplicación de configuraciones

MVE ejecuta una comprobación de conformidad con la impresora. Si algunos ajustes están fuera de conformidad, MVE cambiará los ajustes de la impresora. MVE ejecuta una comprobación de conformidad final tras modificar los ajustes. Las actualizaciones que necesitan que se reinicie la impresora, como las actualizaciones de firmware, es posible que necesiten un segundo reinicio para completarse.

Antes de empezar, asegúrese de que se ha asignado una configuración a la impresora. Para obtener más información, consulte “Asignación de configuraciones a impresoras” en la página 62.

1. En el menú Impresoras , haga clic en **Listado de impresoras**.
2. Seleccione una o más impresoras.
3. Haga clic en **Configurar** > **Aplicar las configuraciones**.

Notas:

- Si la impresora se encuentra en estado de error, es posible que algunos ajustes no se pueden actualizar.
- Para que MVE implemente archivos de firmware y soluciones en una impresora, el control de acceso a la función Actualizaciones de firmware debe estar establecido en **Sin seguridad**. Si se ha aplicado la seguridad, el control de acceso a la función Actualizaciones de firmware debe utilizar la misma plantilla de seguridad que el control de acceso a la función Administración remota. Para obtener más información, consulte “Implementación de archivos en impresoras” en la página 63.
- Se puede programar una tarea de aplicación para que se realice con regularidad. Para obtener más información, consulte “Creación de un programa” en la página 147.

Comprobación de la conformidad de la impresora con una configuración

Durante una comprobación de conformidad, MVE comprueba la configuración de la impresora y confirma si coincide con la configuración asignada. MVE no realiza cambios en la impresora durante esta operación.

Antes de empezar, asegúrese de que se ha asignado una configuración a la impresora. Para obtener más información, consulte “Asignación de configuraciones a impresoras” en la página 62.

1. En el menú Impresoras , haga clic en **Listado de impresoras**.
2. Seleccione una o más impresoras.
3. Haga clic en **Configurar** > **Comprobar la conformidad**.

   Notas:

   - Puede ver los resultados en la página de estado de la tarea.
   - Se puede programar una tarea de comprobación de conformidad para que se realice con regularidad. Para obtener más información, consulte “Creación de un programa” en la página 147.

Implementación de archivos en impresoras

Puede implementar los siguientes archivos en la impresora:

- **Certificados CA**: archivos **.cer** o **.pem** que se añaden al almacén de confianza de la impresora.
- **Paquete de configuración**: archivos **.zip** que se exportan desde una impresora compatible o que se obtienen directamente de Lexmark.
- **Actualización de firmware**: un archivo **.fls** que actualiza el firmware de la impresora.

- **Archivo genérico**: cualquier archivo que desee enviar a la impresora.
  - **Socket básico**: se envía mediante el puerto 9100. La impresora lo trata como cualquier otro dato de impresión.
  - **FTP**: se envía mediante FTP. Este método de implementación no es compatible con las impresoras con seguridad.
- **Certificado de impresora**: un certificado firmado instalado en la impresora como certificado predeterminado.
- **Archivo de configuración universal (UCF)**: un archivo de configuración exportado desde una impresora.
  - **Servicio web**: se utiliza el servicio web HTTPS cuando el modelo de impresora es compatible. En caso contrario, la impresora utiliza el servicio web HTTP.
  - **FTP**: se envía mediante FTP. Este método de implementación no es compatible con las impresoras con seguridad.

1. En el menú Impresoras haga clic en **Listado de impresoras**.
2. Seleccione una o más impresoras.
3. Haga clic en **Configurar** > **Implementar archivo en impresoras**.
4. Haga clic en **Elegir archivo** y, a continuación, busque el archivo.
5. Seleccione un tipo de archivo y un método de implementación.
6. Haga clic en **Implementar archivo**.

Notas:

- Para que MVE implemente archivos de firmware y soluciones en una impresora, el control de acceso a la función Actualizaciones de firmware debe estar establecido en **Sin seguridad**. Si se ha aplicado la seguridad, el control de acceso a la función Actualizaciones de firmware debe utilizar la misma plantilla de seguridad que el control de acceso a la función Administración remota.
- Se puede programar una tarea de implementación de archivos para que se realice con regularidad. Para obtener más información, consulte “Creación de un programa” en la página 147.

Actualización del firmware de la impresora

1. En el menú Impresoras, haga clic en **Lista de impresoras**.
2. Seleccione una o más impresoras.
3. Haga clic en **Configurar** > **Actualizar firmware en impresoras**.
4. Seleccione un archivo de firmware de la biblioteca de recursos o haga clic en **Elegir archivo**y, a continuación, busque el archivo de firmware.

   Nota: Para obtener más información sobre la adición de archivos de firmware en la biblioteca, consulte “Importación de archivos a la biblioteca de recursos” en la página 76.

5 Si es necesario, para programar la actualización, seleccione **Definir ventana de actualización**y, a continuación, seleccione la fecha de inicio, y las horas de inicio y de pausa.

Nota: El firmware se envía a las impresoras dentro la hora de inicio y la hora de pausa especificadas. La tarea se pone en pausa después de la hora de pausa y se reanuda en la siguiente hora de inicio, hasta que se haya completado.

6 Haga clic en **Actualizar firmware**.

Nota: Para que MVE actualice el firmware de la impresora, el control de acceso a la función Actualizaciones de firmware debe estar establecido en **Sin seguridad**. Si se ha aplicado la seguridad, el control de acceso a la función Actualizaciones de firmware debe utilizar la misma plantilla de seguridad que el control de acceso a la función Administración remota. En este caso, MVE debe gestionar la impresora de forma segura. Para obtener más información, consulte "Protección de las comunicaciones de la impresora" en la página 55.

Desinstalación de aplicaciones de las impresoras

MVE solo puede desinstalar las aplicaciones que se han añadido al sistema en el formato Package Builder. Para obtener más información sobre cómo cargar aplicaciones en el sistema, consulte "Importación de archivos a la biblioteca de recursos" en la página 76.

1 En el menú Impresoras, haga clic en **Listado de impresoras**.

2 Seleccione una o más impresoras.

3 Haga clic en **Configurar** > **Desinstalar aplicaciones de las impresoras**.

4 Seleccione las aplicaciones.

5 Haga clic en **Desinstalar aplicaciones**.

Asignación de eventos a impresoras

La asignación de eventos a impresoras permite a MVE realizar la acción asociada cada vez que se produce una de las alertas asociadas en la impresora asignada. Para obtener más información sobre la creación de eventos, consulte "Administración de alertas de impresora" en la página 137.

Nota: Los eventos solo pueden asignarse a impresoras sin seguridad.

1 En el menú Impresoras, haga clic en **Lista de impresoras**.

2 Seleccione una o más impresoras.

3 Haga clic en **Asignar** > **eventos**.

4 Seleccione uno o más eventos.

Nota: Si algunas de las impresoras seleccionadas ya tienen el evento asignado, aparecerá un guion en la casilla de verificación. Si lo deja como un guion, el evento no cambia. Si selecciona la casilla de verificación, el evento se asignará a todas las impresoras seleccionadas. Si desactiva la casilla de verificación, el evento dejará de estar asignado a las impresoras a las que estaba asignado.

5 Haga clic en **Asignar eventos**.

Asignar palabras clave a impresoras

La asignación de palabras clave a impresoras le permite organizar sus impresoras. Para obtener más información sobre la creación de palabras clave, consulte “Administración de palabras clave” en la página 47.

1. En el menú Impresoras, haga clic en **Lista de impresoras**.
2. Seleccione una o más impresoras.
3. Haga clic en **Asignar** > **palabras clave**.
4. Si es necesario, en el menú Ver, seleccione una categoría.
5. Seleccione una o más palabras clave.

   Nota: Las palabras clave se enumeran según una categoría. Si algunas de las impresoras seleccionadas ya tienen la palabra clave asignada, aparecerá un guion en la casilla de verificación. Si deja el guion, no se asignará ni desasignará la palabra clave a las impresoras seleccionadas. Si selecciona la casilla de verificación, la palabra clave se asignará a todas las impresoras seleccionadas. Si desactiva a casilla de verificación, la palabra clave dejará de estar asignada a las impresoras a las que estaba asignada.
6. Haga clic en **Asignar palabras clave**.

Introducción de las credenciales para impresoras protegidas

Las impresoras protegidas pueden detectarse e inscribirse. Para comunicarse con estas impresoras, puede aplicar una configuración o introducir las credenciales directamente en MVE.

Nota: Una impresora es segura cuando aparece un junto a ella.

Para introducir las credenciales, siga estas instrucciones:

1. En el menú Impresoras, haga clic en **Lista de impresoras**.
2. Seleccione una o más impresoras protegidas.
3. Haga clic en **Seguridad** > **Introducir credenciales**.
4. Seleccione el método de autenticación e introduzca las credenciales.
5. Haga clic en **Introducir credenciales**.

   Nota: Las impresoras inscritas que se encuentran protegidas pero no cuentan con las credenciales correctas guardadas en MVE se etiquetan como Faltan las credenciales en el filtro Comunicaciones. Después de introducir las credenciales correctas, las impresoras se etiquetan como Protegida.

Configuración de los certificados de la impresora predeterminada de forma manual

Cuando no utilice la función de administración de certificados automatizados, MVE puede ayudarle a facilitar el proceso de firma del certificado de la impresora predeterminada en una flota de impresoras. MVE reúne las solicitudes de firma de certificado de la flota y, una vez que los certificados están firmados, los implementa en las impresoras correspondientes.

Un administrador del sistema debe realizar las siguientes acciones:

1. Genere las solicitudes de firma de certificado de la impresora.
   a. En el menú Impresoras, haga clic en **Listado de impresoras**.
   b. Seleccione una o más impresoras.
   c. Haga clic en **Seguridad** > **Generar solicitudes de firma de certificado de impresora**.

   Nota: Al generar solicitudes de firma de certificado se puede seleccionar una o más impresoras, pero solo puede haber un conjunto de solicitudes a la vez. Para evitar que se sobrescriba alguna solicitud existente de firma de certificado, debe descargar las solicitudes de firma de certificado antes de generar otro conjunto.
2. Espere a que finalice la tarea y, a continuación, descargue las solicitudes de firma de certificado de impresora.
   a. En el menú Impresoras, haga clic en **Listado de impresoras**.
   b. Haga clic en **Seguridad** > **Descargar solicitudes de firma de certificado de impresora**.
3. Utilice una CA de confianza para firmar las solicitudes de firma de certificado.
4. Guarde los certificados firmados en un archivo ZIP.

   Nota: Todos los certificados firmados deben estar en la ubicación raíz del archivo ZIP. De lo contrario, MVE no podrá analizar el archivo.
5. En el menú Impresoras, haga clic en **Listado de impresoras**.
6. Seleccione una o más impresoras.
7. Haga clic en **Configurar** > **Implementar archivo en impresoras**.
8. Haga clic en **Elegir archivo** y, a continuación, busque el archivo ZIP.
9. En el menú Tipo de archivo, seleccione **Certificados de impresora**.
10. Haga clic en **Implementar archivo**.

Eliminación de impresoras

1. En el menú Impresoras, haga clic en **Listado de impresoras**.
2. Seleccione una o más impresoras.
3. Haga clic en **Impresora**.

4 Si es necesario, para eliminar el certificado de la impresora, seleccione **Eliminar certificados de dispositivo asociados**.

Nota: Si MVE administra los certificados de dispositivo, al eliminar el certificado de la impresora se elimina el certificado predeterminado de la impresora. En ese caso, la impresora genera un nuevo certificado firmado automáticamente.

5 Para ello, realice una de las siguientes acciones:

- Para mantener la información de la impresora, haga clic en **Retirar impresora**.
- Para eliminar la impresora del sistema, haga clic en **Eliminar impresora**.

Administración de configuraciones

Descripción general

MVE emplea configuraciones para administrar las impresoras de su flota.

Una configuración es una recopilación de valores que pueden asignarse y aplicarse a una impresora o a un grupo de modelos de impresora. Dentro de una configuración, puede modificar los valores de la impresora e implementar aplicaciones, licencias, firmware y certificados de impresoras.

Puede crear una configuración que se componga de:

- Valores básicos de la impresora
- Valores de seguridad avanzada
- Permisos de impresión en color

  Nota: Este ajuste solo está disponible en las configuraciones de las impresoras en color compatibles.
- Firmware de la impresora
- Aplicaciones
- certificados CA
- Archivos de recurso

Al utilizar configuraciones, puede hacer lo siguiente para administrar las impresoras:

- Asigne una configuración a las impresoras.
- Aplique las configuraciones a las impresoras. Los valores especificados en la configuración se aplican a las impresoras. Se instala el firmware, las aplicaciones, el certificado de impresora, los archivos de aplicación (.fls) y los certificados de CA.
- Compruebe la conformidad de las impresoras con una configuración. Si una impresora no es conforme, se le puede aplicar la configuración.

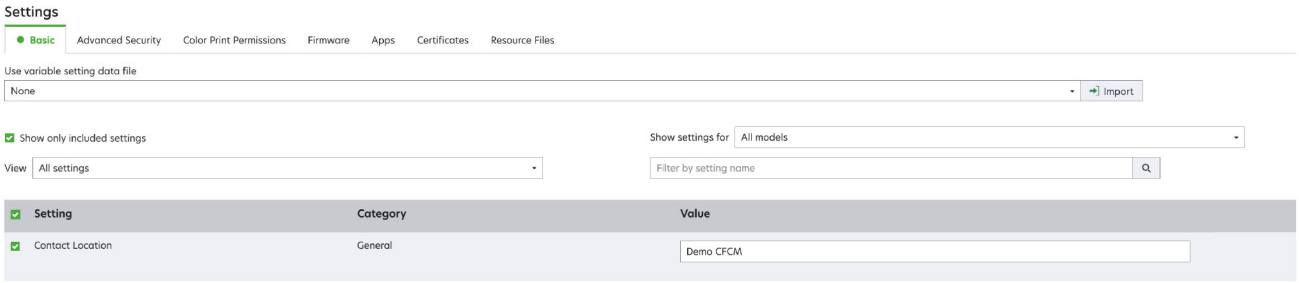
  Nota: La aplicación de la configuración y la comprobación de conformidad se pueden programar para que tengan lugar de forma periódica.
- Si la impresora admite los ajustes de configuración pero los valores no son aplicables, la impresora se muestra como no conforme.

Creación de una configuración

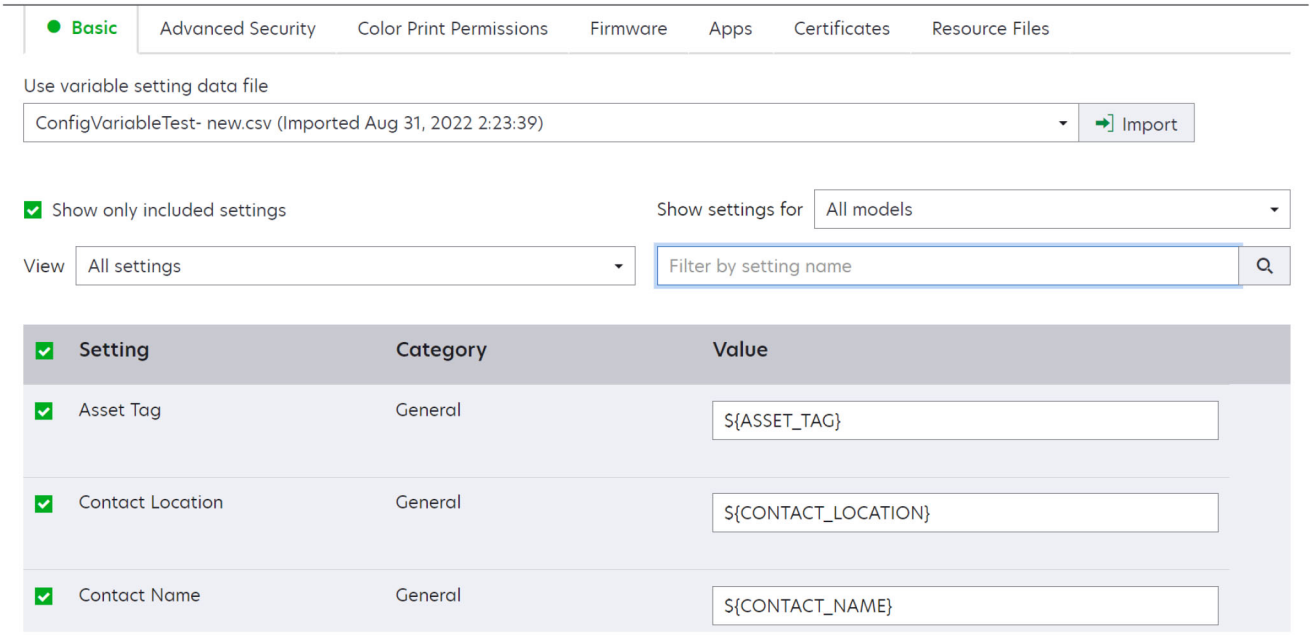
Una configuración es una recopilación de valores que se pueden asignar y aplicar a una impresora o a un grupo de impresoras. Dentro de una configuración, se pueden modificar los valores de la impresora e implementar aplicaciones, licencias, firmware y certificados CA en las impresoras.

1. En el menú Configuraciones, haga clic en **Todas las configuraciones** > **Crear**.
2. Escriba un nombre exclusivo para la configuración y su descripción.
3. En la ventana Ajuste, realice una o varias de las siguientes acciones:
   - En la pestaña Básicas, seleccione uno o más ajustes y, a continuación, especifique los valores. Si el valor es un ajuste variable, incluya el encabezado con **`${}`**. Por ejemplo, **`${Contact_Name}`**. Para utilizar un archivo de ajustes variables, selecciónelo en el menú Usar archivo de datos de configuración de

variables o impórtelo. Para obtener más información, consulte "Descripción de los ajustes de variables" en la página 73.



- Seleccionar uno o más ajustes y luego especificar los valores. Si el valor es un ajuste variable, incluya el encabezado con **${}**. Por ejemplo, **${Contact_Name}**. Para utilizar un archivo de ajustes variables, selecciónelo en el menú Usar archivo de datos de configuración de variables o impórtelo. Para obtener más información, consulte "Descripción de los ajustes de variables" en la página 73.



- Si se agregan uno o más certificados a esta configuración, puede seleccionar cualquiera de los certificados en el menú desplegable **Valor**.

- En la pestaña Seguridad avanzada, seleccione un componente de seguridad avanzada.

  Notas:

  - Para crear un componente de seguridad avanzada, consulte "Creación de un componente de seguridad avanzada desde una impresora" en la página 73.
  - Solo puede administrar la configuración de seguridad avanzada cuando se crea una configuración a partir de una impresora seleccionada. Para obtener más información, consulte "Creación de una configuración desde una impresora" en la página 72.

- Configure los ajustes en la pestaña Permisos de impresión en color. Para obtener más información, consulte "Configuración de los permisos de impresión en color" en la página 74.

  Nota: Este ajuste solo está disponible en las configuraciones de las impresoras en color compatibles.
- En la pestaña Firmware, seleccione un archivo de firmware. Si una configuración contiene varias versiones del mismo firmware, durante la conformidad y la aplicación solo se tiene en cuenta la versión superior del firmware. Para importar un archivo de firmware, consulte "Importación de archivos a la biblioteca de recursos" en la página 76.
- En la pestaña Aplicaciones seleccione una o más aplicaciones que desee implementar. Para obtener más información, consulte "Creación de un paquete de aplicaciones" en la página 75.

  Nota: MVE no admite la implementación de aplicaciones con licencias de prueba. Solo puede implementar aplicaciones gratuitas o aplicaciones con licencias de producción.
- En la pestaña Certificados, seleccione uno o más certificados que desee implementar. Para importar un archivo de certificado, consulte "Importación de archivos a la biblioteca de recursos" en la página 76.

  Nota: Seleccione **Utilizar Markvision para gestionar los certificados de dispositivo** para que MVE evalúe los certificados que falten, que no sean válidos, que estén caducados o que se hayan revocado, y los reemplace de forma automática.

  Seleccione una de las siguientes opciones:
  - Certificado de dispositivo predeterminado
  - Certificado de dispositivo con nombre

    Nota: De forma predeterminada, un usuario puede agregar 10 certificados con nombre por instalación de MVE y 5 certificados con nombre por configuración de MVE.

  Nota: Para obtener más información, consulte "Configuración de MVE para la administración automática de certificados" en la página 79.
- En la pestaña Archivos de recurso, seleccione cualquiera de los siguientes tipos de archivo para implementar:
  - **Archivo de aplicación (.fls)**
  - **Paquete de configuración (.zip)**
  - **Archivo de configuración universal (.ucf)**

  Notas:
  - Cualquier opción de la pestaña de recursos no está verificada para su conformidad.
  - No recomendamos utilizar varios paquetes de configuración y UCF en una sola configuración.
  - Este método no se aplica a los archivos UCF al configurar la digitalización a la red en impresoras anteriores. Los archivos UCF se deben implementar mediante la acción **Implementar archivo en impresora**.

4. Haga clic en **Crear configuración**.

   Nota: La siguiente lista muestra la secuencia de implementación en una configuración:

   - **Certificados CA**
   - **Archivos de aplicación**
   - **Paquetes de soluciones**
   - **Seguridad avanzada**
   - **Certificados de dispositivo**
   - **Valores básicos**

- **Paquete de configuración y UCF**
- **Firmware**

Creación de una configuración desde una impresora

No se incluyen los siguientes componentes:

- Firmware de la impresora
- Aplicaciones
- Certificados

Para añadir el firmware, las aplicaciones y los certificados, edite la configuración en MVE.

1. En el menú Impresoras, haga clic en **Lista de impresoras**.
2. Seleccione la impresora y haga clic en **Configurar** > **Crear configuración desde impresora**.
3. Si fuera necesario, seleccione **Incluir valores de seguridad avanzada** para crear un componente de seguridad avanzada desde la impresora seleccionada.
4. Si la impresora está protegida, seleccione el método de autenticación e introduzca las credenciales.
5. Escriba un nombre exclusivo para la configuración y su descripción y haga clic en **Crear configuración**.
6. En el menú Configuraciones, haga clic en **Todas las configuraciones**.
7. Seleccione la configuración y haga clic en **Editar**.
8. Si es necesario, modifique los ajustes.
9. Haga clic en **Guardar cambios**.

Caso de ejemplo: clonación de una configuración

Se han añadido 15 impresoras Lexmark MX812 al sistema tras la detección. Como personal del equipo de TI, debe aplicar los valores de las impresoras existentes a las nuevas.

Nota: También puede clonar una configuración de una impresora y, a continuación, aplicar la configuración a un grupo de modelos de impresora.

Implementación de ejemplo

1. En la lista de impresoras existentes, seleccione una impresora Lexmark MX812.
2. Cree una configuración desde la impresora.

   Nota: Para proteger las impresoras, incluya los valores de seguridad avanzada.
3. Asigne y, a continuación, aplique dicha configuración a las impresoras recién detectadas.

Creación de un componente de seguridad avanzada desde una impresora

Cree un componente de seguridad avanzada desde una impresora para gestionar los valores de seguridad avanzada. MVE lee todos los valores de esa impresora y, a continuación, crea una configuración que incluye los valores. El componente puede estar asociado a varias configuraciones para modelos de impresora con el mismo marco de seguridad.

1. En el menú Impresoras, haga clic en **Listado de impresoras**.
2. Seleccione la impresora y haga clic en **Configuración** > **Crear componente de seguridad avanzada desde la impresora**.
3. Introduzca un nombre exclusivo para el componente y su descripción.
4. Si la impresora está protegida, seleccione el método de autenticación e introduzca las credenciales.
5. Haga clic en **Crear componente**.

   Nota: Cuando crea y aplica una configuración con un componente de seguridad avanzada que contiene cuentas locales, dichas cuentas locales se añaden a las impresoras. Se conservarán las cuentas locales existentes preconfiguradas en la impresora.

Generación de una versión para imprimir de la configuración

1. Edite una configuración o un componente de seguridad avanzada.
2. Haga clic en **Versión para imprimir**.

Descripción de los ajustes dinámicos

- Estas opciones incluyen Certificado de dispositivo 802.1x, Certificado de dispositivo HTTPS y Certificado de dispositivo IPSec, que se enumeran en la pestaña Básico de una configuración.
- Las opciones de cada una de estos ajustes se rellenan con los certificados seleccionados en la pestaña Certificado.
- Al clonar, exportar o importar una configuración, se borran los valores preseleccionados de estos ajustes. Debe seleccionar los valores manualmente.

Descripción de los ajustes de variables

La configuración de variables le permite administrar la configuración en toda su flota que es exclusiva de cada impresora, como el nombre del host o la etiqueta de activos. Al crear o editar una configuración, puede seleccionar un archivo CSV que asociar con la configuración.

Ejemplo de formato de CSV:

```
IP_ADDRESS,Contact_Name,Address,Disp_Info
1.2.3.4,John Doe,1600 Penn. Ave., Blue
4.3.2.1,Jane Doe,1601 Penn. Ave., Red
```

```
2.3.6.5,"Joe, Jane and Douglas",1601 Penn. Ave.,Yellow
2.3.6.7,"Joe, Jane and Douglas",1600 Penn. Ave.,He is 6’7” tall
```

En la fila de encabezado del archivo variable, la primera columna es un identificador token de impresora exclusivo. El token debe contener uno de los siguientes elementos:

- **HOSTNAME**
- **IP_ADDRESS**
- **SYSTEM_NAME**
- **SERIAL_NUMBER**

Cada una de las columnas en el encabezado del archivo variable es un token de sustitución definido por el usuario. Se debe hacer referencia a este token en la configuración utilizando el formato ${HEADER}. Se sustituye por los valores de las filas posteriores cuando se aplica la configuración. Asegúrese de que los tokens no contienen ningún espacio.

Puede importar el archivo CSV que contiene los ajustes de variables al crear o editar una configuración. Para obtener más información, consulte “Creación de una configuración” en la página 69.

Configuración de los permisos de impresión en color

MVE le permite restringir la impresión en color para ordenadores host y usuarios específicos.

Nota: Este ajuste solo está disponible en las configuraciones de las impresoras en color compatibles.

1. En el menú Configuraciones, haga clic en **Todas las configuraciones**.
2. Cree o edite una configuración.
3. En la pestaña Permisos de impresión en color, realice una de las siguientes acciones:

Configurar los permisos de impresión en color para los ordenadores host

a. En el menú Ver, seleccione **Ordenadores host** y, a continuación, seleccione **Incluir permisos de impresión en color para ordenadores host**.
b. Haga clic en **Agregar** y, a continuación, escriba el nombre del ordenador host.
c. Para permitir que el ordenador host imprima en color, seleccione **Permitir impresión en color**.
d. Para permitir imprimir en color a los usuarios que inician sesión en el ordenador host, seleccione **Anular el permiso del usuario**.
e. Haga clic en **Guardar y agregar** o **Guardar**.

Configurar los permisos de impresión en color para los usuarios

a. En el menú Ver, seleccione **Usuarios** y, a continuación, seleccione **Incluir permisos de impresión en color para usuarios**.
b. Haga clic en **Agregar** y, a continuación, escriba el nombre del usuario.
c. Seleccione **Permitir impresión en color**.
d. Haga clic en **Guardar y agregar** o **Guardar**.

Creación de un paquete de aplicaciones

1. Exporte la vista de la lista de impresoras desde MVE mediante la función Exportar datos.
   a. En el menú Impresoras , haga clic en **Vistas**.
   b. Seleccione **Lista de impresoras** y, a continuación, haga clic en **Exportar datos**.
   c. Seleccione una búsqueda guardada.
   d. En el menú "Seleccione el tipo de archivo para la exportación de datos.", seleccione **CSV**.
   e. Haga clic en **Exportar datos**.
2. Acceda al generador de paquetes.

   Nota: Si necesita acceder al generador de paquetes, póngase en contacto con su representante de Lexmark.

   a. Inicie sesión en el Generador de paquetes en **cdp.lexmark.com/package-builder**.
   b. Importe la lista de impresoras y haga clic en **Siguiente**.
   c. Introduzca la descripción del paquete y su dirección de correo electrónico.
   d. En el menú Producto , seleccione las aplicaciones y, si fuera necesario, añada licencias.
   e. Haga clic en **Siguiente** > **Finalizar**. El enlace de descarga del paquete se enviará a su dirección de correo electrónico.
3. Descargar el paquete.

Notas:

- MVE no admite la implementación de aplicaciones con licencias de prueba. Solo puede implementar aplicaciones gratuitas o aplicaciones con licencias de producción. Si necesita códigos de activación, póngase en contacto con su representante de Lexmark.
- Para agregar las aplicaciones a una configuración, importe el paquete de aplicaciones a la biblioteca de recursos. Para obtener más información, consulte “Importación de archivos a la biblioteca de recursos” en la página 76.

Importación o exportación de una configuración

Antes de comenzar, al importar un archivo de configuración, asegúrese de que se ha exportado desde un MVE de la misma versión.

1. En el menú Configuraciones, haga clic en **Todas las configuraciones**.
2. Para ello, realice una de las siguientes acciones:
   - Para importar un archivo de configuración, haga clic en **Importar**, desplácese hasta el archivo de configuración y, a continuación, haga clic en **Importar**.
   - Para exportar un archivo de configuración, seleccione una configuración y, a continuación, haga clic en **Exportar**.

   Notas:

   – Al exportar una configuración, las contraseñas no se incluyen. Después de la importación, añada manualmente las contraseñas.

- Los UCF, paquetes de configuración y archivos de aplicación no forman parte de una configuración exportada.

Importación de archivos a la biblioteca de recursos

La biblioteca de recursos es una colección de archivos de firmware, certificados de CA y paquetes de aplicaciones que se importan a MVE. Estos archivos pueden asociarse con una o más configuraciones.

1. En el menú Configuraciones, haga clic en **Biblioteca de recursos**.
2. Haga clic en **Importar** > **Elegir archivo** y, a continuación, busque el archivo.

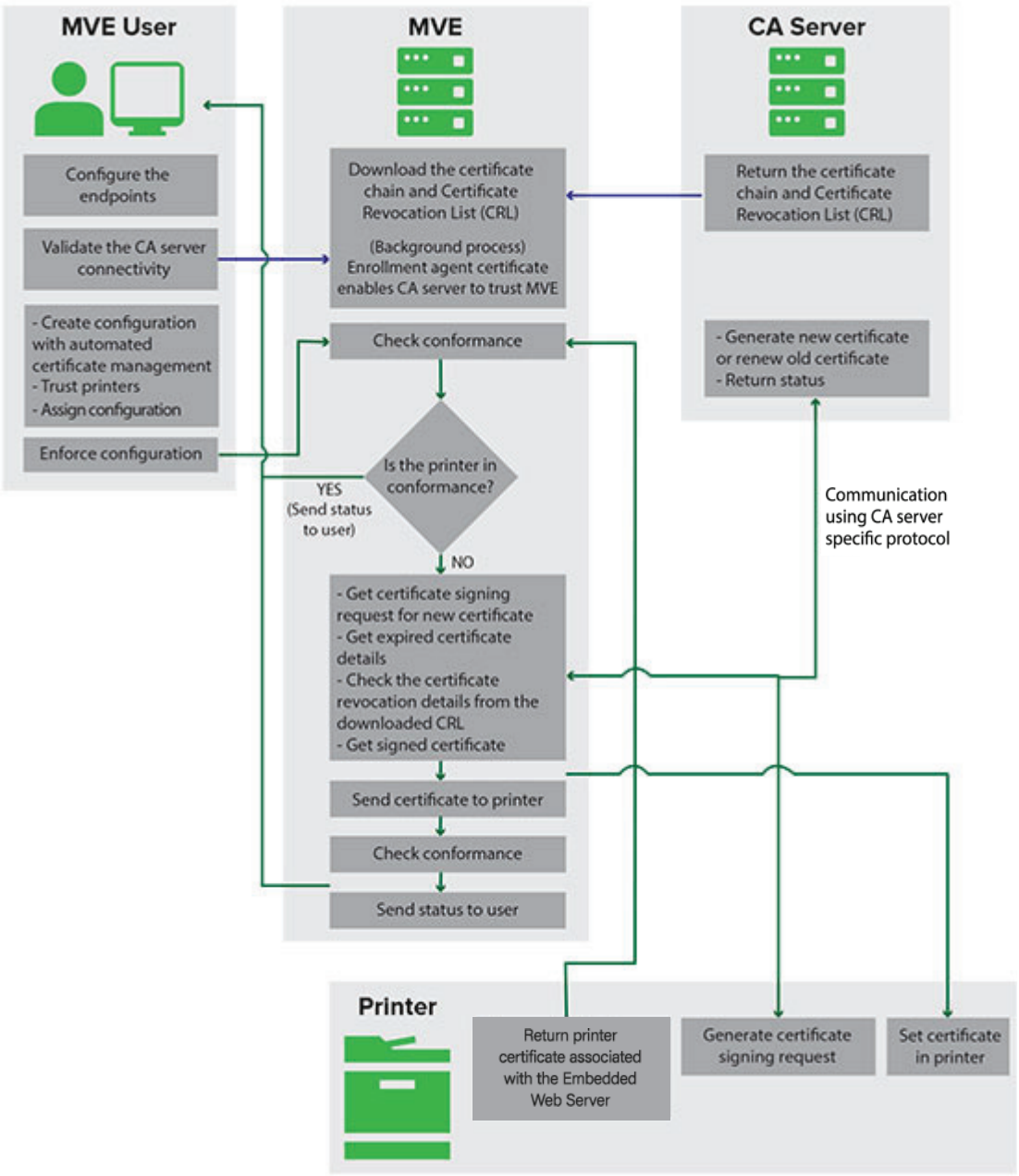
   Nota: Solo se pueden importar archivos de firmware (.fls), archivos de aplicaciones (.fls), paquetes de aplicaciones o paquetes de configuración (.zip), certificados de CA (.pem) y archivos de configuración universal (.ucf).
3. Haga clic en **Importar recurso**.

Administración de certificados

Configuración de MVE para gestionar certificados de forma automática

Descripción de la función de administración automática de certificados

Puede configurar MVE para gestionar certificados de impresora de forma automática y, a continuación, instalarlos en las impresoras mediante la aplicación de la configuración. El siguiente diagrama describe el proceso completo de la función de administración automática de certificados.



Los puntos finales de la autoridad de certificación, como el servidor de la CA y la dirección del servidor, deben establecerse en MVE.

Los servidores de la CA siguientes son compatibles:

- **CA de OpenXPKI**: los usuarios pueden utilizar cualquiera de los siguientes protocolos:
  - Protocolo de cifrado de certificados seguro (SCEP)
  - Conector de EST

  Notas:

  - EST es la forma recomendada de conectarse al servidor de OpenXPKI.
  - Para obtener más información sobre la configuración de la CA de OpenXPKI mediante el protocolo EST, consulte "Administración de certificados mediante la autoridad certificadora de OpenXPKI a través de EST" en la página 119
  - Para obtener más información sobre la configuración de la CA de OpenXPKI mediante el protocolo SCEP, consulte "Administración de certificados mediante la autoridad certificadora de OpenXPKI a través de SCEP" en la página 101
- **CA de Microsoft Enterprise**: los usuarios pueden utilizar cualquiera de los siguientes protocolos
  - Protocolo de cifrado de certificados seguro (SCEP)
  - Servicios web de inscripción de certificados de Microsoft (MSEWS)

  Notas:

  - MSCEWS es la forma recomendada de conectarse al servidor de la CA de Microsoft Enterprise.
  - Para obtener más información sobre la configuración de la CA de Microsoft mediante el protocolo MSCEWS, consulte "Administración de certificados mediante la autoridad certificadora de Microsoft a través de MSCEWS" en la página 90
  - Para obtener más información sobre la configuración de la CA de Microsoft mediante el protocolo SCEP, consulte "Administración de certificados mediante la autoridad certificadora de Microsoft a través de SCEP" en la página 82

Debe validarse la conexión entre MVE y los servidores de la CA. Durante la validación, MVE se comunica con el servidor de la CA para descargar la cadena de certificados y la lista de revocación de certificados (CRL). También se genera el certificado de agente de inscripción o el certificado de prueba. Este certificado permite al servidor de la CA confiar en MVE.

Para obtener más información sobre la definición de los puntos finales y su validación, consulte "Configuración de MVE para la administración automática de certificados" en la página 79.

Una configuración establecida en **Utilizar Markvision para gestionar los certificados de dispositivo** debe asignarse y aplicarse en la impresora.

Para obtener más información, consulte los siguientes temas:

- "Creación de una configuración" en la página 69
- "Aplicación de configuraciones" en la página 62

Durante la aplicación, MVE comprueba la conformidad de la impresora.

Para el **certificado de dispositivo predeterminado**

- El certificado se valida con respecto a la cadena de certificados descargada del servidor de la CA.
- Si la impresora no cumple los requisitos, se pide una solicitud de firma de certificado (CSR) para dicha impresora.

Para el **certificado de dispositivo con nombre**

- El certificado se valida con respecto a la cadena de certificados descargada del servidor de la CA.
- MVE crea un certificado de dispositivo con nombre firmado automáticamente en el dispositivo.
- Si la impresora no cumple los requisitos, se pide una CSR para dicha impresora.

Notas:

- MVE se comunica con el servidor de la CA mediante los protocolos compatibles.
- El servidor de la CA genera el nuevo certificado y, a continuación, MVE envía el certificado a la impresora.
- Si existe un certificado con nombre en la impresora, no se crea un nuevo certificado con nombre, sino que se genera una CSR para la impresora.

Configuración de MVE para la administración automática de certificados

1. Haga clic en , en la esquina superior derecha de la página.
2. Haga clic en **Autoridad de certificación** > **Utilizar el servidor de la autoridad de certificación**.

   Nota: El botón Utilizar el servidor de la autoridad de certificación solo aparecerá cuando configure la autoridad de certificación por primera vez o cuando elimine el certificado.
3. Configure los puntos finales del servidor.
   - **Servidor de la CA**: es el servidor de la autoridad de certificación (CA) que genera los certificados de la impresora. Seleccione una de las siguientes opciones:
     - **CA de OpenXPKI**
     - **CA de Microsoft Enterprise**

     Nota: El usuario también puede configurar un servidor de la CA compatible con el protocolo **Enrollment over Secure Transport (EST)**.

     - El servidor de la CA debe implementar el protocolo EST tal como se define en RFC 7030.

       Nota: Cualquier desviación de la especificación puede dar lugar a una configuración no válida.
     - EST es el protocolo recomendado para conectarse al servidor de la CA de OpenXPKI.

       Nota: El servidor de Microsoft Enterprise no es compatible con el protocolo EST.
   - **Dirección del servidor de la CA**: es la dirección IP o el nombre de host del servidor de la CA. Este campo solo se aplica a los protocolos SCEP y EST.

     Nota: Introduzca una de las siguientes opciones:

     - Para el servidor MSCA (mediante SCEP): <dirección IP del servidor o nombre de host>/certsrv/mssep/mssep.dll
     - Para el servidor OpenXPKI (mediante SCEP): <dirección IP del servidor o nombre de host>/scep/scep
     - Para EST, escriba cualquiera de las siguientes opciones:
       - https://172.87.95.240
       - https://estserver.com
       - estserver.com
   - **Etiqueta de servidor de la CA (opcional)**: si el usuario crea un nuevo dominio, se debe usar el mismo nombre de dominio en este campo.

- **Dirección del servidor del CEP**: este campo solo se aplica al protocolo MSCEWS.

  Nota: Introduzca una de las siguientes opciones:

  - Autenticación de nombre de usuario y contraseña:
    https://democep.com/ADPolicyProvider_CEP_UsernamePassword/service.svc/CEP
  - Para autenticación integrada de Windows:
    https://democep.com/ADPolicyProvider_CEP_Kerberos/service.svc/CEP
  - Para autenticación de certificado de cliente:
    https://democep.com/ADPolicyProvider_CEP_Certificate/service.svc/CEP
- **Nombre de host del servidor de la CA**: es el nombre de host del servidor de la CA.

  Nota: Por ejemplo, para el protocolo MSCEWS, el usuario puede seleccionar **`democa.lexmark.com`**
- **Nombre de host del servidor del CES**: es la dirección IP o el nombre de host del servidor del CES.

  Nota: Por ejemplo, para el protocolo MSCEWS, el usuario puede seleccionar **`democes.lexmark.com`**
- **Contraseña de comprobación**: es la contraseña necesaria para confirmar la identidad de MVE en el servidor de la CA. Esta contraseña sólo es necesaria para la CA OpenXPKI. No es compatible con la CA de Microsoft Enterprise.

Nota: En función del servidor de la CA, debe configurar el modo de autenticación del servidor. Para ello, realice una de las siguientes acciones:

- Si selecciona el protocolo **EST**, en el menú **Modo de autenticación del servidor de la CA**, seleccione una de las siguientes opciones:
  - **Autenticación de nombre de usuario y contraseña**
  - **Autenticación de certificado de cliente**
- Si selecciona el protocolo **MSCEWS**, en el menú **Modo de autenticación del servidor de la CA**, seleccione una de las siguientes opciones:
  - **Autenticación de nombre de usuario y contraseña**
  - **Autenticación de certificado de cliente**
  - **Autenticación integrada de Windows**
- El protocolo **SCEP** solo admite el modo de autenticación **Contraseña de comprobación**.

Nota: Dependiendo del servidor de la CA, consulte cualquiera de las secciones:

- "Administración de certificados mediante la autoridad certificadora de OpenXPKI a través de SCEP" en la página 101
- "Administración de certificados mediante la autoridad certificadora de Microsoft a través de SCEP" en la página 82
- "Administración de certificados mediante la autoridad certificadora de Microsoft a través de MSCEWS" en la página 90
- "Administración de certificados mediante la autoridad certificadora de OpenXPKI a través de EST" en la página 119

4 Haga clic en **Guardar cambios y validar** > **Aceptar**.

Notas:

- La opción **Descartar cambios** solo funciona si los cambios aún no se han guardado o se han guardado y validado.

- El usuario no puede recuperar datos de una configuración no válida porque MVE no almacena el último estado válido de ninguna configuración. MVE solo almacena una configuración de certificado individual a la vez, que puede ser o no válida.

Notas:

- Debe validarse la conexión entre MVE y los servidores de la CA. Durante la validación, MVE se comunica con el servidor de la CA para descargar la cadena de certificados y la lista de revocación de certificados (CRL). También se genera el certificado de agente de inscripción o el certificado de prueba. Este certificado permite al servidor de la CA confiar en MVE.
- Puede seleccionar una o varias plantillas CEP cuando utilice el protocolo MSCEWS. Haga lo siguiente:

a Después de hacer clic en **Guardar cambios y validar**, aparece la ventana Selección de plantilla CEP.

b Seleccione una o más de las plantillas disponibles.

- El cuadro de diálogo Utilizar el servidor de la autoridad certificadora recupera la lista de revocaciones de certificados.
- Un cuadro de diálogo confirma que la validación del certificado se ha realizado correctamente.

c Puede ver las plantillas del CEP seleccionadas en la página de configuración del servidor de la CA.

Nota: Cuando aplica esta configuración a cualquier dispositivo, se crea un certificado según la plantilla seleccionada.

5 Vuelva a la página Configuración del sistema y, a continuación, revise el certificado CA.

Nota: También puede descargar o eliminar el certificado CA.

Configuración de la CA de Microsoft Enterprise con NDES

Descripción general

En el siguiente escenario de implementación, todos los permisos se basan en los permisos definidos en las plantillas de certificado publicadas en el controlador de dominio. Las solicitudes de certificado enviadas a la CA se basan en las plantillas de certificado.

Para esta configuración, asegúrese de que dispone de lo siguiente:

- Un equipo que aloja la CA subordinada
- Un equipo que aloja el servicio NDES
- Un controlador de dominio

Usuarios necesarios

Cree los siguientes usuarios en el controlador de dominio:

- Administrador del servicio
  - Denominado **SCEPAdmin**
  - Debe ser miembro de los grupos **local admin** y **Enterprise Admin**
  - Debe estar registrado localmente cuando se active la instalación de la función NDES
  - Dispone de **permiso de inscripción** para las plantillas de certificado
  - Dispone de **permiso para agregar plantillas** en la CA

- Cuenta de servicio
  - Denominada **SCEPSvc**
  - Debe ser miembro del grupo **IIS_IUSRS** local
  - Debe ser un usuario de dominio y disponer de los permisos de **escritura** e **inscripción** en las plantillas configuradas
  - Dispone de permiso de **solicitud** en la CA
- Administrador de CA de Enterprise
  - Denominado **CAAdmin**
  - Miembro del grupo **Administrador de Enterprise**
  - Debe formar parte del grupo **administrador local**

Administración de certificados mediante la autoridad certificadora de Microsoft a través de SCEP

Esta sección contiene instrucciones sobre lo siguiente:

- Configuración de la autoridad certificadora (CA) de Microsoft Enterprise mediante el servicio de inscripción de dispositivos de red (NDES) de Microsoft
- Creación de un servidor de CA raíz

Nota: Para todas las configuraciones de este documento se utiliza el sistema operativo Windows Server 2016.

Descripción general

El servidor de la CA raíz es el servidor de la CA principal de cualquier organización y el principal de la infraestructura PKI. La CA raíz autentica el servidor de la CA subordinada. Este servidor se mantiene generalmente en modo sin conexión para evitar cualquier intrusión y para proteger la clave privada.

Para configurar el servidor de la CA raíz, haga lo siguiente:

1. Asegúrese de que el servidor de la CA raíz está instalado. Para obtener más información, consulte “Instalación del servidor de la CA raíz” en la página 82.
2. Configure los ajustes de punto de distribución de certificación y acceso a la información de entidad. Para obtener más información, consulte “Configuración de los ajustes de punto de distribución de certificación y acceso a la información de entidad” en la página 85.
3. Configure la accesibilidad de la CRL. Para obtener más información, consulte “Configuración de la accesibilidad de la CRL” en la página 86.

Instalación del servidor de la CA raíz

1. En Server Manager, haga clic en **Administrar** > **Agregar roles y características**.
2. Haga clic en **Funciones de servidor**, seleccione **Servicios de certificados de Active Directory** y todas sus características y, a continuación, haga clic en **Siguiente**.
3. En la sección Servicios de función AD CS, seleccione **Entidad de certificación** y, a continuación, haga clic en **Siguiente** > **Instalar**.

4. Después de la instalación, haga clic en **Configurar Servicios de Certificate Server de Active Directory en el servidor de destino**.
5. En la sección Servicios de función, seleccione **Entidad de certificación** > **Siguiente**.
6. En la sección Tipo de configuración, seleccione **CA independiente** y, a continuación, haga clic en **Siguiente**.
7. En la sección Tipo de CA, seleccione **CA raíz** y, a continuación, haga clic en **Siguiente**.
8. Seleccione **Crear una nueva clave privada** y, a continuación, haga clic en **Siguiente**.
9. En el menú Seleccione un proveedor de criptografía, seleccione **RSA#Microsoft Software Key Storage Provider**.
10. En el menú Longitud de la clave, seleccione **4096**.
11. En la lista de algoritmos hash, seleccione **SHA512** y, a continuación, haga clic en **Siguiente**.
12. En el campo Nombre común de esta CA, escriba el nombre del servidor host.
13. En el campo Sufijo de nombre distinguido, escriba el componente de dominio.

    Ejemplo de configuración de nombre de CA

    Nombre de dominio completamente cualificado (FQDN) del equipo: **`test.dev.lexmark.com`**

    Nombre común (CN): **`TEST`**

    Sufijo de nombre distinguido: **`DC=DEV,DC=LEXMARK,DC=COM`**
14. Haga clic en **Siguiente**.
15. Especifique el período de validez y, a continuación, haga clic en **Siguiente**.

    Nota: Normalmente, el período de validez es de 10 años.
16. No cambie nada en la ventana de ubicaciones de la base de datos.
17. Complete la instalación.

Configuración de la CA de Microsoft Enterprise con NDES

Descripción general

En el siguiente escenario de implementación, todos los permisos se basan en los permisos definidos en las plantillas de certificado publicadas en el controlador de dominio. Las solicitudes de certificado enviadas a la CA se basan en las plantillas de certificado.

Para esta configuración, asegúrese de que dispone de lo siguiente:

- Un equipo que aloja la CA subordinada
- Un equipo que aloja el servicio NDES
- Un controlador de dominio

Usuarios necesarios

Cree los siguientes usuarios en el controlador de dominio:

- Administrador del servicio
  - Denominado **SCEPAdmin**
  - Debe ser miembro de los grupos **local admin** y **Enterprise Admin**
  - Debe estar registrado localmente cuando se active la instalación de la función NDES
  - Dispone de **permiso de inscripción** para las plantillas de certificado
  - Dispone de **permiso para agregar plantillas** en la CA
- Cuenta de servicio
  - Denominada **SCEPSvc**
  - Debe ser miembro del grupo **IIS_IUSRS** local
  - Debe ser un usuario de dominio y disponer de los permisos de **escritura** e **inscripción** en las plantillas configuradas
  - Dispone de permiso de **solicitud** en la CA

Configuración del servidor de la CA subordinada

Descripción general

El servidor de la CA subordinada es el servidor de la CA intermedia y siempre está en línea. Generalmente se ocupa de la administración de certificados.

Para configurar el servidor de la CA subordinada, haga lo siguiente:

1. Asegúrese de que el servidor de la CA subordinada está instalado. Para obtener más información, consulte "Instalación del servidor de la CA subordinada" en la página 84.
2. Configure los ajustes de punto de distribución de certificación y acceso a la información de entidad. Para obtener más información, consulte "Configuración de los ajustes de punto de distribución de certificación y acceso a la información de entidad" en la página 85.
3. Configure la accesibilidad de la CRL. Para obtener más información, consulte "Configuración de la accesibilidad de la CRL" en la página 86.

Instalación del servidor de la CA subordinada

1. En el servidor, inicie sesión como un usuario de dominio **CAAdmin**.
2. En Server Manager, haga clic en **Administrar > Agregar roles y características**.
3. Haga clic en **Funciones de servidor**, seleccione **Servicios de certificados de Active Directory** y todas sus características y, a continuación, haga clic en **Siguiente**.
4. En la sección Servicios de función AD CS, seleccione **Entidad de certificación** e **Inscripción en línea de la entidad de certificación** y, a continuación, haga clic en **Siguiente**.

   Nota: Asegúrese de que se han agregado todas las funciones de Inscripción en línea de la entidad de certificación.
5. En la sección Función de servidor web (IIS) Servicios de función, conserve la configuración predeterminada.

6. Después de la instalación, haga clic en **Configurar Servicios de Certificate Server de Active Directory en el servidor de destino**.
7. En la sección Servicios de función, seleccione **Entidad de certificación** e **Inscripción en línea de la entidad de certificación** y, a continuación, haga clic en **Siguiente**.
8. En la sección Tipo de configuración, seleccione **CA empresarial** y, a continuación, haga clic en **Siguiente**.
9. En la sección Tipo de CA, seleccione **CA subordinada** y, a continuación, haga clic en **Siguiente**.
10. Seleccione **Crear una nueva clave privada** y, a continuación, haga clic en **Siguiente**.
11. En el menú Seleccione un proveedor de criptografía, seleccione **RSA#Microsoft Software Key Storage Provider**.
12. En el menú Longitud de la clave, seleccione **4096**.
13. En la lista de algoritmos hash, seleccione **SHA512** y, a continuación, haga clic en **Siguiente**.
14. En el campo Nombre común de esta CA, escriba el nombre del servidor host.
15. En el campo Sufijo de nombre distinguido, escriba el componente de dominio.

    Ejemplo de configuración de nombre de CA

    Nombre de dominio completamente cualificado (FQDN) del equipo: **`test.dev.lexmark.com`**

    Nombre común (CN): **`TEST`**

    Sufijo de nombre distinguido: **`DC=DEV,DC=LEXMARK,DC=COM`**
16. En el cuadro de diálogo Solicitud de certificado, guarde el archivo de solicitud y, a continuación, haga clic en **Siguiente**.
17. No cambie nada en la ventana de ubicaciones de la base de datos.
18. Complete la instalación.
19. Firme la solicitud de CA de la CA raíz y, a continuación, exporte el certificado firmado con el formato PKCS7.
20. En la CA subordinada, abra **Entidad de certificación**.
21. En el panel de la izquierda, haga clic con el botón derecho del ratón en la CA y, a continuación, haga clic en **Todas las tareas > Instalar certificado de CA**.
22. Seleccione el certificado firmado y, a continuación, inicie el servicio CA.

Configuración de los ajustes de punto de distribución de certificación y acceso a la información de entidad

Nota: Configure los ajustes de punto de distribución de certificación (CDP) y acceso a la información de entidad (AIA) de la lista de revocación de certificados (CRL).

1. En Server Manager, haga clic en **Herramientas > Entidad de certificación**.
2. En el panel de la izquierda, haga clic con el botón derecho del ratón en la CA y, a continuación, haga clic en **Propiedades > Extensiones**.
3. En el menú Seleccionar extensión, seleccione **Puntos de distribución de lista de revocación de certificados (CDP)**.

4. En la lista de revocación de certificados, seleccione la entrada **C:\Windows\system32** y, a continuación, realice lo siguiente:
   a. Seleccione **Publicar las listas de revocación de certificados (CRL) en esta ubicación**.
   b. Desactive **Publicar CRL incrementales en esta ubicación**.
5. Elimine todas las demás entradas excepto **C:\Windows\system32**.
6. Haga clic en **Agregar**.
7. En el campo Ubicación, agregue **`http://serverIP/CertEnroll/<CAName><CRLNameSuffix><DeltaCRLAllowed>.crl`**, donde ***serverIP*** es la dirección IP del servidor.

   Nota: Si puede acceder al servidor mediante FQDN, utilice **<ServerDNSName>** en lugar de la dirección IP del servidor.
8. Haga clic en **Aceptar**.
9. Seleccione **Incluir en la extensión CDP de los certificados emitidos** para la entrada creada.
10. En el menú Seleccionar extensión, seleccione **Acceso a la información de entidad (AIA)**.
11. Elimine todas las demás entradas excepto **C:\Windows\system32**.
12. Haga clic en **Agregar**.
13. En el campo Ubicación, agregue **`http://ServerIP/CertEnroll/<ServerDNSName>_<CAName><CertificateName>.crt`**, donde ***ServerIP*** es la dirección IP del servidor.

    Nota: Si puede acceder al servidor mediante FQDN, utilice **<ServerDNSName>** en lugar de la dirección IP del servidor.
14. Haga clic en **Aceptar**.
15. Seleccione **Incluir en la extensión AIA de los certificados emitidos** para la entrada creada.
16. Haga clic en **Aplicar** > **Aceptar**.

    Nota: Si es necesario, reinicie el servicio de certificación.
17. En el panel de la izquierda, expanda la CA, haga clic con el botón derecho del ratón en **Certificados revocados** y, a continuación, haga clic en **Propiedades**.
18. Especifique el valor de Intervalo de publicación de CRL y de Publicar Delta Intervalo de publicación de CRL y, a continuación, haga clic en **Aplicar > Aceptar**.
19. En el panel de la izquierda, haga clic con el botón derecho del ratón en **Certificados revocados**, haga clic en **Todas las tareas** y, a continuación, publique la CRL Nuevo.

Configuración de la accesibilidad de la CRL

Nota: Antes de comenzar, asegúrese de que está instalado el Administrador de Internet Information Services (IIS).

1. En el Administrador de IIS, expanda la CA y, a continuación, expanda **Sitios**.
2. Haga clic con el botón derecho del ratón en **Sitio web predeterminado** y, a continuación, haga clic en **Agregar directorio virtual**.

3 En el campo Alias, escriba **CertEnroll**.

4 En el campo Ruta física, escriba **C:\Windows\System32\CertSrv\CertEnroll**.

5 Haga clic en **Aceptar**.

6 Haga clic con el botón derecho del ratón en **CertEnroll** y, a continuación, haga clic en **Editar permisos**.

7 En la pestaña Seguridad, elimine todos los accesos de escritura excepto para el sistema.

8 Haga clic en **Aceptar**.

Configuración del servidor NDES

1 En el servidor, inicie sesión como un usuario de dominio **SCEPAdmin**.

2 En Server Manager, haga clic en **Administrar** > **Agregar roles y características**.

3 Haga clic en **Funciones de servidor**, seleccione **Servicios de certificados de Active Directory** y todas sus características y, a continuación, haga clic en **Siguiente**.

4 En la sección Servicios de función AD CS, desactive **Entidad de certificación**.

5 Seleccione **Servicio de inscripción de dispositivos de red** y todas sus características y, a continuación, haga clic **Siguiente**.

6 En la sección Función de servidor web (IIS) Servicios de función, conserve la configuración predeterminada.

7 Después de la instalación, haga clic en **Configurar Servicios de Certificate Server de Active Directory en el servidor de destino**.

8 En la sección Servicios de función, seleccione **Servicio de inscripción de dispositivos de red** y, a continuación, haga clic en **Siguiente**.

9 Seleccione la cuenta de servicio **SCEPSvc**.

10 En la sección CA para NDES, seleccione **Nombre de CA** o **Nombre de equipo** y, a continuación, haga clic en **Siguiente**.

11 En la sección Información de RA, especifique la información y, a continuación, haga clic en **Siguiente**.

12 En la sección Criptografía para NDES, haga lo siguiente:
- Seleccione los proveedores de firma y clave de cifrado adecuados.
- En el menú Longitud de la clave, seleccione la misma longitud de clave que el servidor de la CA.

13 Haga clic en **Siguiente**.

14 Complete la instalación.

Ahora puede acceder al servidor NDES desde un navegador web como un usuario SCEPSvc. En el servidor NDES, puede ver la huella digital del certificado de CA, la contraseña de comprobación de inscripción y el período de validez de la contraseña de comprobación.

Acceso al servidor NDES

Abra un navegador web y, a continuación, escriba **http://*NDESserverIP*/certsrv/mscep_admin**, donde ***NDESserverIP*** es la dirección IP del servidor NDES.

Configuración de NDES para MVE

Nota: Antes de comenzar, asegúrese de que el servidor NDES funcione correctamente.

Creación de una plantilla de certificado

1. En la CA subordinada (certserv), abra **Entidad de certificación**.
2. En el panel de la izquierda, expanda la CA, haga clic con el botón derecho del ratón en **Plantillas de certificado** y, a continuación, haga clic en **Administrar**.
3. En Consola de plantillas de certificados, cree una copia de **Servidor web**.
4. En la pestaña General, escriba **`MVEWebServer`** como nombre de plantilla.
5. En la pestaña Seguridad, otorgue a los usuarios **SCEPAdmin** y **SCEPSvc** los permisos adecuados.

   Nota: Para obtener más información, consulte “Usuarios necesarios” en la página 84.
6. En la pestaña Nombre del sujeto, seleccione **Proporcionar en la solicitud**.
7. En la CA subordinada (certserv), abra **Entidad de certificación**.
8. En la pestaña Extensiones, seleccione **Directivas de aplicación > Editar**.
9. Haga clic en **Agregar >Autenticación del cliente > Aceptar**.
10. En el panel de la izquierda, expanda la CA, haga clic con el botón derecho del ratón en **Plantillas de certificado** y, a continuación, haga clic en **Nueva > Plantilla de certificado que se va a emitir**.
11. Seleccione los certificados que acaba de crear y, a continuación, haga clic en **Aceptar**.

Ahora puede acceder a las plantillas mediante el portal web de inscripción de la CA.

Acceso a las plantillas

1. Abra un navegador web y, a continuación, escriba **`http://CAserverIP/certsrv/certrqxt.asp`**, donde ***`CAserverIP`*** es la dirección IP del servidor de la CA.
2. En el menú Plantilla de certificado, vea las plantillas.

Definición de plantillas de certificado para NDES

1. En el ordenador, inicie el editor del registro.
2. Desplácese a **>SOFTWARE HKEY_LOCAL_MACHINE >Microsoft > Cryptography > MSCEP**.
3. Configure lo siguiente y, a continuación, defínalos en **MVEWebServer**:
   - EncryptionTemplate
   - GeneralPurposeTemplate
   - SignatureTemplate
4. Otorgue al usuario de SCEPSvc permiso completo para MSCEP.
5. En el Administrador de IIS, expanda la CA y, a continuación, haga clic en **Grupos de aplicaciones**.
6. En el panel de la derecha, haga clic en **Reciclar** para reiniciar el grupo de aplicaciones SCEP.

7 En el Administrador de IIS, expanda la CA y, a continuación, expanda **Sitios** > **Sitio web predeterminado**.

8 En el panel de la derecha, haga clic en **Reiniciar**.

Desactivación de la Contraseña de comprobación en el servidor de la CA de Microsoft

1 En el ordenador, inicie el editor del registro.

2 Desplácese a **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Microsoft** > **Cryptography** > **MSCEP**.

3 Defina Aplicar contraseña en **0**.

4 En el Administrador de IIS, expanda la CA, haga clic en **Grupos de aplicaciones** y, a continuación, seleccione **SCEP**.

5 En el panel de la derecha, haga clic en **Configuración avanzada**.

6 Defina Cargar perfil de usuario en **Verdadero** y, a continuación, haga clic en **Aceptar**.

7 En el panel de la derecha, haga clic en **Reciclar** para reiniciar el grupo de aplicaciones SCEP.

8 En el Administrador de IIS, expanda la CA y, a continuación, expanda **Sitios** > **Sitio web predeterminado**.

9 En el panel de la derecha, haga clic en **Reiniciar**.

Al abrir NDES desde el navegador web, ahora solo podrá ver la huella digital de la CA.

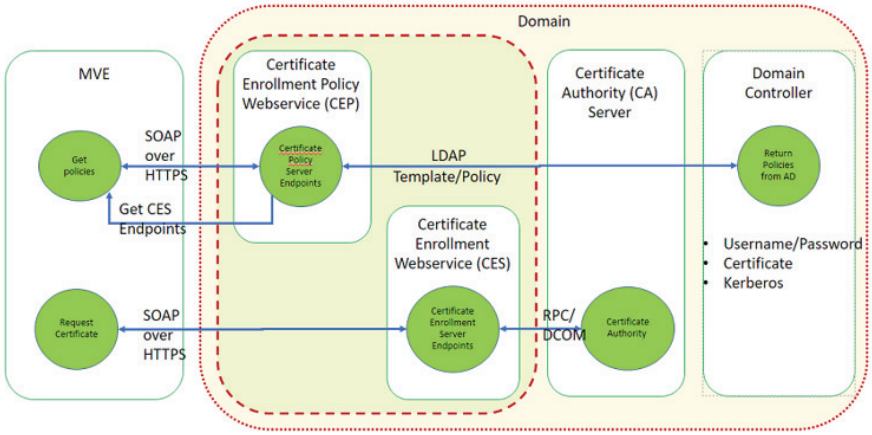
Administración de certificados mediante la autoridad certificadora de Microsoft a través de MSCEWS

En esta sección se proporciona información sobre la configuración del servicio web de la política de inscripción de certificados (CEP) y del servicio web de inscripción de certificados (CES). Puesto que Microsoft recomienda instalar CEP y CES en dos equipos diferentes, en este documento hacemos lo mismo. Nos referimos a estos servicios web como servidor CEP y servidor CES, respectivamente.

Nota: El usuario debe tener una autoridad certificadora (CA) de Enterprise preconfigurada y un controlador de dominio.

Requisitos del sistema

Para todas las configuraciones de este documento se utiliza el sistema operativo Windows Server 2012 R2. Los siguientes requisitos y capacidades de instalación se aplican tanto a CEP como a CES, a menos que se especifique lo contrario.



Cree los siguientes tipos de cuenta en el controlador de dominio:

- Administrador del servicio: Se denomina **CEPAdmin** y **CESAdmin**
  - Este usuario debe formar parte del **grupo administración local** en los respectivos servidores CEP y CES.
  - Este usuario debe formar parte del grupo **Administador de Enterprise**.
- Cuenta de servicio: Se denomina **CEPSvc** y **CESSvc**
  - Este usuario debe formar parte del grupo **IIS_IUSRS local**.
  - Requiere el permiso **Solicitar certificado** en la CA para los **CEPSvc** y **CESSvc** correspondientes.

Requisitos de conectividad de red

- Los requisitos de conectividad de la red son una parte clave de la planificación de la implementación, especialmente en los escenarios en los que CEP y CES se alojan en una red perimetral.
- Toda la conectividad del cliente a ambos servicios se produce dentro de una sesión HTTPS, por lo que sólo se permite el tráfico HTTPS entre el cliente y los servicios web.
- CEP se comunica con los Servicios de dominio de Active Directory (AD DS), utilizando los puertos estándar LDAP (Lightweight Directory Access Protocol) y LDAP (LDAPS) (TCP 389 y 636 respectivamente).
- CES se comunica con CA mediante el modelo de objetos componentes distribuidos (DCOM).

Notas:

- De forma predeterminada, DCOM utiliza puertos efímeros aleatorios.
- CA se puede configurar para reservar un rango específico de puertos para simplificar la configuración del firewall.

Creación de certificados SSL para servidores CEP y CES

CES y CEP deben utilizar Secure Sockets Layer (SSL) para la comunicación con los clientes (mediante HTTPS). Cada servicio debe tener un certificado válido que tenga una directiva de uso de clave mejorado (EKU) de autenticación de servidor en el almacén de certificados del equipo local.

1. Instale el servicio IIS en el servidor.
2. Inicie sesión en el servidor CEP y, a continuación, agregue el Certificado raíz (autoridad certificadora) en el almacén Autoridad certificadora raíz de confianza.
3. Inicie la Consola de IIS Manager y, a continuación, seleccione el **inicio del servidor**.
4. En la sección de vista principal, abra **Certificados de servidor**.
5. Haga clic en **Acciones** > **Crear solicitud de certificado**.
6. En la ventana Propiedades de nombre distinguido, proporcione la información necesaria y, a continuación, haga clic en **Siguiente**.
7. En el cuadro de diálogo Propiedades del proveedor de servicios criptográficos, seleccione la longitud de bit y, a continuación, haga clic en **Siguiente**.
8. Guarde el archivo.
9. Obtenga el archivo firmado por la CA que planea utilizar para CEP y CES.

   Nota: Asegúrese de que EKU de autenticación de servidor está activada en el certificado firmado.
10. Vuelva a copiar el archivo firmado en el servidor CEP.
11. En Consola de IIS Manager, seleccione el **inicio del servidor**.
12. En Vista principal, abra **Certificados de servidor**.
13. Haga clic en **Acciones** > **Completar solicitud de certificado**.
14. En la ventana Especificar respuesta de la autoridad certificadora, seleccione el archivo firmado.
15. Escriba un nombre y, a continuación, en el menú Almacén de certificados, seleccione **Personal**.
16. Complete la instalación del certificado.
17. En Consola del IIS Manager, seleccione el sitio web predeterminado.
18. Haga clic en **Acciones** > **Enlaces**.
19. En el cuadro de diálogo Enlaces de sitio, haga clic en **Agregar**.
20. En el cuadro de diálogo Agregar enlace de sitio, establezca Tipo en **https** y, a continuación, desde el certificado SSL, busque el certificado recién creado.
21. En Consola de IIS Manager, seleccione **Sitio web predeterminado** y, a continuación, abra la configuración de SSL.

22 Active Requerir SSL y establezca Certificado de cliente en **Ignorar**.

23 Reinicie IIS.

Nota: Siga el mismo proceso para el servidor CES.

Creación de plantillas de certificado

El usuario debe crear una plantilla de certificado para la inscripción de certificados. Haga lo siguiente para copiar desde una plantilla de certificado existente:

1 Inicie sesión en la CA de Enterprise con credenciales de administrador de CA.

2 Expanda la CA, haga clic con el botón derecho en **Plantillas de certificado** y, a continuación, haga clic en **Administrar**.

3 En la Consola de plantillas de certificados, haga clic con el botón derecho en **Plantilla de certificado de servidor web** y, a continuación, haga clic en **Duplicar plantilla**.

4 En la ficha General de la plantilla, asigne un nombre a la plantilla **MVEWebServer**.

5 En la ficha Seguridad, otorgue al administrador de CA permisos de **lectura**, **escritura** e **inscripción**.

6 Otorgue permisos de **lectura** e **inscripción** a los usuarios autenticados.

7 En la pestaña Nombre del sujeto, seleccione **Proporcionar** en la solicitud.

8 En la ficha General, establezca el período de validez del certificado.

9 Si piensa utilizar esta plantilla de certificado para emitir un **certificado 802.1X** para impresoras, haga lo siguiente:

   a En la ficha **Extensiones**, seleccione **Políticas de aplicación** en la lista de extensiones incluidas en esta plantilla.

   b Haga clic en **Editar** > **Agregar**.

   c En el cuadro de diálogo Agregar política de aplicación, seleccione **Autenticación de cliente**.

   d Haga clic en **Aceptar**.

10 En el cuadro de diálogo Propìedades de plantilla de certificado, haga clic en **Aceptar**.

11 En la ventana CA, haga clic con el botón derecho en **Plantillas de certificado** y, a continuación, haga clic en **Nuevo** > **Plantilla de certificado**.

12 Seleccione **MVEWebServer** y, a continuación, haga clic en **Aceptar**.

Descripción de los métodos de autenticación

CEP y CES admiten los siguientes métodos de autenticación:

- Autenticación integrada en Windows, también conocida como **autenticación Kerberos**
- Autenticación de certificado de cliente, también conocida como **Autenticación de certificado X.509**
- **Autenticación de nombre de usuario y contraseña**

autenticación integrada de Windows

La autenticación integrada en Windows utiliza Kerberos para proporcionar un flujo de autenticación ininterrumpido para los dispositivos conectados a la red interna. Este método es el preferido para las implementaciones internas porque utiliza la infraestructura Kerberos existente en AD DS. También requiere cambios mínimos en los equipos cliente de certificados.

Nota: Utilice este método de autenticación si necesita que los clientes accedan *sólo* al servicio web mientras está conectado directamente a la red interna.

Autentificación de certificado de cliente

Este método es preferible a la autenticación de nombre de usuario y contraseña porque es más seguro. No requiere una conexión directa a la red corporativa.

Notas:

- Utilice este método de autenticación si tiene previsto proporcionar a los clientes certificados X.509 digitales para la autenticación.
- Este método activa los servicios Web disponibles en Internet.

Información de nombre de usuario y contraseña.

El método de nombre de usuario y contraseña es la forma más sencilla de autenticación. Este método se utiliza normalmente para prestar servicio a clientes que no están conectados directamente a la red interna. Es una opción de autenticación menos segura que la autenticación de certificado de cliente, pero no requiere el aprovisionamiento de un certificado.

Nota: Utilice este método de autenticación cuando pueda acceder al servicio Web en la red interna o a través de Internet.

Requisitos de delegación

La delegación permite a un servicio suplantar a una cuenta de usuario o equipo para tener acceso a los recursos de toda la red.

Se requiere delegación para el servidor CES cuando se aplican todas las situaciones siguientes:

- CA y CES no residen en el mismo equipo.
- CES puede procesar las solicitudes de inscripción iniciales, en lugar de procesar únicamente las solicitudes de renovación de certificados.
- El tipo de autenticación se establece en **Autenticación integrada de Windows** o **Autenticación de certificado de cliente**.

No es necesaria la delegación para el servidor CES en los siguientes casos:

- CA y CES residen en el mismo equipo.
- El nombre de usuario y la contraseña son el método de autenticación.

Notas:

- Microsoft recomienda ejecutar CEP y CES como cuentas de usuario de dominio.
- Los usuarios deben crear un nombre principal de servicio (SPN) adecuado antes de configurar la delegación en la cuenta de usuario de dominio.

Activación de la delegación

1. Para crear un SPN para una cuenta de usuario de dominio, utilice el comando **setspn** de la siguiente manera:

   ```
   setspn -s http/ces.msca.com msca\CESSvc
   ```

   Notas:

   - El nombre de la cuenta es CESSvc.
   - CES se ejecuta en un equipo con un nombre de dominio (FQDN) de **ces.msca.com** en el dominio msca.com.

2. Abra la cuenta de usuario de dominio CESSvc en el controlador de dominio.
3. En la pestaña Delegación, seleccione **Confiar en este usuario para delegar solo a servicios especificados**.
4. Seleccione la delegación adecuada según el método de autenticación.

   Notas:

   - Si selecciona Autenticación integrada en Windows, configure la delegación para que utilice **sólo Kerberos**.
   - Si el servicio utiliza Autenticación de certificado de cliente, configure la delegación para que utilice cualquier protocolo de autenticación.
   - Si tiene previsto configurar varios métodos de autenticación, configure la delegación para utilizar cualquier protocolo de autenticación.

5. Haga clic en **Agregar**.
6. En el cuadro de diálogo Agregar servicios, seleccione **Usuarios** o **Equipos**.
7. Escriba el nombre de host del servidor de la CA y, a continuación, haga clic en **Comprobar nombres**.
8. En el cuadro de diálogo Agregar servicios, seleccione uno de los siguientes servicios para delegar:
   - Servicio host (HOST) para ese servidor de la CA
   - Servicio de sistema de llamada a procedimiento remoto (RPCSS) para ese servidor de la CA
9. Cierre el cuadro de diálogo de propiedades de usuario de dominio.

Para los usuarios del dominio CEP que utilizan la autenticación integrada en Windows, haga lo siguiente:

1. Para crear un SPN para una cuenta de usuario de dominio, utilice el comando **setspn** de la siguiente manera:

   ```
   setspn -s http/cep.msca.com msca\CEPSvc
   ```

   Nota: El nombre de la cuenta es CEPSvc.

2. Abra la cuenta de usuario de dominio CEPSvc en el controlador de dominio.
3. En la pestaña Delegación, seleccione **No confiar en este usuario para la delegación**.

Configuración de la autenticación integrada de Windows

Para instalar CEP y CES, utilice Windows PowerShell.

Configuración de CEP

El cmdlet **Install-AdcsEnrollmentPolicyWebService** configura el servicio web de inscripción de certificados (CEP). También se utiliza para crear otras instancias del servicio en de una instalación existente.

1. Inicie sesión en el servido CEP con el nombre de usuario CEPAdmin y, a continuación, inicie PowerShell en modo administrativo.
2. Ejecute el comando **`Import-Module ServerManager`**.
3. Ejecute el comando **`Add-WindowsFeature Adcs-Enroll-Web-Pol`**.
4. Ejecute el comando **`Install-AdcsEnrollmentPolicyWebService -AuthenticationType Kerberos -SSLCertThumbprint "sslCertThumbPrint"`**.

   Nota: Sustituya *<sslCertThumbPrint>* por la huella digital del certificado SSL creado para el servidor CEP, tras haber eliminado los espacios entre los valores de la huella digital.
5. Complete la instalación seleccionando **Y** o **A**.
6. Inicie la consola de IIS Manager.
7. En el panel Conexiones, expanda el servidor web que aloja CEP.
8. Expanda **Sitios**, **Sitio web predeterminado** y, a continuación, haga clic en el nombre de la aplicación virtual de instalación que corresponda **ADPolicyProvider_CEP_Kerberos**.
9. En la aplicación virtual denominada **Inicio**, haga doble clic en la configuración de la aplicación y, a continuación, haga doble clic en **FriendlyName**.
10. Escriba un nombre en Valor y cierre el cuadro de diálogo.
11. Haga doble clic en **URI** y, a continuación, copie **Valor**.

    Notas:

    - Si desea configurar otro método de autenticación en el mismo servidor CEP, debe cambiar el ID.
    - Esta URL se utiliza en MVE o en cualquier aplicación cliente.
12. En el panel izquierdo, haga clic en **Grupo de aplicaciones**.
13. Seleccione **WSEnrollmentPolicyServer** y, a continuación, en el panel derecho, haga clic en **Acciones** > **Configuración avanzada**.
14. Seleccione el campo de identidad de Modelo de proceso.
15. En el cuadro de diálogo Identidad del grupo de aplicaciones, seleccione la cuenta personalizada e introduzca **`CEPSvc`** como el nombre de usuario de dominio.
16. Cierre todos los cuadros de diálogo y actualice IIS desde el panel derecho de Consola de IIS Manager .
17. En PowerShell, escriba **`iisreset`** para reiniciar IIS.

Configuración de CES

El cmdlet **Install-AdcsEnrollmentWebService** configura el servicio web de inscripción de certificados (CES). También se utiliza para crear otras instancias del servicio en de una instalación existente.

1. Inicie sesión en el servidor CES con el nombre de usuario **`CESAdmin`** y, a continuación, inicie PowerShell en modo administrativo.
2. Ejecute el comando **`Import-Module ServerManager`**.
3. Ejecute el comando **`Add-WindowsFeature Adcs-Enroll-Web-Svc`**.
4. Ejecute el comando **`Install-AdcsEnrollmentWebService -ApplicationPoolIdentity -CAConfig "CA1.contoso.com\contoso-CA1-CA" -SSLCertThumbprint "sslCertThumbPrint" -AuthenticationType Kerberos`**.

   Notas:

   - Sustituya *<sslCertThumbPrint>* por la huella digital del certificado SSL creado para el servidor CES, tras haber eliminado los espacios entre los valores de la huella digital.
   - Sustituya **`CA1.contoso.com`** por el nombre del equipo de la CA.
   - Sustituya **`contoso-CA1-CA`** por el nombre común de la CA.
5. Complete la instalación seleccionando **Y** o **A**.
6. Inicie la consola de IIS Manager.
7. En el panel Conexiones, expanda el servidor web que aloja CES.
8. Expanda **Sitios**, **Sitio web predeterminado** y, a continuación, haga clic en el nombre de la aplicación virtual de instalación que corresponda: **contoso-CA1-CA _CES_Kerberos**.
9. En el panel izquierdo, haga clic en **Grupo de aplicaciones**.
10. Seleccione **WSEnrollmentServer** y, a continuación, en el panel derecho, haga clic en **Acciones** > **Configuración avanzada**.
11. Seleccione el campo de identidad de Modelo de proceso.
12. En el cuadro de diálogo **`Identidad del grupo de aplicaciones`**, seleccione la cuenta personalizada e introduzca **`CESSvc`** como el nombre de usuario de dominio.
13. Cierre todos los cuadros de diálogo y actualice IIS desde el panel derecho de Consola de IIS Manager.
14. En PowerShell, escriba **`iisreset`** para reiniciar IIS.
15. Para los usuarios de dominio CESSvc, active la delegación. Para obtener más información, consulte “Activación de la delegación” en la página 94.

Configuración de la autenticación del certificado de cliente

Configuración de CEP

El cmdlet **Install-AdcsEnrollmentPolicyWebService** configura CEP. También se utiliza para crear otras instancias del servicio en de una instalación existente.

1. Inicie sesión en el servido CEP con el nombre de usuario CEPAdmin y, a continuación, inicie PowerShell en modo administrativo.
2. Ejecute el comando **`Import-Module ServerManager`**.
3. Ejecute el comando **`Add-WindowsFeature Adcs-Enroll-Web-Pol`**.
4. Ejecute el comando **`Install-AdcsEnrollmentPolicyWebService -AuthenticationType Certificate -SSLCertThumbprint "sslCertThumbPrint"`**.

   Nota: Sustituya <*sslCertThumbPrint*> por la huella digital del certificado SSL creado para el servidor CEP, tras haber eliminado los espacios entre los valores de la huella digital.
5. Complete la instalación seleccionando **Y** o **A**.
6. Inicie la consola de IIS Manager.
7. En el panel Conexiones, expanda el servidor web que aloja CEP.
8. Expanda **Sitios**, **Sitio web predeterminado** y, a continuación, haga clic en el nombre de la aplicación virtual de instalación que corresponda **ADPolicyProvider_CEP_Certificate**.
9. En la aplicación virtual denominada **Inicio**, haga doble clic en la configuración de la aplicación y, a continuación, haga doble clic en **FriendlyName**.
10. Escriba un nombre en Valor y cierre el cuadro de diálogo.
11. Haga doble clic en **URI** y, a continuación, copie **Valor**.

    Notas:

    - Si desea configurar otro método de autenticación en el mismo servidor CEP, debe cambiar el ID.
    - Esta URL se utiliza en MVE o en cualquier aplicación cliente.
12. En el panel izquierdo, haga clic en **Grupo de aplicaciones**.
13. Seleccione **WSEnrollmentPolicyServer** y, a continuación, en el panel derecho, haga clic en **Acciones** > **Configuración avanzada**.
14. Seleccione el campo de identidad de Modelo de proceso.
15. En el cuadro de diálogo Identidad del grupo de aplicaciones, seleccione la cuenta personalizada e introduzca **`CEPSvc`** como el nombre de usuario de dominio.
16. Cierre todos los cuadros de diálogo y actualice IIS desde el panel derecho de Consola de IIS Manager .
17. En PowerShell, escriba **`iisreset`** para reiniciar IIS.

Configuración de CES

El cmdlet **Install-AdcsEnrollmentWebService** configura el servicio web de inscripción de certificados (CES). También se utiliza para crear otras instancias del servicio en de una instalación existente.

1. Inicie sesión en el servidor CES con el nombre de usuario **`CESAdmin`** y, a continuación, inicie PowerShell en modo administrativo.
2. Ejecute el comando **`Import-Module ServerManager`**.
3. Ejecute el comando **`Add-WindowsFeature Adcs-Enroll-Web-Svc`**.
4. Ejecute el comando **`Install-AdcsEnrollmentWebService -ApplicationPoolIdentity -CAConfig "CA1.contoso.com\contoso-CA1-CA" -SSLCertThumbprint "sslCertThumbPrint" -AuthenticationType Certificate`**.

   Notas:

   - Sustituya *<sslCertThumbPrint>* por la huella digital del certificado SSL creado para el servidor CES, tras haber eliminado los espacios entre los valores de la huella digital.
   - Sustituya **`CA1.contoso.com`** por el nombre del equipo de la CA.
   - Sustituya **`contoso-CA1-CA`** por el nombre común de la CA.
   - Si ya ha configurado un método de autenticación en al host, elimine **`ApplicationPoolIdentity`** del comando.
5. Complete la instalación seleccionando **Y** o **A**.
6. Inicie la consola de IIS Manager.
7. En el panel Conexiones, expanda el servidor web que aloja CEP.
8. Expanda **Sitios**, **Sitio web predeterminado** y, a continuación, haga clic en el nombre de la aplicación virtual de instalación que corresponda: **contoso-CA1-CA _CES_Certificate**.
9. En el panel izquierdo, haga clic en **Grupo de aplicaciones**.
10. Seleccione **WSEnrollmentServer** y, a continuación, en el panel derecho, haga clic en **Acciones** > **Configuración avanzada**.
11. Seleccione el campo de identidad de Modelo de proceso.
12. En el cuadro de diálogo Identidad del grupo de aplicaciones, seleccione la cuenta personalizada e introduzca **CESSvc** como el nombre de usuario de dominio.
13. Cierre todos los cuadros de diálogo y actualice IIS desde el panel derecho de la Consola de IIS Manager.
14. En PowerShell, escriba **`iisreset`** para reiniciar IIS.
15. Para el usuario de dominio CESSvc, active la delegación. Para obtener más información, consulte "Activación de la delegación" en la página 94.

Creación de un certificado de cliente

1. Abra **certlm.msc** desde una cuenta de usuario de dominio.
2. Haga clic en **Certificados** > **Personal** > **Certificados** > **Todas las tareas** > **Solicitar nuevo certificado**.
3. Haga clic en **Siguiente**.
4. Haga clic en **Inscripción a Active Directory** > **Acceso de cliente**.

Nota: Si no quiere usar las opciones de **Inscripción a Active Directory**, haga lo siguiente:

a Haga clic en **Configurado por usted** > **Agregar nuevo**.

b Introduzca la URI del servidor de políticas de inscripción como dirección de servidor CEP para la autenticación de Nombre de usuario_Contraseña o de Kerberos.

c Seleccione el tipo de autenticación **Integrado en Windows**.

d Haga clic en **Validar servidor**.

e Cuando se haya validado correctamente, haga clic en **Agregar**.

f Haga clic en **Siguiente**.

g Seleccione una plantilla.

5 Haga clic en **Detalles** > **Propiedades**.

6 Haga clic en **Inscribir**.

7 En la pestaña Asunto, proporcione un nombre de dominio completo (FQDN).

8 En la pestaña Clave privada, seleccione **Hacer exportable la clave privada**.

9 Haga clic en **Aplicar** > **Inscribir**.

Después de inscribir el certificado de cliente, haga lo siguiente para exportarlo en formato PFX.

1 Haga clic en **Certificado** > **Todas las tareas** > **Exportar**.

2 Haga clic en **Siguiente** > **Exportar la clave privada**.

3 Haga clic en **Siguiente**.

4 Escriba la contraseña proporcionada por el cliente.

5 Haga clic en **Siguiente**.

6 Especifique el nombre de archivo en el cuadro de diálogoExportación de certificados.

7 Haga clic en **Siguiente** > **Finalizar**.

Configuración de la autenticación nombre de usuario-contraseña

Configuración de CEP

El cmdlet **Install-AdcsEnrollmentPolicyWebService** configura el servicio web de inscripción de certificados (CEP). También se utiliza para crear otras instancias del servicio en de una instalación existente.

1 Inicie sesión en el servido CEP con el nombre de usuario CEPAdmin y, a continuación, inicie PowerShell en modo administrativo.

2 Ejecute el comando **`Import-Module ServerManager`**.

3 Ejecute el comando **`Add-WindowsFeature Adcs-Enroll-Web-Pol`**.

4 Ejecute el comando **`Install-AdcsEnrollmentPolicyWebService -AuthenticationType UserName -SSLCertThumbprint "sslCertThumbPrint"`**.

Nota: Sustituya *<sslCertThumbPrint>* por la huella digital del certificado SSL creado para el servidor CEP, tras haber eliminado los espacios entre los valores de la huella digital.

5 Complete la instalación seleccionando **Y** o **A**.

6 Inicie la consola de IIS Manager.

7 En el panel Conexiones, expanda el servidor web que aloja CEP.

8 Expanda **Sitios**, **Sitio web predeterminado** y, a continuación, haga clic en el nombre de la aplicación virtual de instalación que corresponda: **ADPolicyProvider_CEP_UsernamePassword**.

9 En la aplicación virtual denominada **Inicio**, haga doble clic en la configuración de la aplicación y, a continuación, haga doble clic en **FriendlyName**.

10 Escriba un nombre en **Valor** y cierre el cuadro de diálogo.

11 Haga doble clic en **URI** y, a continuación, copie **Valor**.

Notas:

- Si desea configurar otro método de autenticación en el mismo servidor CEP, debe cambiar el ID.
- Esta URL se utiliza en MVE o en cualquier aplicación cliente.

12 En el panel izquierdo, haga clic en **Grupo de aplicaciones**.

13 Seleccione **WSEnrollmentPolicyServer** y, a continuación, en el panel derecho, haga clic en **Acciones** > **Configuración avanzada**.

14 Seleccione el campo de identidad de Modelo de proceso.

15 En el cuadro de diálogo Identidad del grupo de aplicaciones, seleccione la cuenta personalizada e introduzca **`CESSvc`**.

16 Cierre todos los cuadros de diálogo y actualice IIS desde el panel derecho de Consola de IIS Manager .

17 En PowerShell, escriba **`iisreset`** para reiniciar IIS.

Configuración de CES

El cmdlet **Install-AdcsEnrollmentWebService** configura el servicio web de inscripción de certificados (CES). También se utiliza para crear otras instancias del servicio en de una instalación existente.

1 Inicie sesión en el servidor CES con el nombre de usuario **`CESAdmin`** y, a continuación, inicie PowerShell en modo administrativo.

2 Ejecute el comando **`Import-Module ServerManager`**.

3 Ejecute el comando **`Add-WindowsFeature Adcs-Enroll-Web-Svc`**.

4 Ejecute el comando **`Install-AdcsEnrollmentWebService -ApplicationPoolIdentity -CAConfig "CA1.contoso.com\contoso-CA1-CA" -SSLCertThumbprint "sslCertThumbPrint" -AuthenticationType UserName`**.

Notas:

- Sustituya <*sslCertThumbprint*> por la huella digital del certificado SSL creado para el servidor CES, tras haber eliminado los espacios entre los valores de la huella digital.
- Sustituya **`CA1.contoso.com`** por el nombre del equipo de la CA.
- Sustituya **`contoso-CA1-CA`** por el nombre común de la CA.
- Si ya ha configurado un método de autenticación en al host, elimine **`ApplicationPoolIdentity`** del comando.

5 Complete la instalación seleccionando **Y** o **A**.

6 Inicie la consola de IIS Manager.

7 En el panel Conexiones, expanda el servidor web que aloja CES.

8 Expanda **Sitios**, **Sitio web predeterminado** y, a continuación, haga clic en el nombre de la aplicación virtual de instalación que corresponda: **contoso-CA1-CA_CES_UsernamePassword**.

9 En el panel izquierdo, haga clic en **Grupo de aplicaciones**.

10 Seleccione **WSEnrollmentServer** y, a continuación, en el panel derecho, haga clic en **Acciones** > **Configuración avanzada** en Acciones.

11 Seleccione el campo de identidad de Modelo de proceso.

12 En el cuadro de diálogo Identidad del grupo de aplicaciones, seleccione la cuenta personalizada e introduzca **`CESSvc`** como el nombre de usuario de dominio.

13 Cierre todos los cuadros de diálogo y actualice IIS desde el panel derecho de Consola de IIS Manager.

14 En PowerShell, escriba **`iisreset`** para reiniciar IIS.

Administración de certificados mediante la autoridad certificadora de OpenXPKI a través de SCEP

Esta sección contiene instrucciones sobre cómo configurar la CA de OpenXPKI versión 2.5.x mediante el protocolo SCEP (Protocolo de inscripción de certificados simple).

Notas:

- Asegúrese de que utiliza el sistema operativo Debian 8 Jessie.
- Para obtener más información sobre OpenXPKI, visite **www.openxpki.org**.

Configuración de la CA de OpenXPKI

Instalación de la CA OpenXPKI

1 Conecte el equipo utilizando PuTTY u otro cliente.

2 En el cliente, ejecute el comando **`sudo su -`** para ir al usuario raíz.

3 Introduzca la contraseña raíz.

4 En **nano /etc/apt/sources.list**, cambie el origen para la instalación de las actualizaciones.

5 Actualice el archivo. Por ejemplo:

```
#

# deb cdrom:[Debian GNU/Linux 8.11.1 _Jessie_ - Official amd64 CD Binary-1
20190211-02:10]/ jessie local main
# deb cdrom:[Debian GNU/Linux 8.11.1 _Jessie_ - Official amd64 CD Binary-1
20190211-02:10]/ jessie local main

deb http://security.debian.org/ jessie/updates main
deb-src http://security.debian.org/ jessie/updates main

# jessie-updates, previously known as 'volatile'
# A network mirror was not selected during install.  The following entries
# are provided as examples, but you should amend them as appropriate
```

```
# for your mirror of choice.
#
deb http://ftp.debian.org/debian/jessie-updates main
deb-src http://ftp.debian.org/debian/jessie-updates main
deb http://ftp.us.debian.org/debian/jessie main
```

6 Guarde el archivo.

7 Ejecute los siguientes comandos:

- **apt-get update**
- **apt-get upgrade**

8 Actualice las listas de certificados de CA en el servidor mediante **apt-get install ca-certificates**.

9 Instale **en_US.utf8 locale** mediante **dpkg-reconfigure locales**.

10 Seleccione la configuración regional **en_US.UTF-8 UTF-8** y, a continuación, haga que sea la configuración regional predeterminada del sistema.

Nota: Utilice las teclas de tabulación y barra espaciadora para seleccionar y desplazarse por el menú.

11 Compruebe las configuraciones regionales que ha generado mediante **locale -a**.

Salida de ejemplo

```
C
C.UTF-8
en_IN
en_IN.utf8
en_US.utf8
POSIX
```

12 Copie la huella del paquete de OpenXPKI mediante **nano /home/Release.key**. En este caso, copie la clave en **/home**.

13 Escriba **9B156AD0 F0E6A6C7 86FABE7A D8363C4E 1611A2BE 2B251336 01D1CDB4 6C24BEF3** como valor.

14 Ejecute el siguiente comando:

```
gpg --print-md sha256 /home/Release.key
```

15 Agregue el paquete utilizando el comando **wget https://packages.openxpki.org/v2/debian/Release.key -O - | apt-key add -**.

16 Agregue el repositorio a la lista de orígenes (jessie) mediante **echo "deb http://packages.openxpki.org/v2/debian/jessie release" > /etc/apt/sources.list.d/openxpki.list** y, a continuación, **aptitude update**.

17 Instale el enlace MySQL y Perl MySQL mediante **aptitude install mysql-server libdbd-mysql-perl**.

18 Instale apache2.2-common mediante **aptitude install apache2.2-common**.

19 En **nano /etc/apt/sources.list**, instale el módulo fastcgi para acelerar la interfaz de usuario.

Nota: Recomendamos que se utilice **mod_fcgid**.

20 Agregue la línea **deb http://http.us.debian.org/debian/jessie main** en el archivo y, a continuación, guárdelo.

21 Ejecute los siguientes comandos:

```
apt-get update
aptitude install libapache2-mod-fcgid
```

22 Active el módulo fastcgi mediante **a2enmod fcgid**.

23 Instale el paquete principal de OpenXPKI mediante **aptitude install libopenxpki-perl openxpki-cgi-session-driver openxpki-i18n**.

24 Reinicie el Apache® Servidor mediante **service apache2 restart**.

25 Compruebe si la instalación se ha realizado correctamente mediante **openxpkiadm version**.

Nota: Si la instalación se ha realizado correctamente, el sistema muestra la versión de OpenXPKI instalada. Por ejemplo, **Version (core): 2.5.5**.

26 Cree la base de datos vacía y, a continuación, asigne el usuario de la base de datos mediante **mysql -u root -p**.

Notas:

- Este comando debe escribirse en el cliente. De lo contrario, no podrá introducir la contraseña.
- Escriba la contraseña para MySQL. En este caso, **root** es el usuario MySQL.
- **openxpki** es el usuario en el que está instalado OpenXPKI.

```
CREATE DATABASE openxpki CHARSET utf8;
CREATE USER 'openxpki'@'localhost' IDENTIFIED BY 'openxpki';
GRANT ALL ON openxpki.* TO 'openxpki'@'localhost';
flush privileges;
```

Si el servicio MySQL no se está ejecutando, ejecute **/etc/init.d/mysql start** para iniciar el servicio.

27 Escriba **quit** para salir de MySQL.

28 Almacene las credenciales utilizadas en **/etc/openxpki/config.d/system/database.yaml**.

Contenido de archivo de ejemplo

```
debug: 0
type: MySQL
name: openxpki
host: localhost
port: 3306
user: openxpki
passwd: openxpki
```

Nota: Cambie **user** y **passwd** para que coincidan con el nombre de usuario y la contraseña de MySQL.

29 Guarde el archivo.

30 Para un esquema de base de datos vacío, ejecute **zcat /usr/share/doc/libopenxpki-perl/examples/schema-mysql.sql.gz | \mysql -u root --password --database openxpki** desde el archivo de esquema proporcionado.

31 Introduzca la contraseña de la base de datos.

Configuración de la CA OpenXPKI mediante el script predeterminado

Nota: El script predeterminado solo configura el dominio predeterminado, **ca-one**. El CDP y las CRL no se configuran.

1. Descomprima el script de ejemplo para instalar el certificado mediante **`gunzip -k /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh.gz`**.
2. Ejecute el script mediante **`bash /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh`**.
3. Confirme la configuración mediante **`openxpkiadm alias --realm ca-one`**.

Salida de ejemplo

```
=== functional token ===
scep (scep):
Alias    : scep-1
Identifier: YsBNZ7JYTbx89F_-Z4jn_RPFFWo
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2016-01-30 20:44:40

vault (datasafe):
Alias    : vault-1
Identifier: lZILS1l6Km5aIGS6pA7P7azAJic
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2016-01-30 20:44:40

ca-signer (certsign):
Alias    : ca-signer-1
Identifier: Sw_IY7AdoGUp28F_cFEdhbtI9pE
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2018-01-29 20:44:40

=== root ca ===
current root ca:
Alias     : root-1
Identifier: fVrqJAlpotPaisOAsnxa9cglXCc
NotBefore : 2015-01-30 20:44:39
NotAfter  : 2020-01-30 20:44:39

upcoming root ca:
  not set
```

4. Compruebe si la instalación se realiza correctamente mediante **`openxpkictl start`**.

Salida de ejemplo

```
Starting OpenXPKI...
OpenXPKI Server is running and accepting requests.
DONE.
```

5. Realice lo siguiente para acceder al servidor OpenXPKI:
   a. En un navegador web, escriba **`http://ipaddress/openxpki/`**.
   b. Inicie sesión como **Operador**. La contraseña predeterminada es **`openxpki`**.

      Nota: El inicio de sesión del operador tiene dos cuentas de operador preconfiguradas, **raop** y **raop2**.
6. Cree una solicitud de certificado y, a continuación, pruébela.

Configuración de la CA de OpenXPKI de forma manual

Descripción general

Nota: Antes de comenzar, asegúrese de que tiene conocimientos básicos sobre la creación de certificados OpenSSL.

Para configurar la CA OpenXPKI de forma manual, debe crear lo siguiente:

1. Certificado de la CA raíz. Para obtener más información, consulte "Creación de un certificado de la CA raíz" en la página 106.
2. Certificado del firmante de la CA, firmado por la CA raíz. Para obtener más información, consulte "Creación de un certificado de firmante" en la página 107.
3. Certificado de almacén de datos, autofirmado. Para obtener más información, consulte "Creación de un certificado de almacén" en la página 107.
4. Certificado SCEP, firmado por el certificado del firmante.

Notas:

- Al seleccionar el hash de firma, utilice SHA256 o SHA512.
- El cambio del tamaño de la clave pública es opcional.

En este caso, vamos a utilizar el directorio **/etc/certs/openxpki_ca-one/** para la generación de certificados. Sin embargo, puede utilizar cualquier directorio.

Creación de un archivo de configuración de OpenSSL

1. Ejecute el siguiente comando:

   ```
   nano /etc/certs/openxpki_ca-one/openssl.conf
   ```

   Nota: Si se puede acceder al servidor mediante el nombre de dominio completo (FQDN), utilice el DNS del servidor en lugar de su dirección IP.

Archivo de ejemplo

```
# x509_extensions               = v3_ca_extensions
# x509_extensions               = v3_issuing_extensions
# x509_extensions               = v3_datavault_extensions
# x509_extensions               = v3_scep_extensions
# x509_extensions               = v3_web_extensions
# x509_extensions               = v3_ca_reqexts # not for root self-signed, only for issuing
## x509_extensions              = v3_datavault_reqexts # not required self-signed
# x509_extensions               = v3_scep_reqexts
# x509_extensions               = v3_web_reqexts

[ req ]
default_bits            = 4096
distinguished_name      = req_distinguished_name

[ req_distinguished_name ]
domainComponent         = Domain Component
commonName              = Common Name

[ v3_ca_reqexts ]
subjectKeyIdentifier    = hash
keyUsage                = digitalSignature, keyCertSign, cRLSign

[ v3_datavault_reqexts ]
subjectKeyIdentifier    = hash
```

```
keyUsage                = keyEncipherment
extendedKeyUsage        = emailProtection

[ v3_scep_reqexts ]
subjectKeyIdentifier    = hash

[ v3_web_reqexts ]
subjectKeyIdentifier    = hash
keyUsage                = critical, digitalSignature, keyEncipherment
extendedKeyUsage        = serverAuth, clientAuth

[ v3_ca_extensions ]
subjectKeyIdentifier    = hash
keyUsage                = digitalSignature, keyCertSign, cRLSign
basicConstraints        = critical,CA:TRUE
authorityKeyIdentifier  = keyid:always,issuer

[ v3_issuing_extensions ]
subjectKeyIdentifier    = hash
keyUsage                = digitalSignature, keyCertSign, cRLSign
basicConstraints        = critical,CA:TRUE
authorityKeyIdentifier  = keyid:always,issuer:always
crlDistributionPoints   = URI:http://FQDN of the server/CertEnroll/MYOPENXPKI.crl
authorityInfoAccess     = caIssuers;URI:http://FQDN of the server/CertEnroll/MYOPENXPKI.crt

[ v3_datavault_extensions ]
subjectKeyIdentifier    = hash
keyUsage                = keyEncipherment
extendedKeyUsage        = emailProtection
basicConstraints        = CA:FALSE
authorityKeyIdentifier  = keyid:always,issuer

[ v3_scep_extensions ]
subjectKeyIdentifier    = hash
basicConstraints        = CA:FALSE
authorityKeyIdentifier  = keyid,issuer

[ v3_web_extensions ]
subjectKeyIdentifier    = hash
keyUsage                = critical, digitalSignature, keyEncipherment
extendedKeyUsage        = serverAuth, clientAuth
basicConstraints        = critical,CA:FALSE
subjectAltName          = DNS:stlopenxpki.lexmark.com
crlDistributionPoints   = URI:http://FQDN of the server/CertEnroll/MYOPENXPKI_ISSUINGCA.crl
authorityInfoAccess     = caIssuers;URI:http://FQDN of the
server/CertEnroll/MYOPENXPKI_ISSUINGCA.crt
```

2. Cambie la dirección IP y el nombre del certificado de la CA con la información de configuración.
3. Guarde el archivo.

Creación de un archivo de contraseña para claves de certificado

1. Ejecute el siguiente comando:

   `nano /etc/certs/openxpki_ca-one/pd.pass`

2. Escriba su contraseña.
3. Guarde el archivo.

Creación de un certificado de la CA raíz

Nota: Puede crear un certificado de la CA raíz autofirmado o generar una solicitud de certificado y, a continuación, obtenerlo firmado por la CA raíz.

Ejecute los siguientes comandos:

Nota: Sustituya la longitud de clave, el algoritmo de firma y el nombre del certificado por los valores adecuados.

1. **openssl genrsa -out /etc/certs/openxpki_ca-one/ca-root-1.key -passout file:/etc/certs/openxpki_ca-one/pd.pass 4096**
2. **openssl req -new -key /etc/certs/openxpki_ca-one/ca-root-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=MYOPENXPKI_ROOTCA -out /etc/certs/openxpki_ca-one/ca-root-1.csr**
3. **openssl req -config /etc/certs/openxpki_ca-one/openssl.conf -extensions v3_ca_extensions -x509 -days 3560 -in /etc/certs/openxpki_ca-one/ca-root-1.csr -key /etc/certs/openxpki_ca-one/ca-root-1.key -out /etc/certs/openxpki_ca-one/ca-root-1.crt -sha256**

Creación de un certificado de firmante

Nota: Sustituya la longitud de clave, el algoritmo de firma y el nombre del certificado por los valores adecuados.

1. Ejecute el siguiente comando:

   openssl genrsa -out /etc/certs/openxpki_ca-one/ca-signer-1.key -passout file:/etc/certs/openxpki_ca-one/pd.pass 4096

2. Cambie el asunto de la solicitud con la información de la CA mediante **openssl req -config /etc/certs/openxpki_ca-one/openssl.conf -reqexts v3_ca_reqexts -new -key /etc/certs/openxpki_ca-one/ca-signer-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=MYOPENXPKI_ISSUINGCA -out /etc/certs/openxpki_ca-one/ca-signer-1.csr**.
3. Obtenga el certificado firmado por la CA raíz mediante **openssl x509 -req -extfile /etc/certs/openxpki_ca-one/openssl.conf -extensions v3_issuing_extensions -days 3650 -in /etc/certs/openxpki_ca-one/ca-signer-1.csr -CA /etc/certs/openxpki_ca-one/ca-root-1.crt -CAkey /etc/certs/openxpki_ca-one/ca-root-1.key -CAcreateserial -out /etc/certs/openxpki_ca-one/ca-signer-1.crt -sha256**.

Creación de un certificado de almacén

Notas:

- El certificado de almacén se firma automáticamente.
- Sustituya la longitud de clave, el algoritmo de firma y el nombre del certificado por los valores adecuados.

1. Ejecute el siguiente comando:

   openssl genrsa -out /etc/certs/openxpki_ca-one/vault-1.key -passout file:/etc/certs/openxpki_ca-one/pd.pass 4096

2 Cambie el asunto de la solicitud con la información de la CA mediante **openssl req -config /etc/certs/openxpki_ca-one/openssl.conf -reqexts v3_datavault_reqexts -new -key /etc/certs/openxpki_ca-one/vault-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/DC=STLOPENXPKI_INTERNAL/CN=MYOPENXPKI_DATAVAULT -out /etc/certs/openxpki_ca-one/vault-1.csr**.

3 Ejecute el siguiente comando:

```
openssl req -config /etc/certs/openxpki_ca-one/openssl.conf -extensions
v3_datavault_extensions -x509 -days 3560 -in /etc/certs/openxpki_ca-
one/vault-1.csr -key /etc/certs/openxpki_ca-one/vault-1.key -
out /etc/certs/openxpki_ca-one/vault-1.crt
```

Creación de un certificado SCEP

Nota: El certificado SCEP está firmado por el certificado del firmante.

Ejecute los siguientes comandos:

Nota: Sustituya la longitud de clave, el algoritmo de firma y el nombre del certificado por los valores adecuados.

1 **openssl genrsa -out /etc/certs/openxpki_ca-one/scep-1.key -passout file:/etc/certs/openxpki_ca-one/pd.pass 4096**

2 **openssl req -config /etc/certs/openxpki_ca-one/openssl.conf -reqexts v3_scep_reqexts -new -key /etc/certs/openxpki_ca-one/scep-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=MYOPENXPKI_SCEPCA -out /etc/certs/openxpki_ca-one/scep-1.csr**

3 **openssl x509 -req -extfile /etc/certs/openxpki_ca-one/openssl.conf -extensions v3_scep_extensions -days 900 -in /etc/certs/openxpki_ca-one/scep-1.csr -CA /etc/certs/openxpki_ca-one/ca-signer-1.crt -CAkey /etc/certs/openxpki_ca-one/ca-signer-1.key -CAcreateserial -out /etc/certs/openxpki_ca-one/scep-1.crt -sha256**

Copia del archivo de clave y creación de un enlace simbólico

1 Copie los archivos de clave en **/etc/openxpki/ca/ca-one/ .**

Nota: Los archivos de clave deben ser legibles para OpenXPKI.

```
cp /etc/certs/openxpki_ca-one/ca-signer-1.key /etc/openxpki/ca/ca-one/

cp /etc/certs/openxpki_ca-one/vault-1.key /etc/openxpki/ca/ca-one/

cp /etc/certs/openxpki_ca-one/scep-1.key /etc/openxpki/ca/ca-one/
```

2 Cree el enlace simbólico.

Nota: Los enlaces simbólicos son alias utilizdos por la configuración predeterminada.

```
ln -s /etc/openxpki/ca/ca-one/ca-signer-1.key /etc/openxpki/ca/ca-one/ca-signer-1.pem

ln -s /etc/openxpki/ca/ca-one/scep-1.key /etc/openxpki/ca/ca-one/scep-1.pem

ln -s /etc/openxpki/ca/ca-one/vault-1.key /etc/openxpki/ca/ca-one/vault-1.pem
```

Importación de certificados

Importe el certificado raíz, el certificado del firmante, el certificado de almacén y el certificado SCEP a la base de datos con los tokens adecuados.

Ejecute los siguientes comandos:

1. **openxpkiadm certificate import --file /etc/certs/openxpki_ca-one/ca-root-1.crt**
2. **openxpkiadm certificate import --file /etc/certs/openxpki_ca-one/ca-signer-1.crt --realm ca-one --token certsign**
3. **openxpkiadm certificate import --file /etc/certs/openxpki_ca-one/scep-1.crt --realm ca-one --token scep**
4. **openxpkiadm certificate import --file /etc/certs/openxpki_ca-one/vault-1.crt --realm ca-one --token datasafe**
5. Compruebe que la importación se realiza correctamente mediante **openxpkiadm alias --realm ca-one**..

Salida de ejemplo

```
=== functional token ===
scep (scep):
Alias     : scep-1
Identifier: YsBNZ7JYTbx89F_-Z4jn_RPFFWo
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2016-01-30 20:44:40

vault (datasafe):
Alias     : vault-1
Identifier: lZILS1l6Km5aIGS6pA7P7azAJic
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2016-01-30 20:44:40

ca-signer (certsign):
Alias     : ca-signer-1
Identifier: Sw_IY7AdoGUp28F_cFEdhbtI9pE
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2018-01-29 20:44:40

=== root ca ===
current root ca:
Alias     : root-1
Identifier: fVrqJAlpotPaisOAsnxa9cglXCc
NotBefore : 2015-01-30 20:44:39
NotAfter  : 2020-01-30 20:44:39

upcoming root ca:
  not set
```

Inicio de OpenXPKI

1. Ejecute el comando **openxpkictl start**

Salida de ejemplo

```
Starting OpenXPKI...
OpenXPKI Server is running and accepting requests.
DONE.
```

2 Realice lo siguiente para acceder al servidor OpenXPKI:

a En un navegador web, escriba **`http://ipaddress/openxpki/`**.

Nota: En lugar de **`ipaddress`**, también puede utilizar el FQDN del servidor.

b Inicie sesión como **Operador**. La contraseña predeterminada es **`openxpki`**.

Nota: El inicio de sesión del operador tiene dos cuentas de operador preconfiguradas, **raop** y **raop2**.

3 Cree una solicitud de certificado y, a continuación, pruébela.

Generación de información de la CRL

Nota: Si se puede acceder al servidor mediante el FQDN, utilice el DNS del servidor en lugar de su dirección IP.

1 Detenga el servicio OpenXPKI mediante **`Openxpkictl stop`**.

2 En **nano /etc/openxpki/config.d/realm/ca-one/publishing.yaml**, actualice la sección **`connectors: cdp`** para que muestre lo siguiente:

```
class: Connector::Builtin::File::Path
LOCATION: /var/www/openxpki/CertEnroll/
file: "[% ARGS.0 %].crl"
content: "[% pem %]"
```

a En **nano /etc/openxpki/config.d/realm/ca-one/profile/default.yaml**, actualice lo siguiente:

- **`crl_distribution_points:`** sección

```
critical: 0
uri:
    - http://FQDN of the server/CertEnroll/[% ISSUER.CN.0 %].crl
    - ldap://localhost/[% ISSUER.DN %]
```

- **`authority_info_access:`** sección

```
critical: 0
ca_issuers: http://FQDN of the server/CertEnroll/MYOPENXPKI.crt
ocsp: http://ocsp.openxpki.org/
```

Cambie la dirección IP y el nombre del certificado de la CA de acuerdo con el servidor de la CA.

b En **nano /etc/openxpki/config.d/realm/ca-one/crl/default.yaml**, realice lo siguiente:

- Si es necesario, actualice **`nextupdate`** y **`renewal`**.
- Agregue **`ca_issuers`** a la siguiente sección:

```
extensions:
            authority_info_access:
                    critical: 0
                    # ca_issuers and ocsp can be scalar or list
                    ca_issuers: http://FQDN of the server/CertEnroll/MYOPENXPKI.crt
                   #ocsp: http://ocsp.openxpki.org/
```

Cambie la dirección IP y el nombre del certificado de la CA de acuerdo con el servidor de la CA.

3 Inicie el servicio OpenXPKI mediante **`Openxpkictl start`**.

Configuración de la accesibilidad de la CRL

1. Detenga el servicio Apache mediante **`service apache2 stop`**.
2. Cree un directorio **CertEnroll** para crl en el directorio **/var/www/openxpki/**.
3. Defina **openxpki** como propietario de este directorio y, a continuación, configure los permisos para permitir a Apache leer y ejecutar, y a otros servicios solo leer.

   chown openxpki /var/www/openxpki/CertEnroll

   chmod 755 /var/www/openxpki/CertEnroll
4. Agregue una referencia al archivo alias.conf de Apache mediante **`nano /etc/apache2/mods-enabled/alias.conf`**.
5. Después de la sección **`<Directory "/usr/share/apache2/icons">`**, agregue lo siguiente:

```
Alias /CertEnroll/ "/var/www/openxpki/CertEnroll/"
 <Directory "/var/www/openxpki/CertEnroll">
   Options FollowSymlinks
   AllowOverride None
   Require all granted
 </Directory>
```

6. Agregue una referencia en el archivo apache2.conf utilizando **nano /etc/apache2/apache2.conf**.
7. Agregue lo siguiente en la sección **`Apache2 HTTPD server`**:

```
<Directory /var/www/openxpki/CertEnroll>
  Options FollowSymlinks
  AllowOverride None
  Allow from all
</Directory>
```

8. Inicie el servicio Apache mediante **`service apache2 start`**.

Activación del servicio SCEP

1. Detenga el servicio OpenXPKI mediante **`openxpkictl stop`**.
2. Instale el paquete openca-tools usando **`aptitude install openca-tools`**.
3. Inicie el servicio OpenXPKI mediante **`openxpkictl start`**.

Pruebe el servicio con cualquier cliente; por ejemplo, certnanny con SSCEP.

Nota: SSCEP es un cliente de línea de comandos para SCEP. Puede descargar SSCEP de **https://github.com/certnanny/sscep**.

Activación del certificado Firmante en nombre de un tercero (agente de inscripción)

Para las solicitudes automáticas de certificados, se utilizará la función de certificado Firmante en nombre de un tercero de OpenXPKI.

1. Detenga el servicio OpenXPKI mediante **`openxpkictl stop`**.
2. En **nano /etc/openxpki/config.d/realm/ca-one/scep/generic.yaml**, desde la sección **`authorized_signer:`**, agregue una regla para el nombre del sujeto del certificado de firmante.

   ```
   rule1:
                   # Full DN
                       subject: CN=Markvision_.*
   ```

   Notas:

   - En esta regla, cualquier certificado CN que empiecen por **`MarkVision_`** es el certificado Firmante en nombre de un tercero.
   - El nombre del sujeto se define en MVE para generar el certificado Firmante en nombre de un tercero.
   - Revise el espacio y la sangría en el archivo de script.
   - Si el CN se cambia en MVE, agregue el CN actualizado en OpenXPKI.
   - Solo se puede especificar un certificado como Firmante en nombre de un tercero y, a continuación, especificar el CN completo.
3. Guarde el archivo.
4. Inicie el servicio OpenXPKI mediante **`openxpkictl start`**.

Activación de la aprobación automática de solicitudes de certificado en la CA OpenXPKI

1. Detenga el servicio OpenXPKI mediante **`openxpkictl stop`**.
2. En **nano /etc/openxpki/config.d/realm/ca-one/scep/generic.yaml**, actualice la sección **`eligible`** :

Contenido antiguo

```
eligible:
            initial:
                value@: connector:scep.generic.connector.initial
               args: '[% context.cert_subject_parts.CN.0 %]'
               expect:
                   - Build
                   - New
```

Nuevo contenido

```
eligible:
            initial:
                value: 1
                # value@: connector:scep.generic.connector.initial
                # args: '[% context.cert_subject_parts.CN.0 %]'
                # expect:
                #    - Build
                #    - New
```

Notas:

- Revise el espacio y la sangría en el archivo de script.
- Para aprobar certificados de forma manual, comente **`value: 1`** y, a continuación, quite el comentario de las otras líneas que se hayan comentado previamente.

3 Guarde el archivo.

4 Inicie el servicio OpenXPKI mediante **`openxpkictl start`**.

Creación de un segundo dominio

En OpenXPKI, puede configurar varias estructuras PKI en el mismo sistema. En los temas siguientes se muestra cómo crear otro dominio para MVE con el nombre **ca-two**.

Copia y configuración del directorio

1 Copie el árbol de directorios de ejemplo **/etc/openxpki/config.d/realm/ca-one** en un nuevo directorio (**cp -avr /etc/openxpki/config.d/realm/ca-one /etc/openxpki/config.d/realm/ca-two**) dentro del directorio del dominio.

2 En **/etc/openxpki/config.d/system/reinos.yaml**, actualice la siguiente sección:

Contenido antiguo

```
# This is the list of realms in this PKI
# You only need to enable the realms which are visible on the server

ca-one:
    label: Verbose name of this realm
    baseurl: https://pki.example.com/openxpki/

#ca-two:
#    label: Verbose name of this realm
#    baseurl: https://pki.acme.org/openxpki/
```

Nuevo contenido

```
# This is the list of realms in this PKI
# You only need to enable the realms which are visible on the server

ca-one:
    label: CA-ONE
    baseurl: https://pki.example.com/openxpki/

ca-two:
    label: CA-TWO
    baseurl: https://pki.example.com/openxpki/
```

3 Guarde el archivo.

Creación de certificados

En las siguientes instrucciones se muestra cómo generar el certificado de firmante, el certificado de almacén y el certificado SCEP. La CA raíz firma el certificado de firmante y, a continuación, el certificado de firmante firma el certificado SCEP. El certificado de almacén se firma automáticamente.

1. Genere los certificados y, a continuación, fírmelos. Para obtener más información, consulte "Configuración de la CA de OpenXPKI de forma manual" en la página 105.

   Nota: Cambie el nombre común del certificado para que el usuario pueda distinguir fácilmente entre distintos certificados para diferentes dominios. Puede cambiar **DC=CA-ONE** a **DC=CA-DOS**. Los archivos de certificado se crean en el directorio **/etc/certs/openxpki_ca-two/**.

2. Copie los archivos de clave en **/etc/openxpki/ca/ca-two/**.

   Nota: Los archivos de clave deben ser legibles para OpenXPKI.

   ```
   cp /etc/certs/openxpki_ca-two/ca-signer-1.key /etc/openxpki/ca/ca-two/

   cp /etc/certs/openxpki_ca-two/vault-1.key /etc/openxpki/ca/ca-two/

   cp /etc/certs/openxpki_ca-two/scep-1.key /etc/openxpki/ca/ca-two/
   ```

3. Cree el enlace simbólico. Además, cree un enlace simbólico para el certificado de la CA raíz.

   Nota: Los enlaces simbólicos son alias utilizdos por la configuración predeterminada.

   ```
   ln -s /etc/openxpki/ca/ca-one/ca-root-1.crt /etc/openxpki/ca/ca-two/ca-root-1.crt

   ln -s /etc/openxpki/ca/ca-two/ca-signer-1.key /etc/openxpki/ca/ca-two/ca-signer-1.pem

   ln -s /etc/openxpki/ca/ca-two/scep-1.key /etc/openxpki/ca/ca-two/scep-1.pem

   ln -s /etc/openxpki/ca/ca-two/vault-1.key /etc/openxpki/ca/ca-two/vault-1.pem
   ```

4. Importe el certificado de firmante, el certificado de almacén y el certificado SCEP a la base de datos con los tokens adecuados para **ca-two**.

   ```
   openxpkiadm certificate import --file /etc/certs/openxpki_ca-two/ca-signer-1.crt --realm
   ca-two –issuer /etc/openxpki/ca/ca-two/ca-one-1.crt --token certsign

   openxpkiadm certificate import --file /etc/certs/openxpki_ca-two/scep-1.crt --realm ca-
   two --token scep

   openxpkiadm certificate import --file /etc/certs/openxpki_ca-two/vault-1.crt --realm ca-
   two --token datasafe
   ```

5. Compruebe si la importación se realiza correctamente utilizando **openxpkiadm alias --realm ca-two**.

Salida de ejemplo

```
=== functional token ===
scep (scep):
Alias    : scep-1
Identifier: YsBNZ7JYTbx89F_-Z4jn_RPFFWo
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2016-01-30 20:44:40

vault (datasafe):
Alias    : vault-1
Identifier: lZILS1l6Km5aIGS6pA7P7azAJic
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2016-01-30 20:44:40

ca-signer (certsign):
Alias    : ca-signer-1
Identifier: Sw_IY7AdoGUp28F_cFEdhbtI9pE
```

```
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2018-01-29 20:44:40

=== root ca ===
current root ca:
Alias     : root-1
Identifier: fVrqJAlpotPaisOAsnxa9cglXCc
NotBefore : 2015-01-30 20:44:39
NotAfter  : 2020-01-30 20:44:39

upcoming root ca:
  not set
```

En este caso, la información de la CA raíz es la misma para **ca-one** y **ca-two**.

6. Si ha cambiado la contraseña de la clave de certificado durante la creación del certificado, actualice **nano /etc/openxpki/config.d/realm/ca-two/crypto.yaml**.
7. Genere las CRL para este dominio. Para obtener más información, consulte "Generación de información de la CRL" en la página 110.
8. Publique las CRL para este dominio. Para obtener más información, consulte "Configuración de la accesibilidad de la CRL" en la página 111.
9. Reinicie el servicio OpenXPKI mediante **openxpkictl restart**.

Salida de ejemplo

```
Stopping OpenXPKI
Stopping gracefully, 3 (sub)processes remaining...
DONE.
Starting OpenXPKI...
OpenXPKI Server is running and accepting requests.
DONE.
```

10. Realice lo siguiente para acceder al servidor OpenXPKI:
    a. En un navegador web, escriba **http://ipaddress/openxpki/**.
    b. Inicie sesión como **Operador**. La contraseña predeterminada es **openxpki**.

    Nota: El inicio de sesión del operador tiene dos cuentas de operador preconfiguradas, **raop** y **raop2**.

Configuración del punto final SCEP para varios dominios

El punto final SCEP del dominio predeterminado es **http://<ipaddress>/scep/scep**. Si tiene varios dominios, configure un punto final SCEP único (archivo de configuración diferente) para cada dominio. En las siguientes instrucciones, utilizamos dos dominios PKI, **ca-one** y **ca-two**.

1. Copie el archivo de configuración predeterminado en **cp /etc/openxpki/scep/default.conf /etc/openxpki/scep/ca-one.conf**.

   Nota: Asigne al archivo el nombre **ca-one.conf**.
2. En **nano /etc/openxpki/scep/ca-one.conf**, cambie el valor de dominio a **realm=ca-one**.
3. Cree otro archivo de configuración en **cp /etc/openxpki/scep/default.conf /etc/openxpki/scep/ca-two.conf**.

   Nota: Asigne al archivo el nombre **ca-two.conf**.
4. En **nano /etc/openxpki/scep/ca-two.conf**, cambie el valor de dominio a **realm=ca-two**.
5. Reinicie el servicio OpenXPKI mediante **openxpkictl restart**.

Los puntos finales SCEP son los siguientes:

- **ca-one**—**http://ipaddress/scep/ca-one**
- **ca-two**—**http://ipaddress/scep/ca-two**

Si desea diferenciar entre credenciales de inicio de sesión y plantillas de certificado predeterminadas para diferentes dominios PKI, puede que necesite una configuración avanzada.

Activación de varios certificados activos con el mismo asunto para que estén presentes a la vez

De forma predeterminada, en OpenXPKI sólo puede estar activo un certificado con el mismo nombre de asunto a la vez. Sin embargo, cuando se aplican varios certificados con nombre, deben estar presentes varios certificados activos con el mismo nombre de asunto a la vez.

1. En **/etc/openxpki/config.d/realm/REALM NAME/scep/generic.yaml**, en la sección **policy**, cambie el valor de **max_active_certs** de **1** a **0**.

   Notas:

   - REALM NAME es el nombre de dominio. Por ejemplo, **ca-one**.
   - Revise el espacio y la sangría en el archivo de script.

2. Reinicie el servicio OpenXPKI mediante **openxpkictl restart**.

Definición del número de puerto predeterminado para la CA OpenXPKI

De forma predeterminada, Apache escucha en el número de puerto 80. Defina el número de puerto predeterminado para la CA OpenXPKI para evitar conflictos.

1. En **/etc/apache2/ports.conf**, agregue o modifique un puerto. Por ejemplo, **Listen 8080**.
2. En **/etc/apache2/sites-enabled/000-default.conf**, agregue o modifique la sección **VirtualHost** para asignar un nuevo puerto. Por ejemplo, **<VirtualHost *:8080>**.
3. Reinicie el servidor Apache con **systemctl restart apache2**.

Para comprobar el estado, ejecute **netstat -tlpn| grep apache**. La URL SCEP de OpenXPKI es ahora **http://ipaddress:8080/Scep/ca-one** y la URL web es **http://dirección IP:8080/Openxpki.**.

Cómo rechazar solicitudes de certificado sin Contraseña de comprobación en la CA OpenXPKI

De forma predeterminada, OpenXPKI acepta solicitudes sin comprobar la contraseña de comprobación. La solicitud de certificado no se rechaza y la CA y el administrador de la CA determinan si se debe aprobar o rechazar la solicitud. Para evitar posibles problemas de seguridad, desactive esta función de modo que se rechacen inmediatamente todas las solicitudes de certificado que contengan contraseñas no válidas. En MVE, la Contraseña de comprobación solo es necesaria cuando se genera el certificado del agente de inscripción.

1. En **etc/openxpki/config.d/realm/REALM NAME/scep/generic.yaml**, en la sección **policy**, cambie el valor de **allow_man_authen** de **1** a **0**.

   Notas:

   - REALM NAME es el nombre de dominio. Por ejemplo, **ca-one**.

- Revise el espacio y la sangría en el archivo de script.

2 Reinicie el servicio OpenXPKI mediante **`openxpkictl restart`**.

Adición de EKU de autenticación de cliente en los certificados

1 En **/etc/openxpki/config.d/realm/REALM NAME/profile/I18N_OPENXPKI_PROFILE_TLS_SERVER.yaml**, en la sección **`extended_key_usage:`** cambie el valor de **`client_auth:`** a **`1`**.

Notas:

- REALM NAME es el nombre de dominio. Por ejemplo, **ca-one**.
- Revise el espacio y la sangría en el archivo de script.

2 Reinicie el servicio OpenXPKI mediante **`openxpkictl restart`**.

Obtención del asunto del certificado completo al realizar la solicitud a través de SCEP

De forma predeterminada, OpenXPKI solo lee el CN del asunto del certificado que se solicita. El resto de la información, como el país, la localidad y el DC, están codificados. Por ejemplo, si un asunto de certificado es **`C=US`**, **`ST=KY`**, **`L=Lexington`**, **`O=Lexmark`**, **`OU=ISS`**, **`CN=ET0021B7C34AEC.dhcp.dev.lexmark.com`**, después de firmar el certificado a través de SCEP, el asunto se cambia a **`DC=Test Deployment`**, **`DC= OpenXPKI , CN=ET0021B7C34AEC.dhcp.dev.lexmark.com .`**

Nota: REALM NAME es el nombre de dominio. Por ejemplo, **ca-one**.

1 En **/etc/openxpki/config.d/realm/REALM NAME/profile/I18N_OPENXPKI_PROFILE_TLS_SERVER.yaml**, en la sección **`enroll`**, cambie el valor de **`dn`** a lo siguiente:

```
CN=[% CN.0 %][% IF OU %][% FOREACH entry = OU %],OU=[% entry %][% END %][% END %][% IF O
%][% FOREACH entry = O %],O=[% entry %][% END %][% END %][% IF L %],L=[% L.0 %][% END %]
[% IF ST %],ST=[% ST.0 %][% END %][% IF C %],C=[% C.0 %][% END %][% IF DC %][% FOREACH
entry = DC %],DC=[% entry %][% END %][% END %][% IF EMAIL %][% FOREACH entry = EMAIL
%],EMAIL=[% entry %][% END %][% END %]
```

2 Guarde el archivo.

3 Cree un archivo denominado **l.yaml** en el directorio **/etc/openxpki/config.d/realm/REALM NAME/profile/template**.

4 Agregue lo siguiente:

```
id: L
label: L
description: I18N_OPENXPKI_UI_PROFILE_L_DESC
preset: L
type: freetext
width: 60
placeholder: Kolkata
```

5 Guarde el archivo.

6 Cree un archivo denominado **st.yaml** en el directorio **/etc/openxpki/config.d/realm/REALM NAME/profile/template**.

7 Agregue lo siguiente:

```
id: ST
label: ST
description: I18N_OPENXPKI_UI_PROFILE_ST_DESC
```

```
preset: ST
type: freetext
width: 60
placeholder: WB
```

8 Guarde el archivo.

Nota: OpenXPKI debe ser propietario de ambos archivos y debe permitir la lectura, la escritura y la ejecución.

9 Reinicie el servicio OpenXPKI mediante **`openxpkictl restart`**.

Revocación de certificados y publicación de CRL

1 Acceda al servidor OpenXPKI.

   a En un navegador web, escriba **`http://ipaddress/openxpki/`**.

   b Inicie sesión como **Operador**. La contraseña predeterminada es **`openxpki`**.

   Nota: El inicio de sesión del operador tiene dos cuentas de operador preconfiguradas, **raop** y **raop2**.

2 Haga clic en **Búsqueda de flujo de trabajo** > **Buscar ahora**.

3 Haga clic en el certificado que desee revocar y, a continuación, en el enlace del certificado.

4 En la sección Acción, haga clic en la **solicitud de revocación**.

5 Escriba los valores adecuados y, a continuación, haga clic en **Continuar** > **Enviar solicitud**.

6 En la página siguiente, apruebe la solicitud. La revocación del certificado está esperando la siguiente publicación de la CRL.

7 En la sección Operación PKI, haga clic en **Emitir una lista de revocación de certificados (CRL)**.

8 Haga clic en **Aplicar creación de listas de revocación** > **Continuar**.

9 En la sección Operación PKI, haga clic en **Publicar CA/CRL**.

10 Haga clic en **Búsqueda de flujo de trabajo** > **Buscar ahora**.

11 Haga clic en el certificado revocado con el tipo **certificate_revocation_request_v2**.

12 Haga clic en **Forzar reactivación**.

En la nueva CRL, puede encontrar el número de serie y el motivo de revocación del certificado revocado.

Administración de certificados mediante la autoridad certificadora de OpenXPKI a través de EST

En esta sección se ayuda al usuario a configurar la CA de OpenXPKI versión 3.x.x mediante el protocolo EST.

Notas:

- Asegúrese de que utiliza el sistema operativo Debian 10 Buster.
- Para obtener más información sobre OpenXPKI, visite **www.openxpki.org**.

Configuración de la CA de OpenXPKI

Instalación de la CA OpenXPKI

1. Conecte el equipo utilizando PuTTY u otro cliente.
2. En el cliente, ejecute el comando **`sudo su -`** para ir al usuario raíz.
3. Introduzca la contraseña raíz.
4. En **nano /etc/apt/sources.list**, cambie el origen para la instalación de las actualizaciones.
5. Actualice el archivo. Por ejemplo:

```
#

# deb cdrom:[Debian GNU/Linux testing _Buster_ - Official Snapshot amd64 DVD Binary-1
20190527-04:04]/ buster contrib main
# deb cdrom:[Debian GNU/Linux testing _Buster_ - Official Snapshot amd64 DVD Binary-1
20190527-04:04]/ buster contrib main

deb http://security.debian.org/debian-security buster/updates main contrib
deb-src http://security.debian.org/debian-security buster/updates main contrib

# buster-updates, previously known as 'volatile'
# A network mirror was not selected during install. The following entries
# are provided as examples, but you should amend them as appropriate
# for your mirror of choice.
#
deb http://ftp.debian.org/debian/ buster-updates main
deb-src http://ftp.debian.org/debian/ buster-updates main
deb http://ftp.us.debian.org/debian/ buster main
```

6. Guarde el archivo.
7. Ejecute los siguientes comandos:
   - **`apt-get update`**
   - **`apt-get upgrade`**
8. Actualice las listas de certificados de CA en el servidor mediante **`apt-get install ca-certificates`**.
9. Instale **en_US.utf8 locale** mediante **`dpkg-reconfigure locales`**.
10. Seleccione la configuración regional **en_US.UTF-8 UTF-8** y, a continuación, haga que sea la configuración regional predeterminada del sistema.

    Nota: Utilice las teclas de tabulación y barra espaciadora para seleccionar y desplazarse por el menú.

11 Compruebe las configuraciones regionales que ha generado mediante **locale -a**.

Salida de ejemplo

```
C
C.UTF-8
en_IN
en_IN.utf8
en_US.utf8
POSIX
```

12 Copie la huella del paquete de OpenXPKI mediante **nano /home/Release.key**. En este caso, copie la clave en **/home**.

13 Escriba **55D89776 006F632B E0196E3E D2495509 BAFDDC74 22FEAAD2 F055074E 0FE3A724** como valor.

14 Ejecute el siguiente comando:

```
gpg --print-md sha256 /home/Release.key
```

15 Agregue el paquete utilizando el comando **wget https:**comando **//packages.openxpki.org/v3/debian/Release.key -O - | apt-key add -**.

16 Agregue el repositorio a la lista de orígenes (buster) mediante **echo "deb http://packages.openxpki.org/v3/debian/ buster release" > /etc/apt/sources.list.d/openxpki.list** y, a continuación, **apt update**.

17 Instale el enlace MySQL y Perl MySQL mediante **apt install mariadb-server libdbd-mariadb-perl**.

18 Instale apache2.2-common using **apt install apache2**.

19 En **nano /etc/apt/sources.list**, instale el módulo fastcgi para acelerar la interfaz de usuario.

Nota: Recomendamos que se utilice **mod_fcgid**.

20 Agregue la línea **deb http://http.us.debian.org/debian/ buster main** en el archivo y, a continuación, guárdelo.

21 Ejecute los siguientes comandos:

```
apt-get update
apt install libapache2-mod-fcgid
```

22 Active el módulo fastcgi mediante **a2enmod fcgid**.

23 Instale el paquete principal de OpenXPKI mediante **apt install libopenxpki-perl openxpki-cgi-session-driver openxpki-i18n**.

24 Reinicie el Apache Servidor mediante **service apache2 restart**.

25 Compruebe si la instalación se ha realizado correctamente mediante **openxpkiadm version**.

Nota: Si la instalación se ha realizado correctamente, el sistema muestra la versión de OpenXPKI instalada. Por ejemplo, **Version (core): 3.18.2**.

26 Cree la base de datos vacía y, a continuación, asigne el usuario de la base de datos mediante **mariadb -u root -p**.

Notas:

- Este comando debe escribirse en el cliente. De lo contrario, no podrá introducir la contraseña.

- Escriba la contraseña para MySQL. En este caso, **root** es el usuario MySQL.
- **openxpki** es el usuario en el que está instalado OpenXPKI.

```
CREATE DATABASE openxpki CHARSET utf8;
CREATE USER 'openxpki'@'localhost' IDENTIFIED BY 'openxpki';
GRANT ALL ON openxpki.* TO 'openxpki'@'localhost';
flush privileges;
```

Si el servicio MySQL no se está ejecutando, ejecute **/etc/init.d/mysql start** para iniciar el servicio.

27 Escriba **quit** para salir de MySQL.

28 Almacene las credenciales utilizadas en **/etc/openxpki/config.d/system/database.yaml**.

Contenido de archivo de ejemplo

```
main:
debug: 0
type: MariaDB
name: openxpki
host: localhost
port: 3306
user: openxpki
passwd: openxpki
```

Nota: Cambie **user** y **passwd** para que coincidan con el nombre de usuario y la contraseña de MariaDB.

29 Guarde el archivo.

30 Para un esquema de base de datos vacío, ejecute **zcat /usr/share/doc/libopenxpki-perl/examples/schema-mariadb.sql.gz | \ mysql -u root --password --database openxpki** desde el archivo de esquema proporcionado.

31 Introduzca la contraseña de la base de datos.

Configuración de la CA de OpenXPKI mediante el script predeterminado

Nota: El script predeterminado solo configura el dominio predeterminado, **ca-one**. El CDP y las CRL no se configuran.

1 Ejecute el script mediante **bash /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh**.

2 Confirme la configuración mediante **openxpkiadm alias --realm democa**.

Salida de ejemplo

```
=== functional token ===
scep (scep):
Alias    : scep-1
Identifier: YsBNZ7JYTbx89F_-Z4jn_RPFFWo
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2016-01-30 20:44:40

vault (datasafe):
Alias    : vault-1
Identifier: lZILS1l6Km5aIGS6pA7P7azAJic
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2016-01-30 20:44:40

ca-signer (certsign):
Alias    : ca-signer-1
Identifier: Sw_IY7AdoGUp28F_cFEdhbtI9pE
```

```
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2018-01-29 20:44:40

=== root ca ===
current root ca:
Alias     : root-1
Identifier: fVrqJAlpotPaisOAsnxa9cglXCc
NotBefore : 2015-01-30 20:44:39
NotAfter  : 2020-01-30 20:44:39

upcoming root ca:
  not set
```

3 Compruebe si la instalación se realiza correctamente mediante **openxpkictl start**.

Salida de ejemplo

```
Starting OpenXPKI...
OpenXPKI Server is running and accepting requests.
DONE.
```

4 Realice lo siguiente para acceder al servidor OpenXPKI:

a En un navegador web, escriba **http://ipaddress/openxpki/**.

b Agregue el nombre de usuario y sus contraseñas correspondientes en un archivo **userdb.yaml**. Para agregar el nombre de usuario y la contraseña, haga lo siguiente:

- Eche un vistazo a **/home/pkiadm** y, a continuación, a **nano userdb.yaml**.
- Pegue lo siguiente:

```
estRA:
       digest:"{ssha256}somePassword”
       role: RA Operator
```

Nota: En este caso, estRA hace referencia al nombre de usuario. Para generar la contraseña, escriba **openxpkiadm hashpwd**. Cuando aparezca un mensaje solicitando la contraseña y aparezca una contraseña cifrada ssha256, cópiela y péguela en el resumen de cualquier usuario.

Nota: Las funciones disponibles en el inicio de sesión del operador son Operador de RA, Operador de CA y usuario.

5 Introduzca el nombre de usuario y la contraseña.

6 Cree una solicitud de certificado y, a continuación, pruébela.

Configuración de la CA de OpenXPKI de forma manual

Descripción general

Nota: Antes de comenzar, asegúrese de que tiene conocimientos básicos sobre la creación de certificados OpenSSL.

Para configurar la CA OpenXPKI de forma manual, debe crear lo siguiente:

1 Certificado de la CA raíz. Para obtener más información, consulte “Creación de un certificado de la CA raíz” en la página 106.

2 Certificado del firmante de la CA, firmado por la CA raíz. Para obtener más información, consulte “Creación de un certificado de firmante” en la página 107.

3 Certificado de almacén de datos, autofirmado. Para obtener más información, consulte "Creación de un certificado de almacén" en la página 107.

4 Certificado web, firmado por el certificado del firmante. Para obtener más información, consulte "Configuración del servidor web" en la página 126.

Notas:

- Al seleccionar el hash de firma, utilice SHA256 o SHA512.
- El cambio del tamaño de la clave pública es opcional.

Para la versión 3.10 o posterior, puede administrar las claves directamente mediante el comando openxpkiadm alias:

- Ejecute **mkdir -p /etc/openxpki/local/keys** para crear el directorio. La ubicación predeterminada del directorio es **/etc/openxpki/local/keys**.
- Ejecute **openxpkictl start** para iniciar el servidor.

En este caso, vamos a utilizar el directorio **/etc/certs/openxpki_democa/** para la generación de certificados. Sin embargo, puede utilizar cualquier directorio.

Creación de un archivo de configuración de OpenSSL

El archivo de configuración OpenSSL contiene extensiones X.509 para generar y firmar solicitudes de certificado.

1 Ejecute el siguiente comando:

```
nano /etc/certs/openxpki_democa/openssl.conf
```

Nota: Si se puede acceder al servidor mediante el nombre de dominio completo (FQDN), utilice el DNS del servidor en lugar de su dirección IP.

Archivo de ejemplo

```
# x509_extensions               = v3_ca_extensions
# x509_extensions               = v3_issuing_extensions
# x509_extensions               = v3_datavault_extensions
# x509_extensions               = v3_scep_extensions
# x509_extensions               = v3_web_extensions
# x509_extensions               = v3_ca_reqexts # not for root self-signed, only for issuing
## x509_extensions              = v3_datavault_reqexts # not required self-signed
# x509_extensions               = v3_scep_reqexts
# x509_extensions               = v3_web_reqexts

[ req ]
default_bits            = 4096
distinguished_name      = req_distinguished_name

[ req_distinguished_name ]
domainComponent         = Domain Component
commonName              = Common Name

[ v3_ca_reqexts ]
subjectKeyIdentifier    = hash
keyUsage                = digitalSignature, keyCertSign, cRLSign

[ v3_datavault_reqexts ]
subjectKeyIdentifier    = hash
keyUsage                = keyEncipherment
extendedKeyUsage        = emailProtection

[ v3_scep_reqexts ]
subjectKeyIdentifier    = hash
```

```
[ v3_web_reqexts ]
subjectKeyIdentifier    = hash
keyUsage                = critical, digitalSignature, keyEncipherment
extendedKeyUsage        = serverAuth, clientAuth

[ v3_ca_extensions ]
subjectKeyIdentifier    = hash
keyUsage                = digitalSignature, keyCertSign, cRLSign
basicConstraints        = critical,CA:TRUE
authorityKeyIdentifier  = keyid:always,issuer

[ v3_issuing_extensions ]
subjectKeyIdentifier    = hash
keyUsage                = digitalSignature, keyCertSign, cRLSign
basicConstraints        = critical,CA:TRUE
authorityKeyIdentifier  = keyid:always,issuer:always
crlDistributionPoints   = URI:https://FQDN of your system/openxpki/CertEnroll/MYOPENXPKI.crl
authorityInfoAccess     = caIssuers;URI:https://FQDN of your system/download/MYOPENXPKI.crt

[ v3_datavault_extensions ]
subjectKeyIdentifier    = hash
keyUsage                = keyEncipherment
extendedKeyUsage        = emailProtection
basicConstraints        = CA:FALSE
authorityKeyIdentifier  = keyid:always,issuer

[ v3_scep_extensions ]
subjectKeyIdentifier    = hash
basicConstraints        = CA:FALSE
authorityKeyIdentifier  = keyid,issuer

[ v3_web_extensions ]
subjectKeyIdentifier    = hash
keyUsage                = critical, digitalSignature, keyEncipherment
extendedKeyUsage        = serverAuth, clientAuth
basicConstraints        = critical,CA:FALSE
subjectAltName          = DNS:FQDN of est server
crlDistributionPoints   = URI:https://FQDN of your
system/openxpki/CertEnroll/MYOPENXPKI_ISSUINGCA.cr
authorityInfoAccess     = caIssuers;URI:https://FQDN of your
system/download/MYOPENXPKI_ISSUINGCA.crt
```

2 Sustituya la dirección IP y el nombre del certificado CA por la información de configuración.

3 Guarde el archivo.

Creación de un archivo de contraseña para claves de certificado

1 Ejecute el siguiente comando:

nano /etc/certs/openxpki_democa/pd.pass

2 Escriba su contraseña.

3 Guarde el archivo.

Creación de un certificado de la CA raíz

Puede crear un certificado de la CA raíz autofirmado o generar una solicitud de certificado y, a continuación, obtenerlo firmado por la CA raíz.

Nota: Sustituya la longitud de clave, el algoritmo de firma y el nombre del certificado por los valores adecuados.

1. Ejecute el siguiente comando:

   ```
   openssl genrsa -out /etc/certs/openxpki_democa/ca-root-1.key -passout
   file:/etc/certs/openxpki_democa/pd.pass 4096
   ```

2. Sustituya el asunto de la solicitud por su información de la CA mediante **openssl req -new -key /etc/certs/openxpki_democa/ca-root-1.key -out /etc/certs/openxpki_democa/ca-root-1.csr**.

3. Obtenga el certificado firmado por la CA raíz utilizando **openssl req -config /etc/certs/openxpki_democa/openssl.conf -extensions v3_ca_extensions -x509 -days 3560 -in /etc/certs/openxpki_democa/ca-root-1.csr -key /etc/certs/openxpki_democa/ca-root-1.key -out /etc/certs/openxpki_democa/ca-root-1.crt - sha256**.

4. Vaya a **/etc/certs/openxpki_democa** donde se guarda **ca-root-1.crt**.

5. Ejecute el siguiente comando:

   ```
   openxpkiadm certificate import --file ca-root-1.crt
   ```

Creación de un certificado de firmante

Nota: Sustituya la longitud de clave, el algoritmo de firma y el nombre del certificado por los valores adecuados.

1. Ejecute el siguiente comando:

   ```
   openssl genrsa -out /etc/certs/openxpki_democa/ca-signer-1.key -passout
   file:/etc/certs/openxpki_democa/pd.pass 4096
   ```

2. Cambie el asunto de la solicitud con la información de CA mediante **openssl req -config /etc/certs/openxpki_democa/openssl.conf -reqexts v3_ca_reqexts -new -key /etc/certs/openxpki_democa/ca-signer-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=MYOPENXPKI_ISSUINGCA -out /etc/certs/openxpki_democa/ca-signer-1.csr**.

3. Obtenga el certificado firmado por la CA raíz mediante **openssl x509 -req -extfile /etc/certs/openxpki_democa/openssl.conf -extensions v3_issuing_extensions -days 3650 -in /etc/certs/openxpki_democa/ca-signer-1.csr -CA /etc/certs/openxpki_democa/ca-root-1.crt -CAkey /etc/certs/openxpki_democa/ca-root-1.key -CAcreateserial -out /etc/certs/openxpki_democa/ca-signer-1.crt -sha256**.

4. Ejecute el siguiente comando:

   ```
   openxpkiadm alias --realm democa --token certsign --file ca-signer-1.crt --
   key ca-signer-1.key
   ```

Creación de un certificado de almacén

Notas:

- El certificado de almacén se firma automáticamente.
- Sustituya la longitud de clave, el algoritmo de firma y el nombre del certificado por los valores adecuados.

1. Ejecute el siguiente comando:

   ```
   openssl req -new -x509 -keyout vault.key -out vault.crt -days 1100 -
   config /etc/certs/openxpki_democa/openssl.conf
   ```

2. Cambie el asunto de la solicitud con la información de CA mediante **openxpkiadm certificate import --file vault.crt**.

3. Ejecute el siguiente comando:

   ```
   openxpkiadm alias --realm democa --token datasafe --file vault.crt --key
   vault.key
   ```

   Nota: Proporcione los valores necesarios, pero mantenga **/CN=DataVault** como asunto.

Creación de un certificado web

1. Ejecute el siguiente comando:

   ```
   archivo openssl genrsa -out /etc/certs/openxpki_democa/web-1.key -
   passout:/etc/certs/openxpki_democa/pd.pass 4096
   ```

2. Cambie el asunto de la solicitud con la información de CA mediante **openssl req -config /etc/certs/openxpki_democa/openssl.conf -reqexts v3_web_reqexts -new -key /etc/certs/openxpki_democa/web-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=FQDN of your system -out /etc/certs/openxpki_democa/web-1.csr**.

3. Ejecute el siguiente comando:

   ```
   openssl x509 -req -extfile /etc/certs/openxpki_democa/openssl.conf -
   extensions v3_web_extensions -days 900 -
   in /etc/certs/openxpki_democa/web-1.csr -CA /etc/certs/openxpki_democa/ca-
   signer-1.crt -CAkey /etc/certs/openxpki_democa/ca-signer-1.key -
   CAcreateserial -out /etc/certs/openxpki_democa/web-1.crt -sha256
   ```

Configuración del servidor web

1. Ejecute los siguientes comandos:

   ```
   a2enmod ssl rewrite headers
   a2ensite openxpki
   a2dissite 000-default default-ssl
   mkdir -m755 -p /etc/openxpki/tls/chain
   cp /etc/certs/openxpki_democa/ca-root-1.crt /etc/openxpki/tls/chain/
   cp /etc/certs/openxpki_democa/ca-signer-1.crt /etc/openxpki/tls/chain/
   c_rehash /etc/openxpki/tls/chain/
   mkdir -m755 -p /etc/openxpki/tls/endentity
   ```

```
mkdir -m700 -p /etc/openxpki/tls/private
cp /etc/certs/openxpki_democa/web-1.crt /etc/openxpki/tls/endentity/openxp
ki.crt
cat /etc/certs/openxpki_democa/ca-signer-1.crt
>> /etc/openxpki/tls/endentity/openxpki.crt
archivo openssl rsa -in /etc/certs/openxpki_democa/web-1.key -
passin:/etc/certs/openxpki_democa/pd.pass -
out /etc/openxpki/tls/private/openxpki.pem
chmod 400 /etc/openxpki/tls/private/openxpki.pem
```

2 Reinicie el servicio Apache mediante **apache2 restart**.

3 Ejecute el siguiente comando para comprobar que la importación de los archivos se ha realizado correctamente:

```
openxpkiadm alias --realm democa
```

Salida de ejemplo

```
=== functional token ===
ca-signer (certsign):
          Alias     : ca-signer-2
          Identifier: XjC6MPbsnyfLZkI9Poi9vm4Z5rk
          NotBefore : 2022-04-06 10:03:01
          NotAfter  : 2032-04-03 10:03:01

vault (datasafe):
          Alias     : vault-2
          Identifier: G8ekluAsskGVC0N-jZhB2n9kvdM
          NotBefore : 2022-04-06 09:53:57
          NotAfter  : 2025-04-10 09:53:57

scep (scep):
          not set

ratoken (cmcra):
          not set

=== root ca ===
current root ca:
          Alias     : root-2
          Identifier: prTHU5vCfcJuCnQWyb5wUknvXQM
          NotBefore : 2022-04-06 09:40:27
          NotAfter  : 2032-01-04 09:40:27
```

Poner la contraseña de la clave de certificado a disposición de OpenXPKI

1 Cambie el valor en el archivo **nano /etc/openxpki/config.d/system/crypto.yaml**.

2 Quite los comentarios de la caché: **daemon under secret: default**:

```
secret:
  default:
    label: Global Secret group
    export: 0
    method: literal
    value: root
    cache: daemon
```

Inicio de OpenXPKI

1 Ejecute el comando **openxpkictl start**

Salida de ejemplo

```
Starting OpenXPKI...
OpenXPKI Server is running and accepting requests.
DONE.
```

2 Acceda al servidor de OpenXPKI:

a En un navegador web, escriba **http://ipaddress/openxpki/**.

b Agregue los nombres de usuario y las contraseñas correspondientes en un archivo **userdb.yaml**:

- Eche un vistazo a **/home/pkiadm** y **nano userdb.yaml**.
- Pegue lo siguiente:

```
estRA:
       digest:"{ssha256}somePassword”
       role: RA Operator
```

Nota: Aquí estRA hace referencia al nombre de usuario.

- Para generar la contraseña, escriba **openxpkiadm hashpwd**. Aparece un mensaje que muestra la contraseña y una contraseña cifrada con ssha256.
- Copie la contraseña y péguela en el resumen de cualquier usuario.

Nota: El inicio de sesión del operador tiene dos funciones preconfiguradas disponibles: Operador de RA, Operador de CA y usuario.

3 Introduzca el nombre de usuario y la contraseña.

4 Cree una solicitud de certificado y, a continuación, pruébela.

Generación de información de la CRL

Nota: Si se puede acceder al servidor mediante el FQDN, utilice el DNS del servidor en lugar de su dirección IP.

1 Detenga el servicio OpenXPKI mediante **openxpkictl stop**.

2 En **nano /etc/openxpki/config.d/realm/democa/publishing.yaml**, actualice la sección **connectors: cdp** para que muestre lo siguiente:

```
class: Connector::Builtin::File::Path
LOCATION: /var/www/openxpki/CertEnroll/
file: "[% ARGS.0 %].crl"
content: "[% pem %]"
```

a En **nano /etc/openxpki/config.d/realm/democa/profile/default.yaml**, actualice lo siguiente:

- **crl_distribution_points:** sección

```
critical: 0
uri:
    - https://FQDN of the est/openxkpi/CenrtEnroll/[% ISSUER.CN.0 %].crl
    - ldap://localhost/[% ISSUER.DN %]
```

- **authority_info_access:** sección

```
critical: 0
ca_issuers: http://FQDN of the est/download/MYOPENXPKI.crt
ocsp: http://ocsp.openxpki.org/
```

Cambie la dirección IP y el nombre del certificado de la CA de acuerdo con el servidor de la CA.

Nota: La ruta authority_info_access (AIA) se guarda en la carpeta Download, pero puede establecer la ubicación según sus preferencias.

b En **nano /etc/openxpki/config.d/realm/democa/crl/default.yaml**, realice lo siguiente:

- Si es necesario, actualice **nextupdate** y **renewal**.
- Agregue **ca_issuers** a la siguiente sección:

```
extensions:
            authority_info_access:
                    critical: 0
                    # ca_issuers and ocsp can be scalar or list
                    ca_issuers: https://FQDN of the est/download/MYOPENXPKI.crt
                   #ocsp: http://ocsp.openxpki.org/
```

Cambie la dirección IP y el nombre del certificado de la CA de acuerdo con el servidor de la CA.

3 Inicie el servicio OpenXPKI mediante **openxpkictl start**.

Publicación de información de la CRL

Después de crear las CRL, debe publicarlas para que todos puedan acceder a ellas.

1 Detenga el servicio Apache mediante **service apache2 stop**.

2 Cree un directorio **CertEnroll** para la CRL en el directorio **/var/www/openxpki/**.

3 Defina **openxpki** como propietario de este directorio y, a continuación, configure los permisos para permitir a Apache leer y ejecutar, y a otros servicios solo leer.

chown openxpki /var/www/openxpki/CertEnroll

chmod 755 /var/www/openxpki/CertEnroll

4 Agregue una referencia al archivo alias.conf de Apache mediante **nano /etc/apache2/mods-enabled/alias.conf**.

5 Después de la sección **<Directory "/usr/share/apache2/icons">**, agregue lo siguiente:

```
Alias /CertEnroll/ "/var/www/openxpki/CertEnroll/"
 <Directory "/var/www/openxpki/CertEnroll">
   Options FollowSymlinks
   AllowOverride None
   Require all granted
 </Directory>
```

6 Agregue una referencia en el archivo apache2.conf utilizando **nano /etc/apache2/apache2.conf**.

7 Agregue lo siguiente en la sección **Apache2 HTTPD server**:

```
<Directory /var/www/openxpki/CertEnroll>
  Options FollowSymlinks
  AllowOverride None
  Allow from all
</Directory>
```

8 Inicie el servicio Apache mediante **service apache2 start**.

Activación de la aprobación automática de solicitudes de certificado en la CA OpenXPKI

1. Detenga el servicio OpenXPKI mediante **`openxpkictl stop`**.
2. En **/etc/openxpki/config.d/realm/democa/est/default.yaml**, actualice la sección **`eligible:`** :

Contenido antiguo

```
eligible:
            initial:
                value@: connector:scep.generic.connector.initial
               args: '[% context.cert_subject_parts.CN.0 %]'
               expect:
                   - Build
                   - New
```

Nuevo contenido

```
eligible:
            initial:
                value: 1
                # value@: connector:scep.generic.connector.initial
                # args: '[% context.cert_subject_parts.CN.0 %]'
                # expect:
                #    - Build
                #    - New
```

Notas:

- Revise el espacio y la sangría en el archivo de script.
- Para aprobar certificados de forma manual, comente **`value: 1`** y, a continuación, quite el comentario de las otras líneas que se hayan comentado previamente.

3. Guarde el archivo.
4. Inicie el servicio OpenXPKI mediante **`openxpkictl start`**.

Cambio de detalles para habilitar la descarga de certificados CA

1. Ejecute el siguiente comando:

   `/usr/lib/cgi-bin/est.fcgi`

2. Sustituya **`my $mime = "application/pkcs7-mime; smime-type=certs-only";`** por **`my $mime = "application/pkcs7-mime";`**.
3. Inicie el servicio OpenXPKI mediante **`openxpkictl start`**.

Creación de un segundo dominio

En OpenXPKI, puede configurar varias estructuras PKI en el mismo sistema. En los temas siguientes se muestra cómo crear otro dominio para MVE con el nombre **democa-two**.

Copia y configuración del directorio

1. Cree un directorio, a saber **democa2**, para el segundo dominio dentro **de /etc/openxpki/config.d/realm**.
2. Copie el árbol de directorios de ejemplo **/etc/openxpki/config.d/realm/ca-one** en un nuevo directorio (**cp -r /etc/openxpki/config.d/realm.tpl/*/etc/openxpki/config.d/realm/democa2**) dentro del directorio del dominio.
3. En **/etc/openxpki/config.d/system/reinos.yaml**, actualice la siguiente sección:

Contenido antiguo

```
# This is the list of realms in this PKI
# You only need to enable the realms which are visible on the server

democa:
    label: Verbose name of this realm
    baseurl: https://pki.example.com/openxpki/

#democa2:
#    label: Verbose name of this realm
#    baseurl: https://pki.acme.org/openxpki/
```

Nuevo contenido

```
# This is the list of realms in this PKI
# You only need to enable the realms which are visible on the server

democa:
    label: Example.org Demo CA
    baseurl: https://pki.example.com/openxpki/

democa2:
    label: Example.org Demo CA2
    baseurl: https://pki.example.com/openxpki/
```

4. Guarde el archivo.

Configuración de puntos finales EST para varios dominios

Puede configurar el punto final EST con una tupla compuesta por la parte de autoridad del URI y la etiqueta opcional (por ejemplo, www.ejemplo.com:80 y arbitraryLabel1). En las siguientes instrucciones, utilizamos dos dominios PKI, **`democa`** y **`democa2`**.

1. Copie el archivo de configuración predeterminado en **cp /etc/openxpki/est/default.conf /etc/openxpki/est/democa.conf**.

   Nota: Asigne al archivo el nombre **`democa.conf`**.

2. En **nano /etc/openxpki/est/democa.conf**, cambie el valor de dominio a **`realm=democa`**.

   Nota: De acuerdo a sus necesidades, puede que tenga que quitar los comentarios de las líneas correspondientes para las secciones **simpleenroll**, **simplereenroll**, **csrattrs** y **cacerts**. Mantenga comentadas las secciones de entorno. Haga lo mismo para **default.conf**.

3 Cree otro archivo de configuración en **cp /etc/openxpki/est/default.conf /etc/openxpki/est/democa2.conf**.

Nota: Asigne al archivo el nombre **`democa2.conf`**.

4 En **nano /etc/openxpki/est/democa2.conf**, cambie el valor de dominio a **`realm=democa2`**.

Nota: De acuerdo a sus necesidades, puede que tenga que quitar los comentarios de las líneas correspondientes para las secciones **simpleenroll**, **simplereenroll**, **csrattrs** y **cacerts**. Mantenga comentadas las secciones de entorno.

5 Copie el archivo **default.yaml** en las siguientes ubicaciones:

- **cp /etc/openxpki/config.d/realm/democa/est/default.yaml**
- **/etc/openxpki/config.d/realm/democa/est/democa.yaml**

Nota: Asigne al archivo el nombre **`democa.yaml`**.

6 Copie el archivo **default.yaml** en las siguientes ubicaciones:

- **cp /etc/openxpki/config.d/realm/democa2/est/default.yaml**
- **/etc/openxpki/config.d/realm/democa2/est/democa2.yaml**

Nota: Asigne al archivo el nombre **`democa2.yaml`**.

7 Reinicie el servicio OpenXPKI mediante **`openxpkictl restart`**.

Seleccione las siguientes URL para abrir el servidor de la EST correspondiente a un dominio a través de un navegador web:

- **`democa`**—**http://ipaddress/est/democa**
- **`democa2`**—**http://ipaddress/est/democa2**

Si desea diferenciar entre credenciales de inicio de sesión y plantillas de certificado predeterminadas para diferentes dominios PKI, puede que necesite una configuración avanzada.

Creación de un certificado de firmante

Las siguientes instrucciones muestran cómo generar un certificado de firmante en el segundo dominio. Puede utilizar los mismos certificados raíz y de almacén que los del primer dominio.

1 Cree un archivo de configuración OpenSSL en **nano /etc/certs/openxpki_democa2/openssl.conf**.

Nota: Cambie el nombre común del certificado para que el usuario pueda distinguir fácilmente entre distintos certificados para diferentes dominios. Los archivos de certificado se crean en el directorio **/etc/certs/openxpki_democa2/**.

2 Vaya al directorio del certificado del almacén en el primer dominio y, a continuación, importe el certificado desde el primer dominio.

3 Ejecute el siguiente código:

```
openxpkiadm alias --realm democa2 --token datasafe --file vault.crt
```

Creación de un archivo de contraseña para claves de certificado

1 Ejecute el siguiente comando:

```
nano /etc/certs/openxpki_democa2/pd.pass
```

2 Escriba su contraseña.

3 Cree un certificado de firmante. Para obtener más información, consulte "Creación de un certificado de firmante" en la página 107.

4 Compruebe que la importación se realiza correctamente mediante **openxpkiadm alias --realm democa2**.

Nota: Si cambió la contraseña de clave del certificado durante la creación del certificado, actualice **nano /etc/openxpki/config.d/realm/democa2/crypto.yaml**.

5 Genere las CRL para el segundo dominio. Para obtener más información, consulte "Generación de información de la CRL" en la página 110.

Nota: Asegúrese de utilizar el nombre de certificado CA correcto según el dominio.

6 Publique las CRL para este dominio. Para obtener más información, consulte "Publicación de información de la CRL" en la página 129.

7 Reinicie el servicio OpenXPKI mediante **openxpkictl restart**.

Salida de ejemplo

```
Stopping OpenXPKI
Stopping gracefully, 3 (sub)processes remaining...
DONE.
Starting OpenXPKI...
OpenXPKI Server is running and accepting requests.
DONE.
```

Activación de varios certificados activos con el mismo asunto para que estén presentes a la vez

De forma predeterminada, en OpenXPKI sólo puede estar activo un certificado con el mismo nombre de asunto a la vez. Sin embargo, cuando se aplican varios certificados con nombre, deben estar presentes varios certificados activos con el mismo nombre de asunto a la vez.

1 En **/etc/openxpki/config.d/realm/REALM NAME/est/< REALM NAME >.yaml**, en la sección **`policy`**, cambie el valor de **`max_active_certs`** de **`1`** a **`0`**.

Notas:

- REALM NAME es el nombre de dominio. Por ejemplo, **ca-one**.
- Revise el espacio y la sangría en el archivo de script.

2 Reinicie el servicio OpenXPKI mediante **`openxpkictl restart`**.

Definición del número de puerto predeterminado para la CA OpenXPKI

De forma predeterminada, Apache escucha en el número de puerto 443 para https. Defina el número de puerto predeterminado para la CA OpenXPKI para evitar conflictos.

1 En **/etc/apache2/ports.conf**, modifique el puerto 443 a cualquier otro puerto. Por ejemplo:

Contenido antiguo

```
Listen 80

<IfModule ssl_module>
   Listen 443
</IfModule>

<IfModule mod_gnutls.c>
```

```
  Listen 443
</IfModule>
```

Nuevo contenido

```
Listen 80

<IfModule ssl_module>
   Listen 9443
</IfModule>

<IfModule mod_gnutls.c>
  Listen 9443
</IfModule>
```

2. En **/etc/apache2/sites-available/openxpki.conf**, agregue o modifique la sección **`VirtualHost`** para asignar un nuevo puerto. Por ejemplo, **`<VirtualHost *:443>`** a **`<VirtualHost *:9443>`**.
3. En **/etc/apache2/sites-available/default-ssl.conf**, agregue o modifique la sección **`VirtualHost`** para asignar un nuevo puerto. Por ejemplo, cambie **`<VirtualHost *:443>`** a **`<VirtualHost *:9443>`**.
4. Reinicie el servidor Apache con **`systemctl restart apache2`**.

   Nota: Si solicita la frase de contraseña para **SSL/TLS**, escriba la contraseña mientras agrega el certificado del servidor web TLS en el servidor EST.
5. En **tinddopenxpkiweb01.dhcp.dev.lexmark.com:9443 (RSA):**, introduzca la frase de contraseña para las claves **SSL/TLS**.

Para comprobar el estado, ejecute **`netstat -tlpn| grep apache`**. La URL de OpenXPKI SCEP es ahora **https://ipaddress** y la URL web es **FQDN:9443/openxpki**.

Activación de la autenticación básica

1. Ejecute el siguiente comando:

   `apt -y install apache2-utils`
2. Cree una cuenta de usuario que tenga acceso al servidor. Introduzca la siguiente información:

   ```
   htpasswd -c /etc/apache2/.htpasswd <username>
                  New password:
                  Re-type new password:
                  Adding password for user <username>
   ```
3. Vaya al directorio **`cd /etc/apache2/sites-enabled/`**.
4. En **nano openxpki.conf**, agregue las siguientes líneas en **`<VirtualHost *: 443 block>`**:

   ```
   #HTTPS BASIC AUTH FOR LABELS
   Location /.well-known/est/*/simpleenroll
       AuthType Basic
       AuthName "estrealm"
       AuthUserFile /etc/apache2/.htpasswd
       require valid-user
       </Location>
       #HTTPS BASIC AUTH FOR NO LABEL
       <Location /.well-known/est/simpleenroll>
       AuthType Basic
       AuthName "estrealm"
       AuthUserFile /etc/apache2/.htpasswd
       require valid-user
       </Location>
   ```

5 Agregue **`ErrorDocument 401 %{unescape:%00}`** antes de **SSLEngine** en el mismo bloque de host virtual.

Ejemplo

```
ServerAlias *
DocumentRoot /var/www/
ErrorDocument 401 %{unescape:%00}
SSLEngine On
```

6 Inicie el **apache2** con **service apache2 start**.

Nota: La autenticación básica funciona con el nombre de usuario y la contraseña anteriores.

Activación de la autenticación de certificado de cliente

1 Vaya al siguiente directorio: **`cd /etc/apache2/sites-enabled/`**.

2 Para el host requerido en **nano openxpki.conf**, agregue **SSLVerifyClient require**.

Por ejemplo, si está utilizando el puerto 443, modifique la sección **VirtualHost** a:

```
<VirtualHost *:443>
SSLVerifyClient require
</VirtualHost>
```

3 Elimine el comando **SSLVerifyClient optional_no_ca**.

4 Guarde el archivo y, a continuación, escriba **`quit`** para salir de MySQL.

5 Vaya al siguiente directorio: **`cd /etc/openxpki/config.d/realm/democa/est`**.

6 Abra **default.yaml** y **democa.yaml**.

Nota: Si la etiqueta es diferente, cambie el archivo YAML.

7 Ejecute el siguiente comando:

```
vi default.yaml
```

8 En la sección **authorized_signer**, agregue lo siguiente:

```
authorized_signer:
rule2:
            subject: CN=,.
```

Por ejemplo, si el nombre del asunto del certificado de cliente es **test123**, agregue lo siguiente en la sección **`authorized_signer`**:

```
authorized_signer:
rule1:
        # Full DN
        subject: CN=.+:pkiclient,.
rule2:
        subject: CN=test123,.*
```

9 Guarde el archivo y, a continuación, escriba **`quit`** para salir de MySQL.

10 Reinicie el servicio OpenXPKI mediante **`openxpkictl restart`**.

11 Inicie el servicio Apache mediante **`service apache2 restart`**.

¿Qué causa el error de falta de coincidencia de SAN que impide que el sistema busque la CRL?

El error de falta de coincidencia de SAN puede ocurrir cuando se activa la información de CRL. Este error indica que la dirección IP o el nombre de host no coinciden con el valor de SAN del certificado web. Para evitar que se produzca este error, utilice el FQDN en la ruta de acceso de la CRL en lugar de la IP. También puede configurar el certificado web y utilizar el FQDN del sistema en el campo SAN.

¿Por qué están sin conexión los tokens ca-signer-1 y vault-1?

Si la página Estado del sistema muestra que los tokens ca-signer-1 y vault-1 están sin conexión, haga lo siguiente:

1. En **/etc/openxpki/config.d/realm/realm name/crypto.yaml**, cambie el valor de la clave correspondiente.
2. Reinicie el servicio de OpenXPKI.

Administración de alertas de impresora

Descripción general

Las alertas se activan cuando hay una impresora que requiere atención. Las acciones le permiten enviar correos electrónicos personalizados o ejecutar scripts cuando se produce una alerta. Los eventos definen las acciones que se ejecutan cuando las alertas específicas están activas. Para registrar alertas de una impresora, cree acciones y asócielas a un evento. Asigne el evento a las impresoras que desee controlar.

Nota: Esta función no se aplica a las impresoras protegidas.

Creación de una acción

Una acción es una notificación por correo electrónico o un registro del visor de eventos. Las acciones asignadas a los eventos se activan cuando aparece una alerta de impresora.

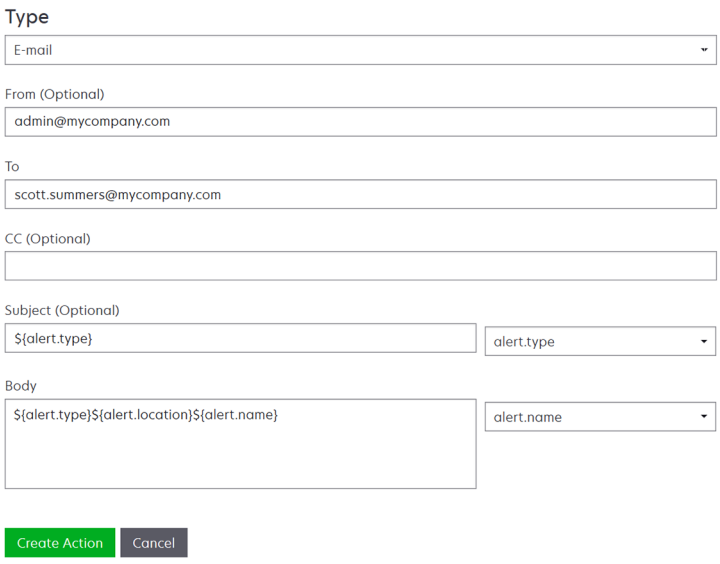
1. En el menú Impresoras, haga clic en **Eventos y acciones** > **Acciones** > **Crear**.
2. Escriba un nombre exclusivo para la acción y su descripción.
3. Seleccione un tipo de acción.

Correo electrónico

Nota: Antes de empezar, asegúrese de que los ajustes del correo electrónico están configurados. Para obtener más información, consulte "Configuración de los valores del correo electrónico" en la página 149.

a. En el menú Tipo, seleccione **Correo electrónico**.

b. Introduzca los valores apropiados en los campos. También puede utilizar los marcadores disponibles como la totalidad o parte del título del asunto, o como parte de un mensaje de correo electrónico. Para obtener más información, consulte "Descripción de los marcadores de posición de acción" en la página 138.

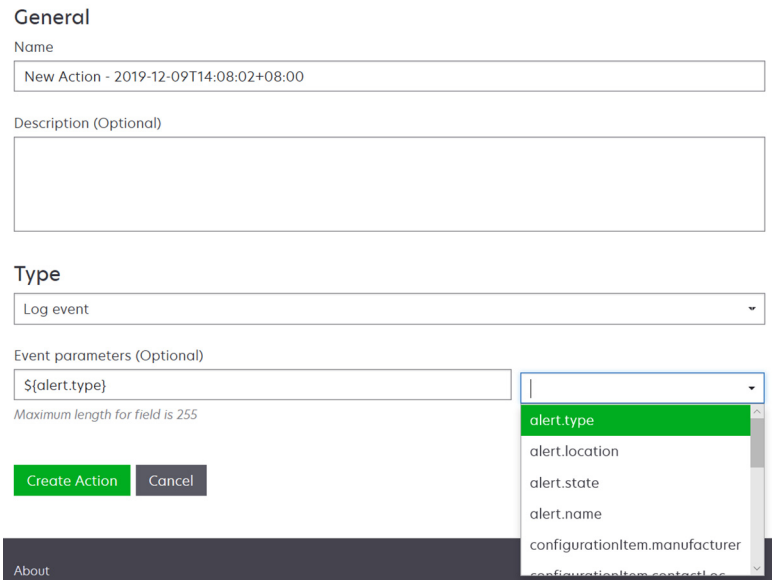


c Haga clic en **Crear acción**.

Registrar evento

a En el menú Tipo, seleccione **Registrar evento**.

b Escriba los parámetros del evento. También puede utilizar los marcadores de posición disponibles en el menú desplegable. Para obtener más información, consulte "Descripción de los marcadores de posición de acción" en la página 138.



c Haga clic en **Crear acción**.

Descripción de los marcadores de posición de acción

Utilice los marcadores disponibles en el título del asunto o el mensaje de correo electrónico. Los marcadores de posición representan elementos variables y se sustituyen por valores reales cuando se utilizan.

- **${eventHandler.timestamp}**—La fecha y la hora en que se MVE ha procesado el evento. Por ejemplo, **14 de marzo de 2017 1:42:24 PM**.
- **${eventHandler.name}**—El nombre del evento.
- **${configurationItem.name}**—El nombre del sistema de la impresora que ha desencadenado la alerta.
- **${configurationItem.address}**—La dirección MAC de la impresora que ha desencadenado la alerta.
- **${configurationItem.ipAddress}**—La dirección IP de la impresora que ha desencadenado la alerta.
- **${configurationItem.ipHostname}**—El nombre de host de la impresora que ha desencadenado la alerta.
- **${configurationItem.model}**—El nombre de modelo de la impresora que ha desencadenado la alerta.
- **${configurationItem.serialNumber}**—El número de serie de la impresora que ha desencadenado la alerta.
- **${configurationItem.propertyTag}**—La etiqueta de propiedad de la impresora que ha desencadenado la alerta.
- **${configurationItem.contactName}**—El nombre de contacto de la impresora que ha desencadenado la alerta.
- **${configurationItem.contactLocation}**—La ubicación de contacto de la impresora que ha desencadenado la alerta.

- **${configurationItem.Manufacturer}**—El fabricante de la impresora que ha desencadenado la alerta.
- **${alert.name}**—El nombre de la alerta que se ha activado.
- **${alert.state}**—El estado de la alerta. Puede estar activa o borrada.
- **${alert.location}**—La ubicación dentro de la impresora donde se ha producido la alerta activada.
- **${alert.Escriba}**—La gravedad de la alerta activada, como **`Advertencia`** o **`Se necesita intervención`**.

Administración de acciones

1. En el menú Impresoras, haga clic en **Eventos y acciones** > **Acciones**.
2. Haga lo siguiente:

Editar una acción

a. Seleccione una acción y haga clic en **Editar**.
b. Configure los valores.
c. Haga clic en **Guardar cambios**.

Eliminar acciones

a. Seleccione una o más acciones.
b. Haga clic en **Eliminar**y, a continuación, confirme la eliminación.

Probar una acción

a. Seleccione una acción y, a continuación, haga clic en **Probar**.
b. Para verificar los resultados, consulte los registros de tareas.

Notas:

- Para obtener más información, consulte “Visualización de archivos de registro” en la página 145.
- Si va a probar una acción de correo electrónico, a continuación, compruebe si el correo electrónico se ha enviado al destinatario.

Creación de un evento

Puede controlar alertas en su grupo de impresoras. Cree un evento y, a continuación, defina una acción para que se ejecute cuando se produzcan las alertas especificadas. Los eventos no se admiten en las impresoras protegidas.

1. En el menú Impresoras, haga clic en **Eventos y acciones** > **Eventos** > **Crear**.
2. Introduzca un nombre exclusivo para el evento y su descripción.
3. En la sección Alertas, seleccione una o más alertas. Para obtener más información, consulte “Descripción de las alertas de impresora” en la página 140.
4. En la sección Acciones, seleccione una o más acciones para ejecutar cuando se activen las alertas seleccionadas.

   Nota: Para obtener más información, consulte “Creación de una acción” en la página 137.

5 Active el sistema para ejecutar las acciones seleccionadas cuando las alertas se desactiven en la impresora.

6 Establezca un periodo de gracia antes de ejecutar las acciones seleccionadas.

Nota: Si se elimina la alerta durante el período de gracia, no se ejecutará la acción.

7 Haga clic en **Crear evento**.

Descripción de las alertas de impresora

Las alertas se activan cuando hay una impresora que requiere atención. Las siguientes alertas se pueden asociar a un evento en MVE:

- **Atasco del Alimentador automático de documentos (ADF) atasco**—Se ha producido un atasco de papel en el ADF y tiene que retirarse físicamente.
  - Atasco de la salida del ADF del escáner
  - Atasco del alimentador del ADF del escáner
  - Atasco del inversor del ADF del escáner
  - Papel eliminado del ADF del escáner
  - Falta papel en el ADF del escáner
  - Atasco del prerregistro del ADF del escáner
  - Atasco del registro del ADF del escáner
  - Alerta de escáner- Reemplace todos los originales si reinicia el trabajo
- **Puerta o cubierta abierta**—Hay una puerta abierta en la impresora y debe cerrarse.
  - Comprobar puerta/cubierta - buzón
  - Puerta abierta
  - Alerta de cubierta
  - Cubierta cerrada
  - Cubierta abierta
  - Cubierta abierta o falta cartucho
  - Cubierta del dúplex abierta
  - Cubierta del ADF del escáner abierta
  - Atasco de escáner Cubierta de acceso abierta
- **Tamaño o tipo de soporte incorrecto**—Se está imprimiendo un trabajo que requiere que se cargue un papel determinado en la bandeja.
  - Tamaño de sobre incorrecto
  - Alimentación manual incorrecta
  - Papel incorrecto
  - Tamaño de papel incorrecto
  - Cargar papel
- **Memoria llena o error**—Se está agotando la memoria de la impresora y se tienen que aplicar cambios.
  - Página compleja
  - Los archivos se eliminarán
  - Memoria clasif. insuficiente
  - Memoria para defragmentar insuficiente

  - Memoria de fax insuficiente
  - Memoria insuficiente
  - Memoria insuficiente: puede que se pierdan los trabajos retenidos
  - Memoria insuficiente para guardar recursos
  - Memoria llena
  - Escasez de memoria PS
  - Demasiadas páginas en el escáner - escáner cancelado
  - Reducción de la resolución
- **Funcionamiento incorrecto de la opción**—Una opción asociada a la impresora se encuentra en estado de error. Las opciones incluyen opciones de entrada, opciones de salida, tarjetas de fuente, tarjetas Flash de usuario, discos y clasificadores.
  - Comprobar alineación/conexión
  - Comprobar conex. del dúplex
  - Comprobar instalación de clasificador/buzón
  - Comprobar alimentación
  - Opción dañada
  - Opción defectuosa
  - Retirar dispositivo
  - Alerta de dúplex
  - Falta bandeja dúplex
  - Adaptador de red externo desconectado
  - Alerta de clasificador
  - Puerta del clasificador o interbloqueo abiertos
  - Placa para el papel del clasificador abierta
  - Dispositivo dúplex incompatible
  - Dispositivo de entrada incompatible
  - Dispositivo de salida incompatible
  - Dispositivo desconocido incompatible
  - Instalación de opción incorrecta
  - Alerta de entrada
  - Error de configuración de bandeja de entrada
  - Alerta de opción
  - Bandeja de salida llena
  - Bandeja de salida casi llena
  - Error de configuración de salida
  - Opción llena
  - Falta la opción
  - Falta mecanismo de alimentación de papel
  - Imprimir trabajos con la opción
  - Reinstalar dispositivo
  - Reinstalar dispositivo de salida

  - Demasiadas entradas instaladas
  - Demasiadas opciones instaladas
  - Demasiadas salidas instaladas
  - Falta la bandeja
  - Falta la bandeja durante encendido
  - Error de sensor de bandeja
  - Entrada no calibrada
  - Opción no formateada
  - Opción no admitida
  - Reinstalar dispositivo de entrada
- **Atasco de papel**—Se ha producido un atasco de papel en la impresora y se tiene que retirar físicamente.
  - Atasco de papel interno
  - Alerta de atasco
  - Atasco de papel
- **Error del escáner**—El escáner tiene un problema.
  - Cable trasero del escáner desenchufado
  - El carro del escáner está bloqueado
  - Limpieza del cristal de la superficie y de la cinta de soporte del escáner
  - Escáner desactivado
  - Cubierta de la superficie del escáner abierta
  - Cable frontal del escáner desenchufado
  - Registro de escáner no válido
- **Error de suministros**—Un suministro de la impresora tiene un problema.
  - Suministro incorrecto
  - La región del cartucho no coincide
  - Suministro defectuoso
  - Faltan la unidad de fusor o el rodillo de aplicación
  - Falta el cartucho izquierdo, o bien, no es válido
  - Falta el cartucho derecho, o bien, no es válido
  - Suministro no válido
  - Fallo importante
  - Alerta de suministro
  - Atasco de suministros
  - Falta suministro
  - Se ha tirado de la palanca de extracción del cartucho de tóner
  - El cartucho de tóner no se ha instalado correctamente
  - Suministro no calibrado
  - Suministro sin licencia
  - Suministro no admitido

- **Suministros o consumibles vacíos**—Un suministro de la impresora tiene que ser sustituido.
  - Entrada vacía
  - Duración agotada
  - Impresora lista para mantenimiento
  - Mantenimiento programado
  - Suministro vacío
  - Suministro lleno
  - Suministro lleno o falta

  Nota: La impresora envía la alerta como error y como advertencia. Si se activa alguna de estas alertas, la acción que tiene asociada se realiza dos veces.
- **Suministros o consumibles bajos**—Un suministro de la impresora se está agotando.
  - Aviso temprano
  - Primero inferior
  - Entrada baja
  - Agotándose
  - Casi vacío
  - Casi bajo
  - Suministro bajo
  - Suministro casi lleno
- **Alerta o condición no clasificada**
  - Error de calibración de color
  - Error de transmisión de datos
  - Fallo de CRC de motor
  - Alerta externa
  - Pérdida de conexión de fax
  - Ventilador detenido
  - Hex. activo
  - Inserte páginas dúplex y pulse Continuar
  - Alerta interna
  - El adaptador de red interno requiere mantenimiento
  - Alerta de unidad lógica
  - Sin conexión
  - Sin conexión para el indicador de advertencia
  - Se ha producido un error en la operación
  - Alerta de intervención del operador
  - Error de página
  - Alerta de puerto
  - Error de comunicación de puerto
  - Puerto desactivado
  - Ahorro energía
  - Apagando

- Tiempo de espera del trabajo PS
- Tiempo de espera manual PS
- Instalación requerida
- Error de totales de validación de SIMM
- Calibración de suministro
- Fallo del sensor de parches de tóner
- Condición de alerta desconocida
- Configuración desconocida
- Condición de alerta de escáner desconocida
- Usuario(s) bloqueado(s)
- Alerta de advertencia

Administración de eventos

1. En el menú Impresoras, haga clic en **Eventos y acciones** > **Eventos**.
2. Realice una de las siguientes acciones:

Editar un evento

a. Seleccione un evento y haga clic en **Editar**.
b. Configure los valores.
c. Haga clic en **Guardar cambios**.

Eliminar eventos

a. Seleccione uno o más eventos.
b. Haga clic en **Eliminar**y, a continuación, confirme la eliminación.

Visualización del estado y el historial de las tareas

Descripción general

Las tareas son cualquier actividad de administración de impresoras realizadas en MVE, tales como la búsqueda de impresoras, auditorías y la ejecución de las configuraciones. La página Estado muestra el estado de todas las tareas que se están ejecutando actualmente y las tareas ejecutadas en las últimas 72 horas. La información sobre las tareas que se están ejecutando actualmente se introduce en el registro. Las tareas anteriores a 72 horas solo se pueden ver como entradas de registro individuales en la página Registro, y se pueden buscar utilizando los identificadores de tarea.

Visualización del estado de la tarea

En el menú Tareas, haga clic en **Estado**.

Nota: El estado de la tarea se actualiza en tiempo real.

Detención de tareas

1. En el menú Tareas, haga clic en **Estado**.
2. En la sección Tareas en ejecución, seleccione uno o más tareas.
3. Haga clic en **Parar**.

Visualización de archivos de registro

1. En el menú Tareas, haga clic en **Registros**.
2. Seleccione las categorías de tareas, los tipos de tareas o un período de tiempo.

   Notas:

   - Utilice el campo de búsqueda para buscar varias ID de tareas. Utilice comas para separar varias ID de tareas o un guión para indicar un intervalo. Por ejemplo, **`11, 23, 30-35`**.
   - Para exportar los resultados de la búsqueda, haga clic en **Exportar a CSV**.

Borrado de registros

1. En el menú Tareas, haga clic en **Registro**.
2. Haga clic en **Borrar registro** y, a continuación, seleccione una fecha.
3. Haga clic en **Borrar registro**.

Exportación de registros

1. En el menú Tareas , haga clic en **Registro**.
2. Seleccione las categorías de tareas, los tipos de tareas o un período de tiempo.
3. Haga clic en **Exportar a CSV**.

Programación de tareas

Creación de un programa

1. En el menú Tareas, haga clic en **Programar** > **Crear**.
2. En la sección General, escriba un nombre exclusivo para las tareas programadas y su descripción.
3. En la sección Tareas, realice una de las siguientes acciones:

Programar una auditoría

a. Seleccione una **Auditoría**.
b. Seleccione una búsqueda guardada.

Programar una comprobación de conformidad

a. Seleccione el grado de **Conformidad**.
b. Seleccione una búsqueda guardada.

Programar una comprobación del estado de una impresora

a. Seleccione **Estado actual**.
b. Seleccione una búsqueda guardada.
c. Seleccione una acción.

Programar una implementación de configuración

a. Seleccione **Implementar archivo**.
b. Seleccione una búsqueda guardada.
c. Busque el archivo y, a continuación, seleccione el tipo de archivo.
d. Si es necesario, seleccione un método de implementación o protocolo.

Programar una búsqueda

a. Seleccione **Búsqueda**.
b. Seleccione un perfil de búsqueda.

Programar una aplicación de configuración

a. Seleccione **Aplicación**.
b. Seleccione una búsqueda guardada.

Programar una validación de certificado

Seleccione **Validar certificado**.

Nota: Durante la validación, MVE se comunica con el servidor de la CA para descargar la cadena de certificados y la lista de revocación de certificados (CRL). También se genera el certificado de agente de inscripción. Este certificado permite al servidor de la CA confiar en MVE.

Programar una exportación de visualización

a Seleccione **Ver exportación**.

b Seleccione una búsqueda guardada.

c Seleccione una plantilla de visualización.

d Escriba la lista de direcciones de correo electrónico donde se envían los archivos exportados.

4 En la sección Programar, establezca la fecha, la hora y la frecuencia de la tarea.

5 Haga clic en **Crear una tarea programada**.

Administración de tareas programadas

1 En el menú Tareas , haga clic en **Programa**.

2 Realice una de las siguientes acciones:

Editar una tarea programada

a Seleccione una tarea y haga clic en **Editar**.

b Configure los valores.

c Haga clic en **Editar tarea programada**.

Nota: La información sobre la última ejecución se elimina cuando se edita una tarea programada.

Eliminar una tarea programada

a Seleccione una tarea y haga clic en **Eliminar**.

b Haga clic en **Eliminar tarea programada**.

Realización de otras tareas administrativas

Configuración de los valores generales

1. Haga clic en la esquina superior derecha de la página.
2. Haga clic en **General** y, a continuación, seleccione una fuente de nombre de host.
   - **Impresora**—El sistema recupera el nombre de host de la impresora.
   - **Búsqueda DNS inversa**—El sistema recupera el nombre de host de la tabla DNS mediante la dirección IP.
3. Establezca la frecuencia de nuevo registro de la alerta.

   Nota: Las impresoras pueden perder el estado de registro de alertas cuando se realizan cambios como, por ejemplo, reiniciar o actualizar el firmware. MVE intenta recuperar el estado automáticamente en el siguiente intervalo establecido de la frecuencia de nuevo registro de alertas.
4. Haga clic en **Guardar cambios**.

Configuración de los valores del correo electrónico

Active la configuración de SMTP para que MVE pueda enviar archivos de exportación de datos y notificaciones de eventos mediante correo electrónico.

1. Haga clic en , en la esquina superior derecha de la página.
2. Haga clic en **Correo electrónico** y, a continuación, seleccione **Habilitar configuración SMTP de correo electrónico**.
3. Escriba el servidor de correo electrónico SMTP y el puerto.
4. Seleccione el cifrado adecuado.

   Notas:

   - Para el cifrado SSL, seleccione el puerto 465.
   - Para el cifrado TLS/STARTTLS, seleccione el puerto 587.
5. Escriba la dirección de correo electrónico del remitente.
6. Si un usuario se tiene que conectar antes de enviar correos electrónicos, seleccione **Inicio de sesión obligatorio** y, a continuación, introduzca las credenciales del usuario.
7. Haga clic en **Guardar cambios**.

Adición de una renuncia de responsabilidad de inicio de sesión

Puede configurar una renuncia de responsabilidad de inicio de sesión que se muestre cuando los usuarios se conecten con una nueva sesión. Los usuarios deben aceptar la renuncia de responsabilidad antes de acceder a MVE.

1. Haga clic en la esquina superior derecha de la página.
2. Haga clic en **Renuncia de responsabilidad** y, a continuación, seleccione **Activar renuncia de responsabilidad antes de iniciar sesión**.
3. Escriba el texto de renuncia de responsabilidad.
4. Haga clic en **Guardar cambios**.

Firma del certificado MVE

Secure Socket Layer (SSL) o Transport Layer Security (TLS) es un protocolo de seguridad que utiliza el cifrado de datos y la autenticación de certificados para proteger la comunicación servidor-cliente. En MVE, se utiliza TLS para proteger la información confidencial que se comparte entre el servidor MVE y el navegador web. La información protegida puede comprender contraseñas de impresora, políticas de seguridad, credenciales de usuario de MVE o información de autenticación de la impresora, como LDAP o Kerberos.

TLS permite al servidor MVE y el navegador web cifrar los datos antes de enviarlos y descifrarlos luego tras su recepción. SSL también requiere que el servidor presente un certificado que demuestre su identidad ante el navegador web. Este certificado se firma automáticamente o mediante una autoridad de certificación externa de confianza. De forma predeterminada, MVE está configurado para utilizar un certificado firmado automáticamente.

1. Descargue la solicitud de firma del certificado.
   a. Haga clic en , en la esquina superior derecha de la página.
   b. Haga clic en **TLS** > **Descargar**.
   c. Seleccione **Solicitud de firma de certificado**.

   Nota: La solicitud de firma de certificado incluye nombres alternativos de sujeto (SAN).
2. Utilice una autoridad de certificación de confianza para firmar la solicitud de certificado.
3. Instale el certificado firmado por la autoridad de certificación.
   a. Haga clic en , en la esquina superior derecha de la página.
   b. Haga clic en **TLS** > **Instalar certificado firmado**.
   c. Cargue el certificado firmado de la autoridad de certificación y haga clic en **Instalar certificado**.
   d. Haga clic en **Reiniciar servicio MVE**.

      Nota: Reiniciar el servicio MVE también reinicia el sistema, por lo que es posible que el servidor no se encuentre disponible en los siguientes minutos. Antes de reiniciar el servicio, asegúrese de que no haya tareas ejecutándose actualmente.

Eliminación de la información de usuario y las referencias a este

MVE cumple con las normas de protección de datos que establece el Reglamento General de Protección de Datos (RGPD). MVE puede configurarse para aplicar el derecho al olvido y eliminar del sistema la información privada del usuario.

Eliminación de usuarios

1. Haga clic en , en la esquina superior derecha de la página.
2. Haga clic en **Usuario** y seleccione uno o más usuarios.
3. Haga clic en **Eliminar** > **Eliminar usuarios**.

Eliminación de las referencias a un usuario de LDAP

1. Haga clic en , en la esquina superior derecha de la página.
2. Haga clic en **LDAP**.
3. Elimine toda la información relacionada con el usuario en los filtros de búsqueda y encuadernación.

Eliminación de las referencias al usuario en el servidor de correo electrónico

1. Haga clic en , en la esquina superior derecha de la página.
2. Haga clic en **Correo**.
3. Elimine cualquier información relacionada con el usuario, como las credenciales de usuario empleadas para la autenticación con el servidor de correo electrónico.

Eliminación de las referencias al usuario en los registros de tareas

Para obtener más información, consulte “Borrado de registros” en la página 145.

Eliminación de las referencias al usuario en una configuración

1. En el menú Configuraciones, haga clic en **Todas las configuraciones**.
2. Haga clic en el nombre de la configuración.
3. En la pestaña Básicas, elimine todos los valores relacionados con el usuario de Printer Settings, como el nombre y la ubicación del contacto.

Eliminación de las referencias al usuario en el componente de seguridad avanzada

1. En el menú Configuraciones, haga clic en **Todos los componentes de seguridad avanzada**.
2. Haga clic en el nombre del componente.
3. En la sección Valores de seguridad avanzada, elimine todos los valores relacionados con el usuario.

Eliminación de las referencias al usuario en búsquedas guardadas

1. En el menú Impresoras, haga clic en **Búsquedas guardadas**.
2. Haga clic en una búsqueda guardada.
3. Elimine cualquier regla de búsqueda que utilice valores relacionados con los usuarios, como el nombre y la ubicación del contacto.

Eliminación de las referencias al usuario en palabras clave

1. En el menú Impresoras, haga clic en **Lista de impresoras**.
2. Elimine la asignación de palabras clave relacionadas con el usuario de las impresoras.
3. En el menú Impresoras, haga clic en **Palabras clave**.
4. Elimine cualquier palabra clave que utilice información relacionada con el usuario.

Eliminación de las referencias al usuario de eventos y acciones

1. En el menú Impresoras, haga clic en **Eventos y acciones**.
2. Elimine las acciones que contengan referencias al correo electrónico de los usuarios.

Preguntas más frecuentes

Preguntas más frecuentes sobre Markvision Enterprise

¿Por qué no puedo seleccionar varias impresoras en la lista de modelos admitidos al crear una configuración?

Los valores de configuración y los comandos difieren entre los distintos modelos de impresora.

¿Pueden acceder otros usuarios a mis búsquedas guardadas?

Sí. Todos los usuarios pueden acceder a las búsquedas guardadas.

¿Dónde se encuentran los archivos de registro?

Encontrará los archivos de registro de instalación en el directorio oculto del usuario que instala MVE. Por ejemplo, **C:\Users\Administrator\AppData\Local\Temp\mveLexmark-install.log**.

Encontrará los archivos de registro de la aplicación ***.log** en la carpeta ***installation_dir*\Lexmark\Markvision Enterprise\tomcat\logs**, donde ***installation_dir*** es la carpeta de instalación de MVE.

¿Cuál es la diferencia entre el nombre de host y la búsqueda DNS inversa?

Un nombre de host es un nombre exclusivo asignado a una impresora en una red. Cada nombre de host corresponde a una dirección IP. La búsqueda DNS inversa se utiliza para determinar el nombre de host designado y el nombre de dominio de una dirección IP determinada.

¿Dónde puedo encontrar la búsqueda DNS inversa en MVE?

La búsqueda DNS inversa se puede encontrar en los valores generales. Para obtener más información, consulte "Configuración de los valores generales" en la página 149.

¿Cómo puedo añadir reglas manualmente al cortafuegos de Windows?

Ejecute la línea de comandos como administrador y escriba lo siguiente:

```
firewall add allowedprogram "installation_dir/Lexmark/Markvision
Enterprise/tomcat/bin/tomcat9.exe" "Markvision Enterprise Tomcat"
firewall add portopening UDP 9187 "Markvision Enterprise NPA UDP"
firewall add portopening UDP 6100 "Markvision Enterprise LST UDP"
```

Donde ***installation_dir*** es la carpeta de instalación de MVE.

¿Cómo puedo configurar MVE para utilizar un puerto distinto al 443?

1. Pare el dispositivo Markvision Enterprise.
   a. Abra el cuadro de diálogo Ejecutar y escriba **services.msc**.
   b. Haga clic con el botón derecho en **Markvision Enterprise** y, a continuación, haga clic en **Detener**.

2 Abra el archivo ***installation_dir*\Lexmark\Markvision Enterprise\tomcat\conf\server.xml**.

Donde ***installation_dir*** es la carpeta de instalación de MVE.

3 Cambie el valor **Connector port** a otro puerto no utilizado.

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
sslImplementationName="org.apache.tomcat.util.net.jsse.JSSEImplementation"
SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
compression="on" compressableMimeType="text/html,text/xml,text/plain,text/css,
text/javascript,application/javascript,application/json" maxThreads="150"
maxHttpHeaderSize="16384" minSpareThreads="25" enableLookups="false"
acceptCount="100" connectionTimeout="120000" disableUploadTimeout="true"
URIEncoding="UTF-8" server="Apache" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
sslProtocol="TLS" keystoreFile="C:/Program Files/Lexmark/Markvision Enterprise/
../mve_truststore.p12" keystorePass="markvision" keyAlias="mve" keyPass="markvision"
keystoreType="PKCS12" ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA"/>
```

4 Cambie el valor **redirectPort** al mismo número de puerto utilizado como puerto conector.

```
<Connector port="9788" maxHttpHeaderSize="16384" maxThreads="150" minSpareThreads="25"
enableLookups="false" redirectPort="443" acceptCount="100" connectionTimeout="120000"
disableUploadTimeout="true" compression="on" compressableMimeType="text/html,text/xml,
text/plain,text/css,text/javascript,application/javascript,application/json"
URIEncoding="UTF-8" server="Apache"/>
```

5 Reinicie el servicio Markvision Enterprise.

a Abra el cuadro de diálogo Ejecutar y escriba **services.msc**.

b Haga clic con el botón derecho en **Markvision Enterprise** y, a continuación, haga clic en **Reiniciar**.

6 Acceda a MVE utilizando el nuevo puerto.

Por ejemplo, abra un navegador web y escriba **https://*MVE_SERVER*:*port*/mve**.

MVE_SERVER es el nombre de host o dirección IP del servidor que aloja MVE y ***port*** es el número de puerto conector.

¿Cómo puedo personalizar los códigos y las versiones de TLS que utiliza MVE?

1 Pare el dispositivo Markvision Enterprise.

a Abra el cuadro de diálogo Ejecutar y escriba **services.msc**.

b Haga clic con el botón derecho en **Markvision Enterprise** y, a continuación, haga clic en **Detener**.

2 Abra el archivo ***installation_dir*\Lexmark\Markvision Enterprise\tomcat\conf\server.xml**.

Donde ***installation_dir*** es la carpeta de instalación de MVE.

3 Configure los códigos y las versiones de TLS.

Para obtener más información acerca de la configuración, consulte las **Instrucciones de configuración de Apache Tomcat SSL/TLS**.

Para obtener más información acerca de los protocolos y los valores de código, consulte la **documentación de información de asistencia de Apache Tomcat SSL**.

4 Reinicie el servicio Markvision Enterprise.
   a Abra el cuadro de diálogo Ejecutar y escriba **`services.msc`**.
   b Haga clic con el botón derecho en **Markvision Enterprise** y, a continuación, haga clic en **Reiniciar**.

¿Cómo puedo gestionar los archivos CRL si utilizo la CA de Microsoft Enterprise?

1 Obtenga el archivo CRL del servidor de la CA.

   Notas:

   - Si utiliza la CA de Microsoft Enterprise, el CRL no se descarga de forma automática a través del protocolo SCEP.
   - Para obtener más información, consulte la *guía de configuración de la autoridad de certificación de Microsoft*.

2 Guarde el archivo CRL en la carpeta ***`installation_dir`*`\Lexmark\Markvision Enterprise\apps\library\crl`**, donde ***`installation_dir`*** es la carpeta de instalación de MVE.

3 Configure la autoridad de certificación en MVE.

Nota: Este proceso sólo es aplicable si se utiliza el protocolo SCEP.

Solución de problemas

El usuario ha olvidado la contraseña

Restablezca la contraseña de usuario

Necesita derechos de administrador para restablecer la contraseña.

1. Haga clic en la esquina superior derecha de la página.
2. Haga clic en **Usuario** y, a continuación, seleccione un usuario.
3. Haga clic en **Editar** y, a continuación, cambie la contraseña.
4. Haga clic en **Guardar cambios**.

Si ha olvidado su contraseña, realice una de las siguientes acciones:

- Póngase en contacto con otro usuario administrador para restablecer su contraseña.
- Póngase en contacto con el Centro de soporte al cliente de Lexmark.

El usuario administrador ha olvidado la contraseña

Cree otro usuario administrador y elimine la cuenta anterior.

Puede utilizar la utilidad de contraseña de Markvision Enterprise para crear otro usuario administrador.

1. Vaya a la carpeta donde se ha instalado Markvision Enterprise.
   Por ejemplo, **`C:\Archivos de programa\`**
2. Ejecute el archivo **mvepwdutility-windows.exe** en el directorio Lexmark\Markvision Enterprise\.
3. Seleccione un dispositivo y, a continuación, haga clic en **Aceptar** > **Siguiente**.
4. Seleccione **Añadir cuenta de usuario** > **Siguiente**.
5. Introduzca las credenciales de usuario.
6. Haga clic en **Siguiente**.
7. Acceda a MVE y elimine el usuario administrador anterior.

   Nota: Para obtener más información, consulte “Administración de usuarios” en la página 30.

La página no se carga

Es posible que este problema ocurra si ha cerrado el navegador web sin cerrar sesión.

Realice al menos una de las siguientes acciones:

Borre la caché y elimine las cookies de su navegador web

Acceda a la página de inicio de sesión de MVE y, a continuación, inicie sesión con sus credenciales

Abra un navegador web y escriba **`https://MVE_SERVER/mve/login`**, donde ***`MVE_SERVER`*** es el nombre de host o la dirección IP del servidor que aloja MVE.

No se puede encontrar una impresora de red

Realice alguna de estas acciones:

Asegúrese de que la impresora está encendida

Asegúrese de que el cable de alimentación está enchufado de manera segura a la impresora y a una toma de alimentación debidamente conectada a tierra

Asegúrese de que la impresora esté conectada a la red

Reinicie la impresora

Asegúrese de que el protocolo TCP/IP está habilitado en la impresora

Asegúrese de que los puertos utilizados por MVE estén abiertos y SNMP y mDNS están activados.

Para obtener más información, consulte “Descripción de puertos y protocolos” en la página 162.

Póngase en contacto con el representante de Lexmark

Información de la impresora incorrecta

Realice una auditoría

Para obtener más información, consulte “Auditoría de impresoras” en la página 61.

MVE no reconoce una impresora como protegida

Asegúrese de que la impresora esté protegida

Para obtener más información sobre la protección de impresoras, consulte el documento *Seguridad de la impresora y Markvision Enterprise*.

Asegúrese de que el mDNS esté activado y de que no esté bloqueado

Elimine la impresora y, a continuación, vuelva a ejecutar la búsqueda de impresoras.

Para obtener más información, consulte “Búsqueda de impresoras” en la página 34.

El uso de las configuraciones con varias aplicaciones genera un error en el primer intento, pero no se producen problemas en los intentos posteriores

Aumentar los tiempos de espera

1. Vaya a la carpeta donde se ha instalado Markvision Enterprise.

   Por ejemplo, **`C:\Archivos de programa\`**
2. Vaya a la carpeta Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes.
3. Utilice un editor de texto para abrir el archivo *platform.properties*.
4. Edite el valor **`cdcl.ws.readTimeout`**.

   Nota: El valor está en milisegundos. Por ejemplo, 90 000 milisegundos es igual a 90 segundos.
5. Utilice un editor de texto para abrir el archivo *devCom.properties*.
6. Edite los valores **`lst.responseTimeoutsRetries`**.

   Nota: El valor está en milisegundos. Por ejemplo, 10 000 milisegundos es igual a 10 segundos.

   Por ejemplo, **`lst.responseTimeoutsRetries=10000 15000 20000`**. El primer reintento de conexión se produce después de 10 segundos; el segundo, después de 15 segundos; y el tercero, después de 20 segundos.
7. Si es necesario, cuando utilice LDAP GSSAPI, a cree un archivo *parameters.properties*.

   Añada el siguiente valor: **`lst.negotiation.timeout=400`**

   Nota: El valor está en segundos.
8. Guarde los cambios.

Aplicación de configuraciones si falla la emisión del certificado de la impresora

En algunas ocasiones, no se emite ningún certificado durante la aplicación.

Aumente el número de reintentos de inscripción

Añada la siguiente clave en el archivo **platform.properties**:

```
enrol.maxEnrolmentRetry=10
```

El valor de reintento debe ser superior a cinco.

Autoridad certificadora de OpenXPKI

Error en la emisión del certificado con el servidor de la CA OpenXPKI

Compruebe que la clave de "firmante en nombre de" en MVE coincide con la clave del firmante autorizado en el servidor de la CA

Por ejemplo:

Si la siguiente es la clave **ca.onBehalf.cn** del archivo **platform.properties** en MVE,

```
ca.onBehalf.cn=Markvision_SQA-2012-23AB.lrdc.lexmark.ds
```

la siguiente debe ser la clave **authorized_signer** del archivo **generic.yaml** en el servidor de la CA.

```
rule1:
            # Full DN
                    Subject: CN=Markvision_SQA-2012-23AB.lrdc.lexmark.ds
```

Para obtener más información sobre la configuración del servidor de la CA OpenXPKI, consulte la *guía de configuración de la autoridad certificadora OpenXPKI*.

Se produce un error interno del servidor

Instale la configuración regional en_US.utf8

1. Ejecute el comando **`dpkg-reconfigure locales`**.
2. Instale la configuración regional **en_US.utf8** (locale -a | grep en_US).

No aparece la solicitud de inicio de sesión

Al acceder a **http://suhost/openxpki/**, solo se muestra el banner Open Source TrustCenter, sin una solicitud de inicio de sesión.

Active `fcgid`

Ejecute los siguientes comandos:

1. **`a2enmod fcgid`**
2. **`reinicio del servicio apache2`**

Se produce un error de conector anidado sin clase

Aparece el error **`EXCEPCIÓN: conector anidado sin clase (scep.scep-server-1.connector.initial)`** en la línea 201 de /usr/share/perl5/Connector/Multi.pm.

Actualice `scep.scep-server-1`

En **/etc/openxpki/config.d/realm/REALM/scep/generic.yaml**, sustituya **`scep.scep-server-1`** por **`scep.generic`**.

Nota: Sustituya **`REALM`** por el nombre de su dominio. Por ejemplo, cuando utilice el dominio predeterminado, utilice **`ca-one`**.

```
eligible:
     initial:
            value@: connector:scep.generic.connector.initial
```

No se pueden aprobar certificados de forma manual

El botón Aprobación manual no aparece cuando se aprueban certificados de forma manual.

Actualice `scep.scep-server-1`

En **/etc/openxpki/config.d/realm/REALM/scep/generic.yaml**, sustituya **`scep.scep-server-1`** por **`scep.generic`**.

Nota: Sustituya **`REALM`** por el nombre de su dominio. Por ejemplo, cuando utilice el dominio predeterminado, utilice **`ca-one`**.

```
eligible:
     initial:
            value@: connector:scep.generic.connector.initial
```

Se produce un error Perl al aprobar solicitudes de inscripción

Actualice `scep.scep-server-1`

En **/etc/openxpki/config.d/realm/REALM/scep/generic.yaml**, sustituya **`scep.scep-server-1`** por **`scep.generic`**.

Nota: Sustituya **`REALM`** por el nombre de su dominio. Por ejemplo, cuando utilice el dominio predeterminado, utilice **`ca-one`**.

```
eligible:
     initial:
            value@: connector:scep.generic.connector.initial
```

Los tokens `ca-signer-1` y `vault-1` están sin conexión

La página Estado del sistema muestra que los tokens **`ca-signer-1`** y **`vault-1`** están sin conexión.

Realice alguna de estas acciones:

Cambie la contraseña de la clave de certificado

En **/etc/openxpki/config.d/realm/ca-one/crypto.yaml**, cambie la contraseña de la clave de certificado.

Cree los enlaces simbólicos correctos y copie el archivo de clave

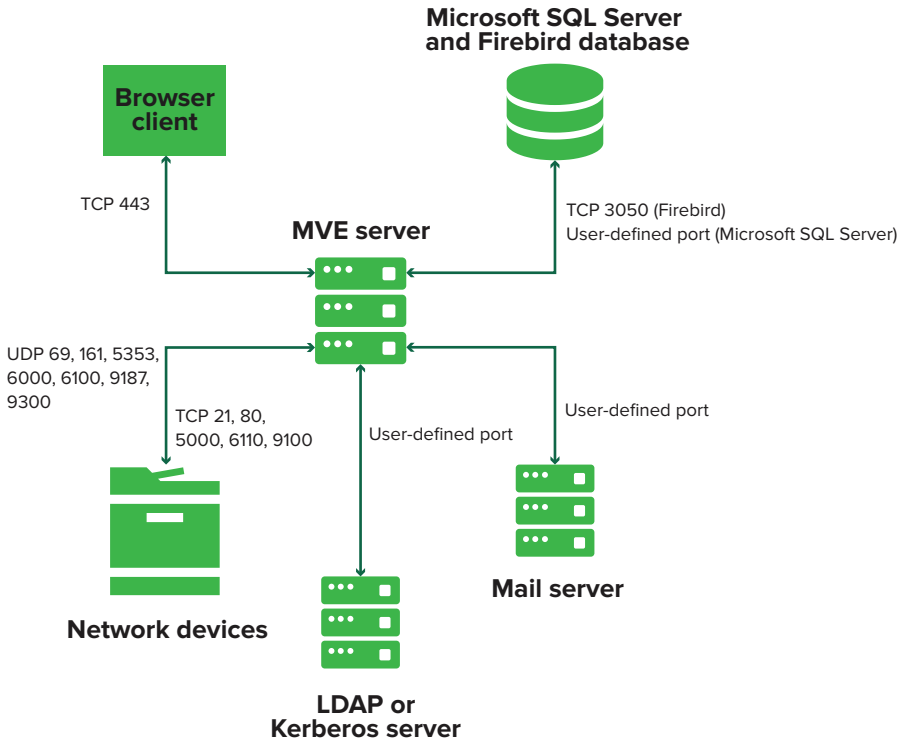
Para obtener más información, consulte “Copia del archivo de clave y creación de un enlace simbólico” en la página 108.

Asegúrese de que el archivo de clave es legible para OpenXPKI

Apéndice

Descripción de puertos y protocolos

MVE utiliza diferentes puertos y protocolos para varios tipos de comunicación de red, como se muestra en el diagrama siguiente:



Notas:

- Los puertos son bidireccionales y deben estar abiertos o activos para que MVE funcione correctamente. Asegúrese de que todos los puertos de la impresora están habilitados.
- Algunas comunicaciones requieren un puerto efímero, que es un intervalo asignado de puertos disponibles en el servidor. Cuando un cliente solicita una sesión de comunicación temporal, el servidor asigna un puerto dinámico al cliente. El puerto es válido sólo durante un breve período de tiempo y puede volver a estar disponible para usarlo cuando la sesión anterior caduca.

Comunicación del servidor a la impresora

Los puertos y protocolos utilizados durante la comunicación del servidor MVE a las impresoras de red

Protocolo	Servidor MVE	Impresora	Se utiliza para
Network Printing Alliance Protocol (NPAP)	UDP 9187	UDP 9300	Comunicación con impresoras de red Lexmark.
Transporte de red XML (XMLNT)	UDP 9187	UDP 6000	Comunicación con algunas impresoras de red Lexmark.
Lexmark Secure Transport (LST)	UDP 6100 Puerto de protocolo de control de transmisión (TCP) efímero (intercambio)	UDP 6100 TCP 6110 (intercambio)	Comunicación segura con algunas impresoras de red Lexmark.
Multicast Domain Name System (mDNS)	Puerto de protocolo de datagramas de usuario (UDP) efímero	UDP 5353	Búsqueda de impresoras de red Lexmark y determinación de los recursos de seguridad de las impresoras. **Nota:** Este puerto es necesario para permitir a MVE comunicarse con impresoras con seguridad.
Protocolo de administración de red simple (SNMP)	Puerto UDP efímero	UDP 161	Búsqueda y comunicación con impresoras de red Lexmark y de terceros.
Protocolo de transferencia de archivos (FTP)	Puerto TCP efímero	TCP 21 TCP 20	Implementación de archivos.
Protocolo de transferencia de hipertexto (HTTP)	Puerto TCP efímero	TCP 80	Implementación de archivos o cumplimiento de configuraciones.
		TCP 443	Implementación de archivos o cumplimiento de configuraciones.
Protocolo de transferencia de hipertexto sobre SSL (HTTPS)	Puerto TCP efímero	TCP 161 TCP 443	Implementación de archivos o cumplimiento de configuraciones.
RAW	Puerto TCP efímero	TCP 9100	Implementación de archivos o cumplimiento de configuraciones.

Comunicación de la impresora al servidor

El puerto y el protocolo utilizados durante la comunicación desde las impresoras de red al servidor MVE

Protocolo	Impresora	Servidor MVE	Se utiliza para
NPAP	UDP 9300	UDP 9187	Generar y recibir alertas

Comunicación del servidor a la base de datos

Puertos utilizados durante la comunicación del servidor MVE a las bases de datos

Servidor MVE	Base de datos	Se utiliza para
Puerto TCP efímero	Puerto definido por el usuario. El puerto predeterminado es TCP 1433.	Comunicación con una base de datos SQL Server.
Puerto TCP efímero	TCP 3050	Comunicación con una base de datos Firebird.

Comunicación del cliente al servidor

El puerto y el protocolo utilizados durante la comunicación del navegador local al servidor MVE

Protocolo	Navegador local	Servidor MVE
Protocolo de transferencia de hipertexto sobre SSL (HTTP)	Puerto TCP	TCP 443

Comunicación entre servidor y servidor de correo

Puerto y protocolo utilizados durante la comunicación del servidor MVE a un servidor de correo

Protocolo	Servidor MVE	Servidor SMTP	Se utiliza para
Protocolo simple de transferencia de correo (SMTP)	Puerto TCP efímero	Puerto definido por el usuario. El puerto predeterminado es TCP 25.	Proporcionar la función de correo electrónico que se utiliza para recibir alertas de las impresoras.

Comunicación entre servidor y servidor LDAP

Los puertos y protocolos utilizados durante la comunicación del servidor MVE a un servidor LDAP que implican a grupos de usuarios y la función de autenticación

Protocolo	Servidor MVE	Servidor LDAP	Se utiliza para
Protocolo ligero de acceso a directorios (LDAP)	Puerto TCP efímero	Puerto definido por el usuario. El puerto predeterminado es TCP 389.	Autenticación de usuarios de MVE mediante un servidor LDAP.
Lightweight Directory Access Protocol sobre TLS (LDAPS)	Puerto TCP efímero	Puerto definido por el usuario. El puerto predeterminado es TCP 636.	Autenticación de usuarios MVE mediante un servidor LDAP sobre TLS.
Kerberos	Puerto UDP efímero	Puerto definido por el usuario. El puerto predeterminado es UDP 88.	Autenticación de usuarios MVE con Kerberos.

Activación de la aprobación automática de solicitudes de certificado en la CA de Microsoft

De forma predeterminada, todos los servidores de la CA están en modo pendiente y debe aprobar manualmente cada solicitud de certificado firmada. Dado que este método no es factible para solicitudes masivas, debe activar la aprobación automática de certificados firmados.

1. En Server Manager, haga clic en **Herramientas > Entidad de certificación**.
2. En el panel de la izquierda, haga clic con el botón derecho del ratón en la CA y, a continuación, haga clic en **Propiedades > Módulo de directivas**.
3. En la pestaña Gestión de solicitudes, haga clic en **Seguir la configuración de la plantilla de certificado si procede** y, a continuación, haga clic en **Aceptar**.

   Nota: Si **Establecer el estado de solicitud de certificado en pendiente** está seleccionado, deberá aprobar el certificado de forma manual.
4. Reinicie el servicio CA.

Revocación de certificados

Nota: Antes de comenzar, asegúrese de que el servidor de la CA está configurado para las CRL y que están disponibles.

1. En el servidor de la CA, abra **Entidad de certificación**.
2. En el panel de la izquierda, expanda la CA y, a continuación, haga clic en **Certificados emitidos**.
3. Haga clic con el botón derecho del ratón en un certificado para revocarlo y, a continuación, haga clic en **Todas las tareas > Revocar certificado**.
4. Seleccione un código de motivo y la fecha y hora de la revocación y, a continuación, haga clic en **Sí**.
5. En el panel de la izquierda, haga clic con el botón derecho del ratón en **Certificados revocados** y, a continuación, haga clic en **Todas las tareas > Publicar**.

   Nota: Asegúrese de que el certificado revocado se encuentra en Certificados revocados.

Puede ver el número de serie del certificado revocado en la CRL.

Avisos

Nota sobre la edición

Septiembre de 2022

El párrafo siguiente no se aplica a los países en los que tales disposiciones son contrarias a la legislación local: LEXMARK INTERNATIONAL, INC, PROPORCIONA ESTA PUBLICACIÓN «TAL CUAL» SIN GARANTÍA DE NINGÚN TIPO, NI EXPLÍCITA NI IMPLÍCITA, LO QUE INCLUYE, PERO SIN LIMITARSE A ELLO, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD O IDONEIDAD PARA UN PROPÓSITO EN PARTICULAR. Algunos estados no permiten la renuncia a garantías explícitas ni implícitas en algunas transacciones; por lo tanto, es posible que la presente declaración no se aplique en su caso.

Esta publicación puede incluir inexactitudes técnicas o errores tipográficos. Periódicamente se realizan modificaciones en la presente información; dichas modificaciones se incluyen en ediciones posteriores. Las mejoras o modificaciones en los productos o programas descritos pueden efectuarse en cualquier momento.

Las referencias hechas en esta publicación a productos, programas o servicios no implican que el fabricante tenga la intención de ponerlos a la venta en todos los países en los que opere. Cualquier referencia a un producto, programa o servicio no indica o implica que sólo se pueda utilizar dicho producto, programa o servicio. Se puede utilizar cualquier producto, programa o servicio de funcionalidad equivalente que no infrinja los derechos de la propiedad intelectual. La evaluación y comprobación del funcionamiento junto con otros productos, programas o servicios, excepto aquellos designados expresamente por el fabricante, son responsabilidad del usuario.

Para obtener soporte técnico de Lexmark, visite **http://support.lexmark.com**.

Para obtener información sobre la política de privacidad de Lexmark que rige el uso de este producto, visite **www.lexmark.com/privacy**.

Para obtener información sobre los consumibles y descargas, visite **www.lexmark.com**.

© **2017 Lexmark International, Inc.**

Reservados todos los derechos.

Marcas comerciales

Lexmark, el logotipo de Lexmark y Markvision son marcas comerciales o marcas comerciales registradas de Lexmark International, Inc., en EE. UU. o en otros países.

Windows, Microsoft, Microsoft Edge, PowerShell, SQL Server y Windows Server son marcas comerciales del grupo de compañías Microsoft.

Firebird es una marca comercial registrada de Firebird Foundation.

Google Chrome es una marca comercial de Google LLC.

Apple and Safari are registered trademarks of Apple Inc.

Java es una marca comercial registrada de Oracle o sus filiales.

Las otras marcas comerciales pertenecen a sus respectivos propietarios.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commerical Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

JmDNS License

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Arthur van Hoff

avh@strangeberry.com

Rick Blair

rickblair@mac.com

** JmDNS

Avisos de licencia

Todos los avisos de licencia relacionados con este producto se pueden consultar en la carpeta del programa.

Glosario

acción
Una notificación de correo electrónico o una operación de línea de comandos. Las acciones asignadas a los eventos se activan cuando aparece una alerta de impresora.

ajustes variables
Un conjunto de ajustes de la impresora que contiene valores dinámicos que se pueden integrar en una configuración.

auditoría
La tarea de recopilar los datos de la impresora, como el estado de la impresora, los consumibles y las capacidades.

configuración
Una recopilación de los valores que se pueden asignar y aplicar a una impresora o a un grupo de modelos de impresora. Dentro de una configuración, se pueden modificar los valores de la impresora e implementar aplicaciones, licencias, firmware y certificados CA en las impresoras.

evento
Define las acciones que se ejecutan cuando las alertas específicas están activas.

impresora protegida
Una impresora configurada para comunicarse a través de una canal cifrado y que requiere autenticación para acceder a sus funciones o aplicaciones.

palabra clave
Un texto personalizado asignado a las impresoras que puede usarse para buscar esas impresoras dentro del sistema. Cuando se filtra una búsqueda por palabra clave, solo se muestran las impresoras etiquetadas con la palabra clave.

perfil de búsqueda
Un perfil que contiene un conjunto de parámetros que se utilizan para encontrar impresoras en una red. También puede contener configuraciones predeterminadas que se pueden asignar y aplicar a las impresoras automáticamente durante la búsqueda.

token
Un identificador que representa los valores de datos de la impresora para los ajustes variables en una configuración.

Índice

A

accesibilidad de la CRL
  configuración 86, 111
Acceso a la información de entidad
  configuración 85
acceso a MVE 23
acción
  marcadores de posición 138
acción de correo electrónico 137
acción de registro de eventos 137
acciones
  administración 139
  creación 137
  edición 139
  eliminación 139
  prueba 139
activación de certificados Firmante en nombre de un tercero 112
activación de la aprobación automática de solicitudes de certificado en la CA de Microsoft 165
activación de la aprobación automática de solicitudes de certificado en la CA de OpenXPKI 112
activación de la autenticación básica 134
activación de la autenticación del servidor LDAP 31
activación de varios certificados activos
  mismo asunto 116
activación del servicio SCEP 111
actualización a la última versión de MVE 25
actualización del estado de la impresora 61
actualización del firmware de la impresora 64
adición de EKU de autenticación de cliente en los certificados 117
adición de una renuncia de responsabilidad de inicio de sesión 150
administración de acciones 139
administración de búsquedas guardadas 53
administración de certificados 77
administración de certificados automatizados
  configuración 79
administración de configuraciones 69
administración de eventos 144
administración de palabras clave 47
administración de perfiles de búsqueda 36
administración de programas 148
administración de usuarios 30
administración de vistas 44
AIA
  configuración 85
ajustes dinámicos
  descripción 73
ajustes variables
  descripción 73
alertas de impresora
  descripción 140
anulación de la asignación de configuraciones 62
aplicación de configuraciones 62
aplicación de configuraciones si falla la emisión del certificado de la impresora 159
aplicaciones
  desinstalación 65
aprobación automática de solicitudes de certificado
  activación en la CA de Microsoft 165
  activación en la CA de OpenXPKI 112, 130
archivo de configuración de OpenSSL
  creación 105, 123
archivos
  implementación 63
archivos clave
  copia 108
archivos de contraseña para claves de certificado
  creación 106, 124, 132
archivos de registro
  localización 153
archivos de registro de instalación
  localización 153
archivos de registro de la aplicación
  localización 153
asignación de configuraciones a impresoras 62
asignación de eventos a impresoras 65
asignación de una palabra clave 66
asuntos de certificado completos
  solicitud a través de SCEP 117
auditoría de impresoras 61
autenticación
  certificado de cliente 93
  integrado en Windows 93
  nombre de usuario y contraseña 93
autenticación básica
  activación 134, 135
autenticación de certificado de cliente 93
autenticación de nombre de usuario y contraseña 93
autenticación integrada de Windows 93

B

barra de búsqueda
  filtrado de impresoras 46
base de datos
  configuración 19
  realización de una copia de seguridad 26
  requisitos 15
  restauración 26
base de datos Firebird 19
bases de datos admitidas 15
biblioteca de recursos
  importación de archivos a 76

borrado de registros 145
búsqueda de impresoras 37
búsqueda de nombre de host
  búsqueda inversa 153
búsqueda DNS inversa 153
búsqueda guardada
personalizada
  creación 49
búsquedas guardadas
  acceso 153
  administración 53
  copia 53
  edición 53
  ejecución 49
  eliminación 53

C

CA de Microsoft Enterprise
  configuración 153
CA de Microsoft Enterprise con
NDES
  configuración 81, 83
CA de OpenXPKI
  configuración manual 105, 122
  configuración mediante el script
    predeterminado 104, 121
  instalación 101, 119
ca-signer-1 está sin conexión
  solución de problemas 161
cambio de la configuración del
instalador tras la instalación 28
cambio de la contraseña 24
cambio de la vista de lista de
impresoras 46
cambio del idioma 24
caso de ejemplo de clonación de
configuraciones 72
CDP
  configuración 85
CEP
  configuración 95, 97, 99
  instalación 94
certificado de cliente 98
certificado MVE
  firma 150
certificado web
  creación 126
certificados
  creación 114, 132
  importación 109
  revocación 118, 165
certificados CA raíz
  creación 106, 125
certificados con el mismo asunto
  activación 133
certificados de almacén
  creación 107, 126
certificados de firmante
  creación 107, 125, 132
certificados de impresora
  configuración manual 67
certificados de servidor LDAP
  instalación 33
certificados Firmante en nombre
de un tercero
  activación 112
certificados SCEP
  creación 108
certificados SSL
  creación 91
CES
  configuración 96, 98, 100
  instalación 94
cifrado AES256
  configuración 153
claves de certificado
  creación de archivos de
    contraseña 106, 124, 132
clonación de configuraciones
  caso de ejemplo 72
códigos
  personalización 153
componente de seguridad
avanzada
  creación 73
Comprobación de cumplimiento
del dispositivo
  administración 39
comprobación del cumplimiento
de las impresoras con una
configuración 63
comunicaciones de la impresora
  protección 59
configuración
  creación 69, 72
  cumplimiento 63
  exportación 75
  importación 75
configuración de ajustes de
acceso a la información de
entidad 85
configuración de ajustes del
punto de distribución de
certificación 85
configuración de CEP 95, 97, 99
configuración de
CES 96, 98, 100
configuración de la accesibilidad
de la CRL 86, 111
configuración de la base de
datos 19
configuración de la CA de
Microsoft Enterprise con NDES
  descripción general 81, 83
configuración de la CA de
OpenXPKI de forma
manual 105, 122
configuración de la CA de
OpenXPKI mediante el script
predeterminado 104, 121
configuración de la seguridad de
la impresora 58
configuración de los certificados
de la impresora de forma
manual 67
configuración de los criterios de
búsqueda
  descripción 51
configuración de los permisos de
impresión en color 74
configuración de los valores del
correo electrónico 149
configuración de los valores
generales 149
configuración de MVE para
ejecutar como usuario 20
configuración de MVE para la
administración de certificados
automatizados 79
configuración de puntos finales
EST para varios dominios 131
configuración de puntos finales
SCEP para varios dominios 115
configuración de servidores del
servicio de inscripción de
dispositivos de red 87
configuración de servidores
NDES 87
configuración del directorio 131
configuración del instalador
  cambio 28
configuración del servidor
web 126

configuraciones
  administración 69
  anulación de la asignación 62
  aplicación 62
  asignación 62
configuraciones predeterminadas 56
contraseña
  cambio 24
  restablecimiento 156
contraseña de clave de certificado
  poner a disposición de openXPKI 127
Contraseña de comprobación
  desactivación en el servidor de la CA de Microsoft 89
control de impresoras 54
controles de acceso a funciones
  descripción 58
copia de archivos de clave 108
copia de búsquedas guardadas 53
copia de perfiles de búsqueda 36
copia de seguridad y restauración de la base de datos 26
copia de vistas 44
copia del directorio 113, 131
cortafuegos de Windows
  adición de reglas 153
creación de archivos de configuración de OpenSSL 105
creación de archivos de contraseña para claves de certificado 106, 132
creación de certificados 114
creación de certificados CA raíz 106
creación de certificados de almacén 107
creación de certificados de firmante 107
creación de certificados SCEP 108
creación de certificados SSL
  servidores CEP y CES 91
creación de enlaces simbólicos 108
creación de palabras clave 47
creación de perfiles de búsqueda 34
creación de plantillas de certificado 88, 92
creación de un certificado de cliente 98
creación de un componente de seguridad avanzada desde una impresora 73
creación de un evento 139
creación de un paquete de aplicaciones 75
creación de un programa 147
creación de una acción 137
creación de una búsqueda guardada personalizada 49
creación de una configuración 69
creación de una configuración desde una impresora 72
credenciales
  introducción 66
criterios de búsqueda
  operadores 51
  parámetros 51
CRL
  publicación 118
CSV
  ajustes variables 73
cumplimiento
  comprobación 63

D

datos de impresora
  exportación 44
delegación
  activación 94
  requisitos 93
desactivación de la contraseña de comprobación en el servidor de la CA de Microsoft 89
descarga de certificados de ca
  cambio de detalles para activar 130
descripción de las alertas de impresora 140
descripción de las funciones de usuario 29
descripción de los estados de la vida útil de la impresora 47
descripción de los marcadores de posición de acción 138
descripción general
  administración de alertas de impresora 137
  administración de configuraciones 69
  configuración del acceso de usuario 29
  configuración del servidor de la CA raíz 82
  configuración del servidor de la CA subordinada 84
  Markvision Enterprise 12
  panel de seguridad 38
  visualización del estado y el historial de las tareas 145
descripción general de la administración de alertas de impresoras 137
descripción general de la configuración del acceso de usuario 29
descripción general de la configuración del servidor de la CA raíz 82
descripción general de la configuración del servidor de la CA subordinada 84
descripción general de la visualización del estado y el historial de las tareas 145
desinstalación de aplicaciones de las impresoras 65
detención de tareas 145
directorio
  copia y configuración 131

E

edición de acciones 139
edición de búsquedas guardadas 53
edición de palabras clave 47
edición de perfiles de búsqueda 36
edición de programas 148
edición de vistas 44
ejecución como usuario
  configuración 20
ejecución de perfiles de búsqueda 36
ejecución de una búsqueda guardada 49

EKU de autenticación de cliente
adición de certificados 117
el uso de las configuraciones con varias aplicaciones genera un error en el primer intento, pero no se producen problemas en los intentos posteriores 158
el usuario administrador ha olvidado la contraseña 156
el usuario ha olvidado la contraseña 156
eliminación de acciones 139
eliminación de búsquedas guardadas 53
eliminación de impresoras 67
eliminación de la información de usuario y las referencias a este 151
eliminación de palabras clave 47
eliminación de perfiles de búsqueda 36
eliminación de programas 148
eliminación de vistas 44
Embedded Web Server
visualización 61
enlaces simbólicos
creación 108
error de conector anidado sin clase 160
error en la emisión del certificado con el servidor de la CA de OpenXPKI 159
error interno del servidor 159
error Perl 160
establecimiento de los números de puerto predeterminados para la CA de OpenXPKI 116
establecimiento de plantillas de certificado para NDES 88
establecimiento de una vista predeterminada 44
establecimiento del directorio 113
establecimiento del estado de la impresora 62
estado de la impresora
actualización 61
establecimiento 62
estado de la tarea
visualización 145
estados de la vida útil de la impresora
descripción 47
estados de seguridad de la impresora
descripción 55
evento
creación 139
eventos
administración 144
asignación 65
edición 144
eliminación 144
exportación de CSV
ajustes variables 73
exportación de datos de impresora 44
exportación de registros 146

F

filtrado de impresoras mediante la barra de búsqueda 46
firma del certificado MVE 150
firmware de la impresora
actualización 64
función de administración de certificados automatizados 77
funciones de usuario
descripción 29

G

generación de información de la CRL 110

H

historial de cambios 8

I

idioma
cambio 24
idiomas
compatibles 16
idiomas compatibles 16
implementación de archivos en impresoras 63
importación de archivos a la biblioteca de recursos 76
importación de certificados 109
importación de CSV
ajustes variables 73
importación o exportación de una configuración 75
impresora
cumplimiento 63
reinicio 61
impresoras
auditoría 61
búsqueda 37
eliminación 67
eventos 65
filtrado 46
implementación de archivos 63
protección 56, 60
impresoras protegidas
autenticación 66
información de la CRL
generación 110, 128
publicación 129
información de la impresora
visualización 43
información de la impresora incorrecta 157
Información de seguridad del dispositivo
administración 38
información de usuario
eliminación 151
inicio de OpenXPKI 109
instalación de certificados de servidor LDAP 33
instalación de la CA de OpenXPKI 101, 119
instalación de MVE 20
instalación de servidores de la CA raíz 82
instalación de servidores de la CA subordinada 84
instalación silenciosa
MVE 21
instalación silenciosa de MVE 21
introducción de las credenciales para impresoras protegidas 66

L

la página tarda mucho en cargar 157
lista de impresoras
visualización 40

M

marcadores de posición 137

marcadores de posición de acción
  descripción 138
Markvision Enterprise
  descripción 12
mejores prácticas 13
métodos de autenticación 92
Microsoft SQL Server 19
modelos admitidos
  configuración 153
modelos de impresora admitidos 16
MVE
  acceso 23
  actualización 25
  instalación 20
MVE no reconoce una impresora como protegida 158

N

navegadores web admitidos 15
no aparece la solicitud de inicio de sesión 160
no se puede encontrar una impresora de red 157
no se pueden aprobar certificados de forma manual 160
números de puerto predeterminados
  cambio para la CA de OpenXPKI 133
  configuración para la CA de OpenXPKI 116
Números de puerto predeterminados de la CA de OpenXPKI
  cambio 133
números de puerto predeterminados para la CA de OpenXPKI
  cambio 133

O

obtención de asuntos de certificado completos al realizar la solicitud a través de SCEP 117
OpenXPKI
  inicio 109, 128

P

palabra clave
  asignación 66
palabras clave
  administración 47
  creación 47
  edición 47
  eliminación 47
panel
  acceso 38
paquete de aplicaciones
  creación 75
perfil de búsqueda
  creación 34
perfiles de búsqueda
  administración 36
  copia 36
  edición 36
  ejecución 36
  eliminación 36
permisos
  descripción 58
permisos de impresión en color
  configuración 74
plantillas de certificado 92
  creación 88
plantillas de certificado para NDES
  establecimiento 88
preguntas frecuentes 136
preguntas más frecuentes 136
programa
  creación 147
programas
  administración 148
  edición 148
  eliminación 148
protección de impresoras 60
protección de impresoras con la configuración predeterminada 56
protección de las comunicaciones de la impresora en su flota 59
Protocolo de inscripción de certificados simple
  activación 111
protocolos
  descripción 162
prueba de acciones 139
publicación de CRL 118
puertos
  configuración 153
  descripción 162
Punto de distribución de certificación
  configuración 85
puntos finales EST
  configuración para varios dominios 131
puntos finales SCEP
  configuración para varios dominios 115

R

rechazo de solicitudes de certificado sin Contraseña de comprobación en CA de OpenXPKI 116
registros
  borrado 145
  exportación 146
  visualización 145
reinicio de la impresora 61
renuncia de responsabilidad de inicio de sesión
  adición 150
requisitos
  conectividad de red 90
  sistema 90
requisitos de base de datos 15
requisitos de conectividad 90
requisitos de conectividad de red 90
requisitos de delegación 93
requisitos de servidor web 15
requisitos del sistema 90
requisitos del sistema de usuario 15
revocación de certificados 118, 165

S

seguridad de la impresora
  configuración 58
servicio SCEP
  activación 111
Servidor LDAP
  activación de la autenticación 31
servidor web
  configuración 126

requisitos 15
servidores admitidos 15
servidores CEP y CES
creación de certificados SSL 91
servidores de la CA raíz
instalación 82
servidores de la CA subordinada
instalación 84
servidores del servicio de inscripción de dispositivos de red
configuración 87
servidores NDES
configuración 87
sistema de usuario
requisitos 15
sistemas operativos compatibles 15
solicitudes de certificado en la CA de Microsoft
aprobación automática 165
solicitudes de certificado en la CA de OpenXPKI
aprobación automática 112, 130
solicitudes de certificado sin contraseña de comprobación
cómo rechazar en la CA de OpenXPKI 116
solución de problemas
aplicación de configuraciones si falla la emisión del certificado de la impresora 159
ca-signer-1 está sin conexión 161
el uso de las configuraciones con varias aplicaciones genera un error en el primer intento, pero no se producen problemas en los intentos posteriores 158
el usuario administrador ha olvidado la contraseña 156
el usuario ha olvidado la contraseña 156
error de conector anidado sin clase 160
error en la emisión del certificado con el servidor de la CA de OpenXPKI 159
error interno del servidor 159
error Perl 160
información de la impresora incorrecta 157
la página tarda mucho en cargar 157
MVE no reconoce una impresora como protegida 158
no aparece la solicitud de inicio de sesión 160
no se puede encontrar una impresora de red 157
no se pueden aprobar certificados de forma manual 160
vault-1 está sin conexión 161

T

tareas
detención 145

U

usuarios
adición 30
administración 30
edición 30
eliminación 30

V

valores de configuración
versión para imprimir 73
valores del correo electrónico
configuración 149
valores generales
configuración 149
varios certificados activos con el mismo asunto
activación 133
vault-1 está sin conexión
solución de problemas 161
versiones de TLS
personalización 153
vista de lista de impresoras
cambio 46
vistas
administración 44
copia 44
edición 44
eliminación 44
visualización de Embedded Web Server de la impresora 61
visualización de la información de la impresora 43
visualización de la lista de impresoras 40
visualización de registros 145
visualización del estado de la tarea 145