Markvision Enterprise

Guía del usuario

Abril de 2012

www.lexmark.com

Aviso de la edición

Abril de 2012

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 asistencia técnica de Lexmark, visite **support.lexmark.com**.

Para obtener información acerca de consumibles y descargas, visite **www.lexmark.com**.

Si no dispone de acceso a Internet, puede ponerse en contacto con Lexmark por correo:

Lexmark International, Inc.
Bldg 004-2/CSC
740 New Circle Road NW
Lexington, KY 40550
EE. UU.

© 2012 Lexmark International, Inc.

Reservados todos los derechos.

Marcas comerciales

Lexmark, Lexmark con diamante y MarkVision son marcas comerciales de Lexmark International, Inc., registradas en EE.UU. y/o en otros países.

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.

Avisos de licencia

Todos los avisos de licencia relacionados con este producto se pueden consultar en el directorio raíz del CD del software de instalación.

Índice general

Aviso de la edición.....2

Descripción general.....7

¿Qué es Markvision Enterprise?.....7

Introducción.....8

Instrucciones de compatibilidad.....8

Requisitos del sistema.....8

Servidores de bases de datos admitidos.....8

Instalación de Markvision.....8

Actualización a la última versión de Markvision.....9

Copia de seguridad y restauración de la base de datos Firebird.....9

Acceso a Markvision.....10

Migración de MarkVision Professional a Markvision Enterprise.....11

Uso de Markvision.....12

Comprensión de la pantalla principal.....14

Descripción de puertos y protocolos.....15

Administración de activos.....18

Búsqueda de dispositivos.....18

Creación de un perfil de búsqueda.....18

Edición o eliminación de un perfil de búsqueda.....19

importación de dispositivos desde un archivo.....20

Administración de dispositivos.....21

Establecimiento del estado de duración del dispositivo.....21

Auditoría de un dispositivo.....21

Visualización de propiedades de los dispositivos.....22

Búsqueda y organización de dispositivos en el sistema.....24

Búsqueda de dispositivos en el sistema.....24

Trabajo con marcadores.....27

Creación de marcadores.....27

Acceso a marcadores.....27

Eliminación de marcadores.....27

Uso de categorías y palabras clave.....27

Adición, edición o eliminación de categorías.....28

Adición, edición o eliminación de palabras clave.....28

Asignación de palabras clave a un dispositivo 28
Eliminación de palabras clave asignadas de dispositivos 29

Administración de políticas 30

Creación de políticas 30
Creación de nuevas políticas 30
Creación de políticas desde dispositivos 31
Descripción de la política de seguridad 31
Descripción de los dispositivos seguros 32
Descripción de la configuración para políticas de seguridad 33
Creación de una política de seguridad 34
Modificación de los credenciales de comunicación de un dispositivo restringido 39
Edición o eliminación de políticas 40
Asignación de políticas 41
Comprobación de cumplimiento con políticas 41
Aplicación de políticas 41
Eliminación de políticas 42

Administración de la asistencia técnica 43

Trabajo con políticas 43
Comprobación del cumplimiento de los dispositivos con las políticas 43
Aplicación de políticas 43
Trabajo con dispositivos 43
Comprobación del estado de un dispositivo 43
Visualización de dispositivos de forma remota 44
Visualización de la página web incorporada 44

Administración de eventos de dispositivo 45

Creación de un destino 45
Editar o eliminar un destino 46
Creación de un evento 46
Edición o eliminación de un evento 46
Asignación de un evento a un dispositivo 47
Eliminación de eventos de dispositivos 47
Visualización de detalles de eventos 47

Realización de otras tareas administrativas 48

Descarga de archivos genéricos 48
Configuración de los valores del correo electrónico 48
Configuración de los valores del sistema 49

Adición, edición o eliminación de usuarios en el sistema....49
Activación de la autenticación del servidor LDAP....50
Generación de informes....55
Programación de tareas....56
Visualización de registros del sistema....57

Preguntas más frecuentes....58

Solución de problemas....59

El usuario ha olvidado la contraseña....59
La aplicación no encuentra ningún dispositivo de red....59
Compruebe las conexiones de la impresora....59
Asegúrese de que el servidor de impresión interno está correctamente instalado y activado....59
Asegúrese de que el nombre del dispositivo en la aplicación es el mismo que el establecido en el servidor de impresión....60
Asegúrese de que el servidor de impresión se comunica en la red....60
La información del dispositivo es incorrecta....60

Glosario de términos de seguridad....61

Índice alfabético....62

Descripción general

¿Qué es Markvision Enterprise?

Markvision™ Enterprise (MVE) es una utilidad de administración de dispositivos basada en web diseñada para profesionales de TI. MVE funciona como una aplicación cliente-servidor. El servidor busca y se comunica con los dispositivos en la red y proporciona información sobre ellos al cliente. El cliente muestra información sobre los dispositivo y proporciona una interfaz de usuario para administrarlos. Cada servidor de Markvision puede administrar miles de dispositivos a la vez.

Las disposiciones de seguridad incorporadas evitan el acceso no autorizado a la aplicación, y sólo los usuarios autorizados pueden utilizar el cliente para acceder a las opciones de administración.

Markvision permite controlar y administrar la flota de impresión completa, que está compuesta por impresoras y servidores de impresión. En la *biblioteca de infraestructuras de tecnologías de la información* (ITIL, Information Technology Infrastructure Library), las impresoras y los servidores de impresión también se conocen como *elementos de configuración* (CI, Configuration Items). En este documento, los elementos de configuración, las impresoras o los servidores de impresión a veces se denominan dispositivos.

Introducción

Instrucciones de compatibilidad

Si desea obtener la lista completa de sistemas operativos navegadores web, consulte las *notas de la versión*.

Requisitos del sistema

RAM

- Necesario: 1 GB
- Recomendado: 2 GB o más

Velocidad del procesador

- Necesario: 1 unidad física a 2 GHz o superior (tecnología Hyper-Thread y doble núcleo)
- Recomendado: Más de 1 unidad física a más de 3 GHz (tecnología Hyper-Thread y doble núcleo o superior)

Espacio en la unidad de disco duro del ordenador

- Al menos 60 GB de espacio de almacenamiento disponibles

Resolución de pantalla

- Al menos 1024 x 768 píxeles (sólo para clientes MVE)

Servidores de bases de datos admitidos

- Firebird
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

Notas:

- La aplicación admite únicamente las versiones de 32 bits y contiene una base de datos de Firebird preconfigurada.
- El servidor de base de datos donde MVE esté instalado deberá tener únicamente una *tarjeta de interfaz de red* (NIC).

Instalación de Markvision

Con Markvision, puede utilizar Firebird o Microsoft SQL Server como base de datos back-end.

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

- Active la autenticación en modo mixto y la ejecución automática.
- Establezca las bibliotecas de red para utilizar un puerto estático y sockets TCP/IP.
- Cree una cuenta de usuario que Markvision utilizará para crear el esquema y las conexiones de la base de datos.

- Cree las siguientes bases de datos:
  - FRAMEWORK
  - MONITOR
  - QUARTZ

  Nota: asegúrese de que la cuenta de usuario que ha creado es la propietaria de estas bases de datos o tiene los privilegios adecuados para crear un esquema y realizar operaciones de *lenguaje de manipulación de datos* (DML).

1 Descomprima los archivos de instalación en una ruta que *no* contenga espacios.

2 Inicie **setup.exe** y, a continuación, siga las instrucciones de la pantalla del ordenador.

Actualización a la última versión de Markvision

La actualización está concebida para funcionar únicamente desde la versión inmediatamente anterior.

1 Realice una copia de seguridad de la base de datos.

  Notas:

  - Si utiliza una base de datos Firebird, consulte “Copia de seguridad de la base de datos Firebird” en la página 9 para obtener más información.
  - Si utiliza MS SQL Server, póngase en contacto con su administrador de MS SQL.

2 Descomprima los archivos de instalación en una ubicación temporal y asegúrese de que la ruta *no* contiene espacios.

3 Inicie el archivo **setup.exe** y siga las instrucciones que se indican en la pantalla del equipo.

Copia de seguridad y restauración de la base de datos Firebird

Copia de seguridad de la base de datos Firebird

Nota: Si utiliza MS SQL Server como base de datos, póngase en contacto con su administrador de MS SQL.

1 Pare el dispositivo Markvision Enterprise.

  a Haga clic en o en **Inicio** > **Configuración**.

  b Seleccione **Panel de control** y, si es necesario, haga clic en **Sistema & Seguridad**.

  c Haga doble clic en **Herramientas administrativas**.

  d Si es necesario, haga doble clic en **Servicios de componentes**.

  e Haga doble clic en **Servicios**.

  f En el panel Servicios, seleccione **Markvision Enterprise** y, a continuación, haga clic en **Detener**.

2 Localice la carpeta en la que se instaló Markvision Enterprise y navegue a firebird\data.

  Por ejemplo, `C:\Archivos de programa\Lexmark\Markvision Enterprise\firebird\data`

3 Copie las bases de datos siguientes a un repositorio seguro.

  - FRAMEWORK.FDB
  - MONITOR.FDB

- QUARTZ.FDB

4 Reinicie el servicio Markvision Enterprise.

   a Repita los pasos del **1a** a **1e**.

   b En el panel Servicios, seleccione **Markvision Enterprise** y, a continuación, haga clic en **Reiniciar**.

Restauración de la base de datos Firebird

1 Asegúrese de que ha finalizado el proceso de copia de seguridad de la base de datos Firebird.

2 Pare el dispositivo Markvision Enterprise.

   Para obtener más información, consulte paso 1 de “Copia de seguridad de la base de datos Firebird” en la página 9.

3 Localice la carpeta en la que se instaló Markvision Enterprise y navegue a firebird\data.

   Por ejemplo, **`C:\Archivos de programa\Lexmark\Markvision Enterprise\firebird\data`**

4 Sustituya las bases de datos siguientes con bases de datos que haya guardado durante la compleción del proceso de copia de seguridad.

   - FRAMEWORK.FDB
   - MONITOR.FDB
   - QUARTZ.FDB

5 Reinicie el servicio Markvision Enterprise.

   Para obtener más información, consulte paso 4 de “Copia de seguridad de la base de datos Firebird” en la página 9.

Acceso a Markvision

1 Abra un navegador web y escriba **`http://`*`MVE_SERVER`*`:9788/mve/`** en el campo de URL.

   Nota: Sustituya ***`MVE_SERVER`*** por el nombre de host o la dirección IP de la máquina que aloja Markvision.

2 En el campo Usuario, escriba **`admin`**.

3 En el campo Contraseña, escriba **`Administrator1`** y, a continuación, haga clic en **Conectar**.

   Nota: Para cambiar la contraseña, haga clic en **Cambiar contraseña** en la esquina superior derecha de la pantalla de inicio.

Si Markvision está inactivo durante más de 30 minutos, la sesión se cerrará automáticamente. Deberá volver a iniciar sesión para acceder a Markvision.

Migración de MarkVision Professional a Markvision Enterprise

Nota: Markvision Enterprise (MVE) sólo admite la migración de datos desde MarkVision Professional (MVP) v11.2.1.

Exportación de datos de MVP

Uso de la página web del servidor de MVP

1 Abra un navegador web y, a continuación, escriba **`http://MVP_SERVER:9180/~MvServer`** en el campo URL.

Nota: sustituya ***`MVP_SERVER`*** por la dirección IP o el nombre de host del servidor de MVP.

2 En la página web del servidor de MarkVision, haga clic en la opción de **directorio de datos**.

3 Introduzca el nombre de usuario y la contraseña si se le indica.

4 En la página de descarga de directorio de datos, haga clic en para descargar los datos de MVP en un archivo zip.

5 Guarde el archivo zip.

Uso del sistema de archivos

1 En el sistema que ejecuta el servidor de MVP, desplácese a la ubicación en la que está instalado dicho servidor.

2 Comprima la carpeta de datos en un archivo zip.

Importación de datos a MVE

1 Conéctese a Markvision Enterprise.

2 En el cuadro de diálogo “Importar datos de MarkVision Professional”, haga clic en **Sí** y, a continuación, haga clic en **Examinar**.

Notas:

- Si hace clic en **Sí**, el cuadro de diálogo no aparecerá la próxima vez que se conecte a MVE.
- Si hace clic en **No** y no desea volver a ver el cuadro de diálogo, seleccione **No volver a mostrar este mensaje**.

3 Desplácese a la ubicación en la que está almacenado el archivo zip y, a continuación, haga clic en **Abrir**.

4 En el área “Datos para importación”, seleccione el tipo de datos que desea importar.

Datos	Detalles
Usuarios	• En MarkVision Professional, a los usuarios se les otorgan privilegios para funciones individuales. • En Markvision Enterprise, se les asignan funciones asociadas a otras diferentes. • A todos los usuarios importados de MVP se les asignan automáticamente todas las funciones, excepto **`ROLE_ADMIN`**. • Si la contraseña de un usuario de MVP no cumple los criterios de contraseña de MVE, la cadena **`Administrator1`** se agrega a la contraseña actual del usuario.

Datos	Detalles
Disposi-tivos	• MVE sólo importa información de dispositivo básica de MVP, incluidos el nombre del modelo, el número de serie, la dirección MAC y la dirección IP. • Si ya existe una impresora en MVE, ésta se ignora durante la importación. • Durante la importación, MVE pasa por alto las impresoras conectadas a adaptadores de red externos (ENA), ya que MVE no admite actualmente ENA. • Los dispositivos importados se establecen automáticamente en el estado de duración **Administrado (normal)**. • MVP administra impresoras y servidores de impresión. MVE sólo administra impresoras. Por lo tanto, dos entradas en MVP se convierten en una única entrada en MVE.
Perfiles de búsqueda	• Cuando se importan perfiles de MVP al sistema MVE, sólo se importan los siguientes detalles: – Nombre de comunidad SNMP – Reintentos – Tiempo\ de\ espera – Dirección de exclusión – Dirección de inclusión • En MVP, cada entrada de inclusión/exclusión contiene un juego de nombres de comunidad SNMP de lectura/escritura. Un perfil que contiene varias entradas de inclusión/exclusión también puede contener varios juegos de nombres de comunidad de lectura/escritura únicos. En MVE, el juego de nombres de comunidad de lectura/escritura pertenece al propio perfil. Cada perfil puede contener solamente un juego de nombres de comunidad de lectura/escritura. Por lo tanto, un perfil de búsqueda en MVP (contiene varios juegos de nombres de comunidad de lectura/escritura únicos) se divide en varios perfiles de búsqueda al importarse a MVE (cada uno contiene un juego de nombres de comunidad de lectura/escritura). El número de perfiles en MVE es igual que el número de juegos de nombres de comunidad de lectura/escritura únicos en el perfil de MVP original. • Para el tiempo de espera, MVE convierte el tiempo de espera de MVP en milisegundos multiplicando el valor de MVP (en segundos) por 1.000. • La opción de administración automática se establece en `Falso` durante la importación.

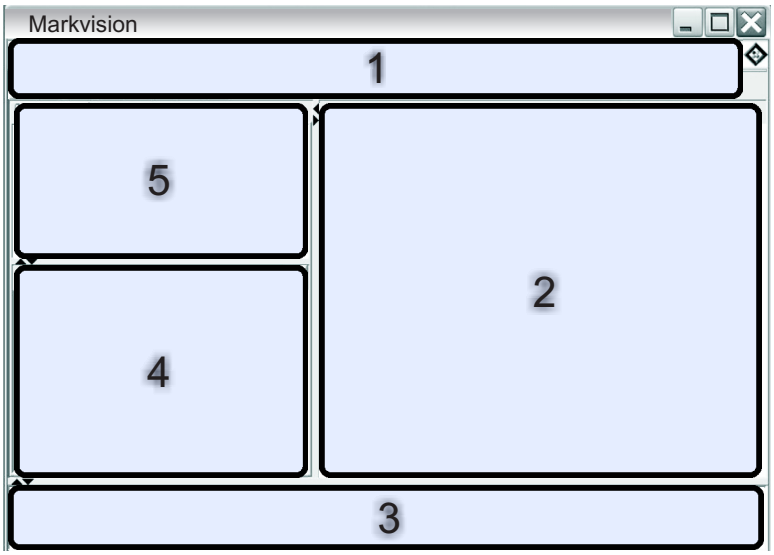
5 Haga clic en **Importar**.

Uso de Markvision

Las características y funciones de Markvision se dividen en cuatro ámbitos de servicio. Esto ofrece una mayor facilidad de uso al garantizar que la vista de la interfaz sólo incluye las características y funciones necesarias para la tarea disponibles. Se puede acceder a todos los ámbitos de servicio a través de una ficha en la pantalla de inicio; cada uno de estos ámbitos corresponde a una fase de la duración del servicio en la versión 3 de la biblioteca de infraestructuras de tecnologías de la información (ITIL, Information Technology Infrastructure Library). La disciplina ITIL es conocida mundialmente por su compilación de mejores prácticas para la administración de recursos de TI en una organización.

Utilice esta ficha	Para
Activos	Buscar, identificar, clasificar, organizar y realizar un seguimiento de los activos físicos (impresoras y dispositivos multifunción) que forman la flota de impresión. Aquí, puede obtener y mantener información sobre los modelos, las capacidades, las opciones instaladas y la duración de la flota. En ITIL, esto se incluye en el área Transición de mantenimiento. Si una de las responsabilidades incluye la administración de activos de TI, vaya a “Administración de activos” en la página 18.
Directrices	Definir y administrar la configuración de software de la flota de impresión. Aquí, puede asignar una política definida que especifica los valores de configuración concretos para cada modelo. Puede controlar si la flota de impresión cumple con las políticas y aplicarlas cuando sea necesario. En ITIL, esto se incluye en el área Transición de mantenimiento. Si una de las responsabilidades incluye la administración y el mantenimiento de las herramientas de gestión de configuración, vaya a “Administración de políticas” en la página 30.
Servicio de mantenimiento	Interactuar directamente con un único dispositivo de la flota de impresión. Aquí, puede administrar el dispositivo de forma remota, comprobar el cumplimiento de políticas y aplicarlas, así como personalizar los valores de configuración a través del Embedded Web Server del dispositivo. En ITIL, esto se incluye en el área Funcionamiento del servicio. Si una de las responsabilidades incluye la administración del servicio de asistencia de TI, vaya a “Administración de la asistencia técnica” en la página 43.
Gestor de incidencias	Crear un evento automatizado cuando un dispositivo envía una alerta a la red. Puede elegir entre enviar un correo electrónico o realizar otras acciones con scripts para notificar al personal identificado. En ITIL, esto se incluye en el área Funcionamiento del servicio. Si una de las responsabilidades incluye la administración de problemas o incidentes, vaya a “Administración de eventos de dispositivo” en la página 45.

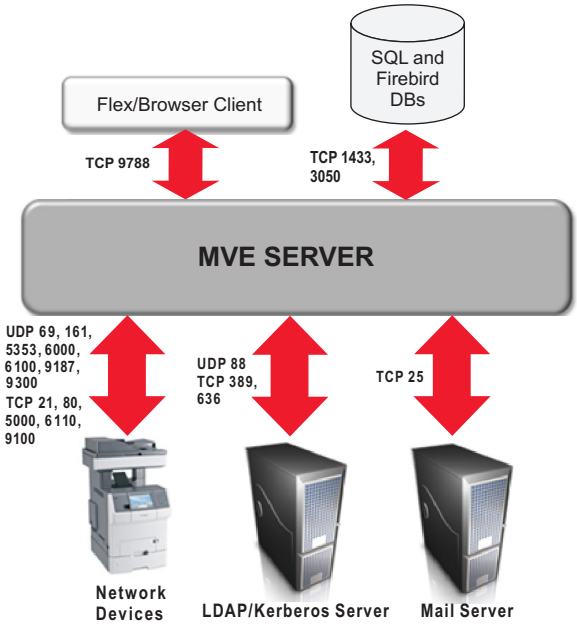
Comprensión de la pantalla principal



Utilice esta área		Para
1	Cabecera	Acceder a las cuatro fichas del ámbito de servicio y realizar otras tareas administrativas.
2	Resultados de búsqueda	Ver la lista paginada completa de dispositivos que coinciden con la selección actual del marcador o la búsqueda.
3	Información de la tarea	Ver el estado de la actividad más reciente.
4	Resumen de los resultados de búsqueda	Ver un resumen clasificado de la selección actual del marcador o la búsqueda.
5	Marcadores y búsqueda avanzada	Administrar y seleccionar marcadores, así como redefinir consultas de búsqueda.

Descripción de puertos y protocolos

Markvision utiliza diferentes puertos y protocolos para los distintos tipos de comunicación de red, como se muestra en el diagrama siguiente.



Nota: Los puertos son bidireccionales y deben estar abiertos o activos para que Markvision funciones correctamente. Asegúrese de que todos los puertos de dispositivo se han establecido en **Seguro e inseguro** o **Activado**, en función del dispositivo.

Comunicación del servidor al dispositivo

Estos son los puertos y protocolos utilizados durante la comunicación del servidor de Markvision a los dispositivos de red.

Protocolo	Servidor de Markvision	Dispositivo	Se utiliza para
NPAP *Network Printer Alliance Protocol*	Puerto de *protocolo de datagramas de usuario* (UDP) efímero	UDP 9300	Comunicación con impresoras de red Lexmark
XMLNT *XML Network Transport* (Almacén de objetos)	Puertos de *protocolo de control de transmisión* (TCP) y UDP efímeros	UDP 6000 TCP 5000	Comunicación con impresoras de red Lexmark
LST *Lexmark Secure Transport*	UDP 6100 Puerto TCP efímero (intercambio)	UDP 6100 TCP 6110 (intercambio)	Comunicación codificada con impresoras de red Lexmark
mDNS *Multicast Domain Name System*	Puerto UDP efímero	UDP 5353	Búsqueda de determinadas impresoras de red Lexmark y determinación de los recursos de seguridad de los dispositivos
SNMP *Protocolo simple de administración de redes*	Puerto UDP efímero	UDP 161	Búsqueda y comunicación con impresoras de red Lexmark y de terceros

Protocolo	Servidor de Markvision	Dispositivo	Se utiliza para
FTP *Protocolo de transferencia de archivos*	Puerto TCP efímero	TCP 21	Descargas de archivos genéricos
TFTP *Protocolo trivial de transferencia de archivos*	Puerto UDP efímero	UDP 69	Descargas de actualizaciones de firmware y archivos genéricos
HTTP *Protocolo de transferencia de hipertexto*	Puerto TCP efímero	TCP 80	Descargas de archivos genéricos
Raw Print Port	Puerto TCP efímero	TCP 9100	Descargas de archivos genéricos

Comunicación del dispositivo al servidor

Este es el puerto y protocolo utilizado durante la comunicación de los dispositivos de red al servidor de Markvision.

Protocolo	Dispositivo	Servidor de Markvision	Se utiliza para
NPAP	UDP 9300	UDP 9187	Generar y recibir alertas

Comunicación del servidor a la base de datos

Estos son los puertos utilizados durante la comunicación del servidor de Markvision a las bases de datos.

Servidor de Markvision	Base de datos	Se utiliza para
Puerto TCP efímero	TCP 1433 (SQL Server) Este es el puerto predeterminado, que puede configurar el usuario.	Comunicación con una base de datos de SQL Server
Puerto TCP efímero	TCP 3050	Comunicación con una base de datos Firebird

Comunicación del cliente al servidor

Este es el puerto y protocolo utilizado durante la comunicación del cliente flex/navegador al servidor de Markvision.

Protocolo	Cliente flex/navegador	Servidor de Markvision
AMF *ActionScript Message Format*	Puerto TCP	TCP 9788

Mensajería y avisos

Este es el puerto y protocolo utilizado durante la comunicación del servidor de Markvision a un servidor de correo.

Protocolo	Servidor de Markvision	Servidor SMTP	Se utiliza para
SMTP *Protocolo simple de transferencia de correo*	Puerto TCP efímero	TCP 25 Este es el puerto predeterminado, que puede configurar el usuario.	Proporcionar la función de correo electrónico que se utiliza para recibir alertas de los dispositivos

Comunicación del servidor de Markvision al servidor LDAP

Estos son los puertos y protocolos utilizados durante la comunicación que implica grupos de usuarios y funcionalidad de autenticación.

Protocolo	Servidor de Markvision	Servidor LDAP	Se utiliza para
LDAP *Protocolo ligero de acceso a directorios*	Puerto TCP efímero	TCP 389 o el puerto en el que se ha configurado el servidor LDAP para escuchar	Autenticación de usuarios de Markvision Enterprise que utilizan un servidor LDAP
LDAPS *Protocolo ligero de acceso seguro a directorios*	Puerto TCP efímero	*Transport Layer Security* (TLS) o el puerto en el que se ha configurado el servidor LDAP para escuchar Se utiliza para conexiones TLS cifradas.	Autenticación de usuarios de Markvision Enterprise que utilizan un servidor LDAP a través de un canal seguro mediante TLS
Kerberos	Puerto UDP efímero	UDP 88 Este es el puerto predeterminado del servicio de autenticación Kerberos.	Autenticación Kerberos

Administración de activos

Búsqueda de dispositivos

La aplicación permite buscar dispositivos en la red. Cuando se encuentran dispositivos, la información de identificación correspondiente se almacena en el sistema. Utilice marcadores o búsquedas para visualizar los dispositivos en el área Resultados de búsqueda.

Los dispositivos encontrados están establecidos, de forma predeterminada, en **Nuevo** y no los administra el sistema. Antes de realizar una acción en un dispositivo, debe establecerlo en **Administrado**. Para obtener más información, consulte “Administración de dispositivos” en la página 21.

Hay dos formas de agregar dispositivos al sistema:

- **Utilizar un perfil de búsqueda**: busque dispositivos en la red mediante parámetros personalizados.
- **Importar dispositivos de un archivo**: utilice un archivo de *valores separados por comas* (CSV) para importar dispositivos.

Nota: Solo puede utilizar uno de estos dos métodos. Si realiza ambos procedimientos para añadir dispositivos al sistema, se duplicarán los dispositivos.

Después de añadir un dispositivo al sistema, realícele una auditoría inmediatamente. La realización de una auditoría proporciona información adicional sobre el dispositivo, que es necesaria para poder completar correctamente algunas tareas. Para obtener más información sobre la auditoría de un dispositivo, consulte “Auditoría de un dispositivo” en la página 21.

Nota: Nota: Esto se aplica *únicamente* a dispositivos sin restringir. Para dispositivos restringidos, asigne primero una política de seguridad y ejecútela en los dispositivos restringidos antes de realizar una auditoría. En caso de no hacerlo, se producirá un error de auditoría y se definirá el estado de los dispositivos restringidos a **(Administrado) falta**. Para obtener más información sobre dispositivos restringidos, consulte “Descripción de los dispositivos seguros” en la página 32.

Creación de un perfil de búsqueda

1. Si es necesario, en la ficha Activos, haga clic en **Perfiles de búsqueda** para acceder a la sección de perfiles de búsqueda.
2. Haga clic en ✚ y, a continuación, escriba el nombre del nuevo perfil de búsqueda.
3. En la ficha Direcciones, seleccione **Incluir** o **Excluir**.
4. Para importar una lista de elementos de un archivo para incluirlos o excluirlos, realice las siguientes acciones:
   a. Haga clic en ↶.
   b. Desplácese a la carpeta en la que está guardado el archivo.
   c. Seleccione el archivo y haga clic en **Abrir**.

Nota: El archivo puede contener cualquiera de los patrones que se pueden introducir en el campo de texto sobre Dirección/Rango. Para ver ejemplos de un patrón válido, desplace el ratón sobre el campo de texto.

5. Junto a ✚, escriba la dirección IP, el nombre de host DNS completo, las subredes con caracteres comodín o los rangos de direcciones que desee y, a continuación, haga clic en ✚.

Notas:

- Solo puede escribir una entrada cada vez. Para ver ejemplos de una entrada válida, desplace el ratón sobre el campo de texto sobre Dirección/Rango.
- Al escribir los rangos de direcciones, *no* utilice caracteres comodín.
- Para eliminar una entrada, selecciónela y, a continuación, haga clic en —.

6 Haga clic en la ficha **SNMP** y, a continuación, seleccione **Versión 1,2c** o **Versión 3**.

Nota: Si no está seguro de qué versión de SNMP está utilizando, póngase en contacto con el personal de asistencia técnica.

7 Si selecciona **Versión 1,2c** en paso 6, especifique el perfil de privacidad en el área Nombres de comunidad.

Si selecciona **Versión 3**, especifique el perfil de seguridad en el área Seguridad.

Nota: Si no está seguro de cómo configurar el perfil de seguridad de SNMP Version 3, póngase en contacto con el personal de asistencia técnica.

8 Haga clic en la ficha **General** y, a continuación, en el área Rendimiento, haga lo siguiente:

- En el campo Tiempo de espera, especifique la cantidad de tiempo (en milisegundos) que desee esperar para que respondan los dispositivos.
- En el campo Reintentos, especifique el número de reintentos antes de que el sistema deje de intentar comunicarse con un dispositivo.

9 Seleccione si desea incluir dispositivos seguros en la búsqueda.

Notas:

- Si no cuenta con un dispositivo seguro, *no* seleccione esta opción. Si lo hace, se obtendría una penalización de rendimiento, que supone una mayor duración del proceso de búsqueda de dispositivos.
- Cuando un dispositivo es seguro, se aplica una de las condiciones siguientes o ambas: (a) los puertos de comunicación se desactivan y (b) se requiere autenticación para obtener información del dispositivo.

10 Seleccione si desea que el perfil de búsqueda administre automáticamente los dispositivos encontrados.

Nota: Si selecciona esta opción, todos los dispositivos encontrados se establecen automáticamente en el estado **Administrado**.

11 Haga clic en **Guardar** >**Cerrar**.

Notas:

- Al hacer clic en ▶ se ejecuta el perfil de búsqueda y *no* se guarda.
- Un nuevo perfil de búsqueda obtiene solo la información suficiente para identificar un dispositivo de forma fiable. Para obtener la información completa de un dispositivo, establézcalo en el estado **Administrado** y, a continuación, realice una auditoría del mismo.
- Para asegurarse de que la información del dispositivo es actual, se puede programar una búsqueda para que se realice de forma regular. Para obtener más información, consulte “Programación de tareas” en la página 56.

Edición o eliminación de un perfil de búsqueda

1 En la pestaña Activos, haga clic en **Perfiles de búsqueda** para acceder a la sección de perfiles de búsqueda.

2 Seleccione un perfil y haga clic en para editar el perfil de búsqueda o en — para eliminarlo.

3 Siga las instrucciones que aparecen en la pantalla del ordenador.

importación de dispositivos desde un archivo

Utilice un archivo de valores separados por comas (CSV) para importar dispositivos.

Nota: Durante la preparación de una implementación, Markvision permite agregar dispositivos al sistema incluso *antes* de que éstos estén disponibles en la red.

1 En la ficha Activos, haga clic en **Importar** y, a continuación, en **Examinar**.

2 Desplácese a la carpeta en la que está almacenado el archivo CSV.

   Nota: asegúrese de que cada línea del archivo CSV representa un único dispositivo.

3 Seleccione el archivo CSV y haga clic en **Abrir**.

4 En la sección Posibles columnas, seleccione las columnas de forma que coincidan con los valores del archivo CSV.

5 Si está utilizando el protocolo SNMP V3 para comunicarse con el dispositivo, *debe* seleccionar las siguientes columnas:
   - **SNMP V3 Datos de escritura/lectura**
   - **SNMP V3 Contraseña contra lectura/escritura**
   - **SNMP V3 Nivel de autenticación mínimo**
   - **SNMP V3 Hash de autenticación**
   - **SNMP V3 Algoritmo de privacidad**

   Nota: En el archivo CSV que ha seleccionado en paso 3, asegúrese de que los siguientes parámetros contienen cualquiera de los valores especificados a continuación debajo de ellos:
   - Nivel de autenticación mínimo
     - `SIN_AUTENTICACIÓN_SIN_PRIVACIDAD`
     - `AUTENTICACIÓN_SIN_PRIVACIDAD`
     - `AUTENTICACIÓN_PRIVACIDAD`
   - Hash de autenticación
     - `MD5`
     - `SHA1`
   - Algoritmo de privacidad
     - `DES`
     - `AES_128`
     - `AES_192`
     - `AES_256`

   Nota: Si el archivo CSV no contiene los valores exactos especificados, MVE no puede detectar el dispositivo.

6 Haga clic en **Agregar** para mover las columnas seleccionadas a la sección Columnas del archivo CSV.
   - Si desea que el sistema ignore una columna del archivo CSV, seleccione **Ignorar**. Realice este proceso con cada columna del archivo CSV que no aparezca en la sección Posibles columnas.
   - Para cambiar el orden de las columnas seleccionadas para que coincidan con el archivo CSV, seleccione una columna de la sección Columnas del archivo CSV y, a continuación, utilice las flechas para mover las cabeceras hacia arriba o hacia abajo.

7 Seleccione si desea que la primera fila del archivo CSV incluya una cabecera.

8 Seleccione si desea que los dispositivos importados se establezcan automáticamente en el estado de duración **Administrado**.

9 Haga clic en **Aceptar**.

Administración de dispositivos

A un dispositivo se le pueden asignar tres estados de duración diferentes:

- **Administrado**: incluye el dispositivo en todas las actividades que se pueden realizar en el sistema.
  - **Administrado (normal)**: el dispositivo tiene un estado fijo.
  - **Administrado (modificado)**: hay cambios en las propiedades físicas del dispositivo desde la última auditoría. La próxima vez que el sistema se comunique con el dispositivo y no haya más cambios en sus propiedades físicas, el dispositivo volverá al estado Administrado (normal).
  - **Administrado (falta)**: el sistema no puede comunicarse correctamente con el dispositivo. La próxima vez que el sistema pueda comunicarse correctamente con el dispositivo y no haya ningún cambio en sus propiedades físicas, el dispositivo volverá al estado Administrado (encontrado).
  - **Administrado (encontrado)**: anteriormente faltaba el dispositivo, pero ha podido comunicarse correctamente con el sistema en el último intento. La próxima vez que el sistema pueda comunicarse correctamente con el dispositivo y no haya ningún cambio en sus propiedades físicas, el dispositivo volverá al estado Administrado (normal).
- **No administrado**: excluye el dispositivo de todas las actividades realizadas en el sistema.
- **Retirado**: el dispositivo estaba anteriormente en el estado Administrado, pero ahora se ha eliminado de la red. El sistema conserva la información del dispositivo, pero no espera volver a detectarlo en la red. Si el dispositivo aparece de nuevo en la red, el sistema establecerá su estado en Nuevo.

Establecimiento del estado de duración del dispositivo

Antes de realizar una acción en el dispositivo, asegúrese de que éste se ha establecido en **Administrado**.

1 En la ficha Activos, seleccione la opción de **nuevas impresoras** del menú desplegable Marcadores y búsquedas.

2 Active la casilla de verificación situada junto a la dirección IP del dispositivo.

Nota: puede seleccionar varios o todos los dispositivos.

3 En el menú desplegable “Establecer estado en”, seleccione **Administrado** y, a continuación, haga clic en **Sí**.

Auditoría de un dispositivo

Una auditoría recopila información de cualquier dispositivo gestionado de la red y la almacena en el sistema. Para asegurarse de que la información del sistema es actual, realice una auditoría regularmente.

1 En el área Resultados de búsqueda, active la casilla de verificación situada junto a la dirección IP de un dispositivo.

Notas:

- Si no conoce la dirección IP del dispositivo, búsquelo en la columna Nombre del sistema o Nombre de host.
- Para auditar varios dispositivos, active las casillas de verificación situadas junto a las direcciones IP correspondientes.

- Para auditar todos los dispositivos, active la casilla de verificación situada junto a "Dirección IP".

2 Haga clic en **Auditoría**.

El estado de la auditoría aparece en el área de información de la tarea.

3 Cuando la auditoría haya terminado, haga clic en en el área Cabecera.

Los resultados de la auditoría más reciente aparecen en el cuadro de diálogo Registro.

Después de auditar los dispositivos, las instancias siguientes pueden pedir al sistema que establezca un dispositivo en estado **Administrado (modificado)**:

- Hay cambios en cualquiera de estos valores de identificación de dispositivos o capacidades de dispositivos:
  - Etiqueta de propiedad
  - Nombre de host
  - Nombre de contacto
  - Ubicación de contacto
  - Dirección IP
  - Tamaño de la memoria
  - Nombre de opción de la fotocopiadora
  - Impresión a doble cara
- Hay adiciones o supresiones en cualquiera de estas opciones de hardware:
  - Suministros
  - Opciones de entrada
  - Opciones de salida
  - Puertos
- Hay adiciones o supresiones en cualquiera de estas aplicaciones o funciones de dispositivo:
  - Fuentes
  - Aplicaciones eSF

Nota: Una auditoría se puede programar para que se realice a una hora determinada o de forma regular. Para obtener más información, consulte “Programación de tareas” en la página 56.

Visualización de propiedades de los dispositivos

Para ver la lista completa de información sobre el dispositivo, asegúrese de que ya ha realizado una auditoría del mismo.

1 En la ficha Activos, seleccione la opción de **impresoras administradas** en el menú desplegable Marcadores y búsquedas.

2 En la sección Todas las impresoras, seleccione la dirección IP del dispositivo.

Nota: si no conoce la dirección IP del dispositivo, búsquelo en la columna Nombre del sistema.

3 En el cuadro de diálogo Propiedades del activo:

Haga clic en	Para ver
Identificación	La información de identificación de la red del dispositivo.
Fechas	La lista de eventos del dispositivo. Aquí se incluye la fecha de adición al sistema, la fecha de búsqueda y la fecha de la auditoría más reciente.

Haga clic en	Para ver
Firmware	Los niveles de código de firmware del dispositivo.
Capacidades	Las características del dispositivo.
Puertos	Los puertos disponibles en el dispositivo.
Suministros	Los datos y los niveles de suministro del dispositivo.
Cartuchos de fuentes	Información sobre los cartuchos de fuentes instalados.
Opciones	Información sobre las opciones del dispositivo, como el disco duro y el espacio libre restante.
Opciones de entrada	Los valores de las bandejas de papel disponibles y otros dispositivos de entrada.
Opciones de salida	Los valores de las bandejas de salida de papel disponibles.
Aplicaciones eSF	Información sobre las aplicaciones *Embedded Solutions Framework* (eSF) instaladas en el dispositivo, como el número de versión y el estado.
Estadísticas del dispositivo	Los valores específicos de todas las propiedades del dispositivo.
Cambiar detalles	Información sobre las modificaciones del dispositivo. **Nota:** Esto *solo* se aplica a dispositivos que se establezcan en el estado **Administrado (modificado)**.

Búsqueda y organización de dispositivos en el sistema

Búsqueda de dispositivos en el sistema

Uso de marcadores predeterminados

Los marcadores indican la búsqueda de un dispositivo guardada. Cuando se selecciona un marcador, los dispositivos que se muestran coinciden con los criterios de búsqueda.

Los marcadores predeterminados se basan en el estado del ciclo de vida útil del dispositivo.

1 En el menú desplegable Marcadores y búsquedas, seleccione un marcador:

Seleccionar	Para
Impresoras administradas	Buscar dispositivos activos en el sistema. **Nota:** Los dispositivos que aparecen al seleccionar este marcador pueden tener cualquiera de los siguientes estados: • Administrado (normal) • Administrado (modificado) • Administrado (falta) • Administrado (encontrado)
Impresoras administradas (normales)	Buscar dispositivos activos en el sistema con las mismas propiedades del dispositivo que en la última auditoría.
Impresoras administradas (modificadas)	Buscar dispositivos activos en el sistema con las propiedades del dispositivo que han cambiado en la última auditoría.
Impresoras administradas (faltan)	Buscar dispositivos con los que el sistema no pudo establecer comunicación.
Impresoras administradas (encontradas)	Buscar dispositivos que faltaban en las solicitudes de búsqueda anteriores, pero que ahora se han encontrado.
Nuevas impresoras	Buscar dispositivos que se han añadido al sistema por primera vez.
Impresoras no administradas	Buscar dispositivos que se han marcado para excluirlos en las actividades llevadas a cabo en el sistema.
Impresoras retiradas	Buscar dispositivos que ya no están activos en el sistema.

2 En el área Resumen de los resultados de búsqueda, seleccione un criterio para afinar de forma rápida y sencilla los resultados de la búsqueda marcada.

Uso de la búsqueda avanzada

La función Búsqueda avanzada le permite realizar búsquedas complejas basadas en uno o varios parámetros.

1 En el menú desplegable Marcadores y búsquedas, seleccione **Búsqueda avanzada**.

2 Seleccione si tiene que coincidir con un criterio o con todos.

3 Para añadir un criterio de búsqueda, haga clic en ✚.

Para agrupar criterios de búsqueda, haga clic en [+] y, a continuación, haga clic en ✚ para añadir criterios individuales.

Nota: Si agrupa criterios de búsqueda, el sistema unirá todos los criterios definidos como grupo en un solo criterio.

4 En el menú desplegable Parámetro, seleccione un parámetro:

Seleccionar	Para
Etiqueta de activo	Buscar dispositivos que tienen asignada una etiqueta de activo.
Capacidad de color	Buscar dispositivos por su capacidad de imprimir a color.
Ubicación de contacto	Buscar dispositivos que tienen una ubicación específica.
Nombre de contacto	Buscar dispositivos que tengan un nombre de contacto especificado.
Capacidad de copia	Buscar dispositivos por su capacidad de copiar archivos.
Capacidad dúplex	Buscar dispositivos por su capacidad de realizar impresiones a doble cara.
Capacidad de eSF	Buscar dispositivos por su capacidad para administrar una aplicación Embedded Solutions Framework (eSF).
Aplicación eSF (Nombre)	Buscar dispositivos por el nombre específico de la aplicación eSF instalada actualmente.
Aplicación eSF (estado)	Buscar dispositivos por el estado actual de la aplicación eSF instalada.
Aplicación eSF (Versión)	Buscar dispositivos por la versión de la aplicación eSF instalada.
Versión del firmware	Buscar dispositivos por la versión de firmware.
Firmware: AIO	Buscar dispositivos por el valor de AIO de su firmware.
Firmware: base	Buscar dispositivos por la versión base de firmware.
Firmware: motor	Buscar dispositivos por el motor del firmware.
Firmware: fax	Buscar dispositivos por el valor de fax del firmware.
Firmware: fuente	Buscar dispositivos por el valor de fuente del firmware.
Firmware: núcleo	Buscar dispositivos por el valor de núcleo del firmware.
Firmware: cargador	Buscar dispositivos por el valor de cargador del firmware.
Firmware: red	Buscar dispositivos por el valor de red del firmware.
Firmware: controlador de red	Buscar dispositivos por el valor de controlador de red del firmware.
Firmware: panel	Buscar dispositivos por la versión del panel del firmware.
Firmware: escáner	Buscar dispositivos por la versión del escáner del firmware.
Nombre de host	Buscar dispositivos por los nombres de host.
Dirección IP	Buscar dispositivos por las direcciones IP. **Nota:** Puede utilizar un asterisco (`*`) como un carácter comodín en los tres últimos octetos de la dirección IP para encontrar todas las direcciones IP que coincidan. Si se utiliza un asterisco en el octeto, los octetos restantes también deben contener asteriscos. • Algunos ejemplos válidos son `157.184.32.*`, `157.184.*.*`y `157.*.*.*`. • Un *ejemplo no válido* es `157.184.*.10`.
Palabra clave	Buscar dispositivos por las palabras clave asignadas, si las hay.

Seleccionar	Para
Número total de páginas impresas	Buscar dispositivos por los valores de número de páginas de duración.
Dirección MAC	Buscar dispositivos por las direcciones MAC.
Contador de mantenimiento	Buscar dispositivos por el valor del contador de mantenimiento.
Fabricante	Buscar dispositivos por el nombre del fabricante.
Capacidad de impresora multifunción	Buscar dispositivos por su capacidad para ser una impresora multifunción (MFP).
Tecnología de marca	Buscar dispositivos por el valor de la tecnología de marca que admiten.
Model	Buscar dispositivos por los nombres del modelo.
Estado de la impresora	Buscar dispositivos por su estado actual (por ejemplo: `Lista`, `Atasco de papel`, `Falta bandeja 1`).
Capacidad de perfil	Buscar dispositivos por la capacidad de perfil admitida.
Capacidad de recepción de fax	Buscar dispositivos por su capacidad para recibir faxes entrantes.
Capacidad de digitalización para correo electrónico	Buscar dispositivos por su capacidad para realizar una tarea de digitalización de correo electrónico.
Capacidad de digitalización para fax	Buscar dispositivos por su capacidad para realizar una tarea de digitalización de fax.
Capacidad de digitalización para red	Buscar dispositivos por su capacidad para realizar una tarea de digitalización de red.
Número de serie	Buscar dispositivos por el número de serie.
Estado	Buscar dispositivos por su estado actual en la base de datos.
Estado de suministro	Buscar dispositivos por el estado actual de los suministros.
Nombre del sistema	Buscar dispositivos por los nombres del sistema.

5 En el menú desplegable Operación, seleccione un operador:

Seleccionar	Para
Contiene	Buscar dispositivos con un parámetro que contiene un valor específico.
No contiene	Buscar dispositivos con un parámetro que no contiene un valor específico.
No es igual	Buscar dispositivos con un parámetro que no es equivalente a un valor exacto.
Finaliza con	Buscar dispositivos con un parámetro que termina con un valor específico.
Igual	Buscar dispositivos con un parámetro que es equivalente a un valor exacto.
Comienza con	Buscar dispositivos con un parámetro que empieza con un valor específico.

6 En el campo o menú desplegable Valor, introduzca el valor del parámetro.

Nota: Si desea eliminar el criterio, haga clic en **X**.

7 Haga clic en **Aceptar** para iniciar la búsqueda.

   Los dispositivos encontrados aparecen en el área Resultados de búsqueda.

8 En el área Resumen de los resultados de búsqueda, seleccione un criterio para afinar de forma rápida y sencilla los resultados de la búsqueda marcada.

Trabajo con marcadores

Los marcadores indican una búsqueda guardada.

Cuando un dispositivo accede al sistema y cumple los criterios especificados por un marcador, se incluye en los resultados de búsqueda cada vez que se selecciona el marcador.

Creación de marcadores

1 En el menú desplegable Marcadores y búsquedas, seleccione el marcador que representa el grupo de dispositivos desde el que desea iniciar la búsqueda.

   Para redefinir la búsqueda, haga clic en **Búsqueda avanzada**.

2 Si es necesario, en el resumen de los resultados de búsqueda, haga clic en las subcategorías disponibles para redefinir aún más la búsqueda.

3 Cuando el dispositivo o grupo de dispositivos que desea aparezca en la ventana de búsqueda, haga clic en .

4 Introduzca un nombre para el marcador y, a continuación, haga clic en **Aceptar**.

Acceso a marcadores

1 En el menú desplegable Marcadores y búsquedas, seleccione el marcador que desea ver.

2 Si es necesario, en el resumen de los resultados de búsqueda, haga clic en las subcategorías disponibles para redefinir aún más la búsqueda.

Eliminación de marcadores

1 En el menú desplegable Marcadores y búsquedas, seleccione **Administrar marcadores**.

2 Seleccione los marcadores que desea eliminar y, a continuación, haga clic en —.

3 Haga clic en **Sí** y, a continuación, haga clic en **Cerrar**.

Uso de categorías y palabras clave

Las palabras clave permiten asignar etiquetas personalizadas a dispositivos, lo que proporciona una flexibilidad adicional en la búsqueda y organización de dispositivos en el sistema. Agrupe las palabras clave en categorías y, a continuación, asigne varias palabras clave de varias categorías a un dispositivo.

Antes de crear una palabra clave, cree primero una categoría a la que pertenecerá dicha palabra clave.

Por ejemplo, puede crear una categoría denominada **Ubicación** y, a continuación, crear palabras clave dentro de esa categoría. Algunos ejemplos de palabras clave dentro de la categoría Ubicación pueden ser **Edificio 1**, **Edificio 2** o algo más específico para las necesidades de la empresa.

Después de crear las categorías y palabras clave, podrá asignar estas últimas a varios dispositivos. Puede buscar dispositivos basándose en las palabras clave que tienen asignadas y, a continuación, asignar un marcador a los resultados de la búsqueda para un uso posterior.

Adición, edición o eliminación de categorías

1. Si es necesario, en la ficha Activos, haga clic en **Palabras clave** para mostrar la sección correspondiente.
2. En el panel Categoría, haga clic en ✚ para agregar, en ✎ para editar o en — para eliminar una categoría.

   Nota: al eliminar una categoría también se eliminan las palabras clave y se suprimen de los dispositivos a los que se han asignado las palabras clave.
3. Siga las instrucciones que aparecen en la pantalla del ordenador.

Adición, edición o eliminación de palabras clave

1. Si es necesario, en la ficha Activos, haga clic en **Palabras clave** para mostrar la sección correspondiente.
2. En el panel Palabras clave, realice una de las siguientes acciones:
   - Para agregar una palabra clave:
     - **a** En el panel Categoría, seleccione la categoría a la que pertenece la palabra clave.
     - **b** En el panel Palabra clave, haga clic en ✚.
     - **c** Escriba el nombre de la nueva palabra clave y, a continuación, pulse **Intro**.
   - Para editar una palabra clave:
     - **a** Seleccione una palabra clave existente y, a continuación, haga clic en ✎.
     - **b** Edite el nombre y, a continuación, pulse **Intro**.
   - Para eliminar una palabra clave:
     - **a** Seleccione una palabra clave existente y, a continuación, haga clic en —.
     - **b** Haga clic en **Sí**.

Nota: al eliminar una palabra clave, se elimina también de los dispositivos a los que se ha asignado.

Asignación de palabras clave a un dispositivo

1. Si es necesario, en la ficha Activos, haga clic en **Palabras clave** para mostrar la sección Palabras clave y, a continuación, seleccione una.

   Nota: para seleccionar varias palabras clave, utilice **Mayús** + **clic** o bien **Ctrl** + **clic**.
2. Active la casilla de verificación situada junto a la dirección IP del dispositivo al que desea que se asigne la palabra clave.

   Nota: puede seleccionar varios o todos los dispositivos.
3. Haga clic en ✚📌.

4 En el área de información de la tarea, compruebe que la tarea ha terminado.

5 Para comprobar si la palabra clave se ha asignado correctamente al dispositivo, consulte las propiedades de éste último seleccionando su dirección IP.

En la sección de propiedad de identificación, aparece el nuevo valor de la palabra clave para el dispositivo.

Eliminación de palabras clave asignadas de dispositivos

1 En la ficha Activos, active la casilla de verificación situada junto a la dirección IP del dispositivo del que desea eliminar una palabra clave.

2 Si es necesario, haga clic en **Palabras clave** para mostrar la sección Palabras clave.

3 Seleccione una palabra clave y, a continuación, haga clic en .

4 Seleccione la palabra clave que desea eliminar y, a continuación, haga clic en **Aceptar**.

Nota: para seleccionar varias palabras clave, utilice **Mayús** + **clic** o bien **Ctrl** + **clic**.

5 En el área de información de la tarea, compruebe que la tarea ha terminado.

6 Para comprobar si la palabra clave se ha eliminado correctamente del dispositivo, haga lo siguiente:

a Seleccione la dirección IP del dispositivo.

b En la sección de propiedad de identificación, asegúrese de que la palabra clave ya no aparece.

Administración de políticas

Una política es un conjunto de información de configuración que se puede asignar a un dispositivo o grupo de dispositivos del mismo modelo. Compruebe que la información de configuración de un dispositivo o grupo de dispositivos coincide con la política concreta realizando una comprobación de cumplimiento. Si la comprobación de cumplimiento indica que el dispositivo no cumple con la política, puede elegir aplicar dicha política en el dispositivo o grupo de dispositivos.

Cree políticas mediante un tipo funcional predefinido:

- Copiar
- Correo electrónico/FTP
- Fax
- Unidad flash
- Firmware
- General
- Red
- Papel
- Imprimir
- Seguridad

  Nota: Para obtener más información sobre la política de seguridad, consulte “Descripción de la política de seguridad” en la página 31.

Cada tipo de política contiene configuración exclusiva que garantiza que la configuración conflictiva no se produzca cuando se asignan varios tipos de políticas a un dispositivo.

Creación de políticas

Creación de nuevas políticas

1. Si es necesario, en la ficha Políticas, haga clic en **Políticas de dispositivos** para mostrar la sección correspondiente.
2. Haga clic en ✚ y, a continuación, escriba el nombre de la nueva política.

   Nota: asegúrese de que el nombre de la política de cada modelo de dispositivo sea único y no exista ya en la base de datos.
3. En la lista Modelos admitidos, seleccione un dispositivo.
4. En el menú desplegable Tipo, seleccione un tipo de política y, a continuación, haga clic en **Aceptar**.
5. En el cuadro de diálogo Nueva política, active la casilla de verificación **Nombre del ajuste**.

   Todos los valores se seleccionan automáticamente, lo que permite personalizarlos.
6. Desactive la casilla de verificación situada junto a un valor para *excluirlo* al llevar a cabo una comprobación de cumplimiento o tarea de aplicación de política.
7. Seleccione un valor para cada ajuste que desee incluir al llevar a cabo una comprobación de cumplimiento o tarea de aplicación de política.
8. Haga clic en **Guardar**.

Creación de políticas desde dispositivos

1 En la ficha Políticas, active la casilla de verificación situada junto a la dirección IP del dispositivo.

2 Haga clic en **Políticas de dispositivos** para mostrar la sección Políticas de dispositivos y, a continuación, haga clic en .

3 En el campo Nombre, escriba el nombre de la nueva política.

4 Seleccione el tipo de política y, a continuación, haga clic en **Aceptar**.

Nota: también puede seleccionar varios o todos los tipos de políticas.

5 Si es necesario, edite los valores de la política recién creada.

a En la sección Políticas de dispositivos, seleccione el nombre de la política recién creada y, a continuación, haga clic en .

b Seleccione un valor para cada ajuste que desee incluir al llevar a cabo una comprobación de cumplimiento o tarea de aplicación de política.

c Desactive la casilla de verificación situada junto a un valor para *excluirlo* al llevar a cabo una comprobación de cumplimiento o tarea de aplicación de política.

d Haga clic en **Guardar**.

6 Asegúrese de que los valores de la política recién creada contienen valores válidos.

Si la política aparece en texto de color rojo y su nombre empieza por un signo de exclamación, no se puede asignar a un dispositivo. Esto significa que uno o varios ajustes de la política contienen un valor no válido y, por lo tanto, no se puede aplicar en un dispositivo en su estado actual.

Para que una política se pueda asignar a un dispositivo, realice las siguientes acciones:

a Seleccione la política y, a continuación, haga clic en .

b Introduzca un valor válido para los ajustes y, a continuación, haga clic en **Guardar**.

c Si aparece un mensaje de advertencia, anote los ajustes con valores no válidos.

d Haga clic en **No** y, a continuación, introduzca un valor válido para cada uno de los ajustes especificados.

e Haga clic en **Guardar**.

f Si es necesario, repita del paso c al paso e hasta que deje de aparecer el mensaje de advertencia.

Descripción de la política de seguridad

Markvision puede configurar la configuración de los dispositivos Lexmark compatibles con seguridad, incluida la configuración de seguridad de las variadas funciones de dispositivo y también el modo de realizar la comunicación remota.

Cuando utilice la política de seguridad, asegúrese de utilizar *solo* Markvision para administrar la configuración de seguridad en sus dispositivos. Si utiliza algún otro sistema junto con Markvision, se producirá un comportamiento inesperado.

La política de seguridad se puede asignar solo a un subconjunto específico de dispositivos. Si desea obtener la lista completa de dispositivos admitidos, consulte las *notas de la versión*.

Descripción de los dispositivos seguros

Puede haber varias configuraciones para un dispositivo seguro. Sin embargo, actualmente Markvision solo admite dispositivos que sean *completamente sin restringir* o *completamente restringidos*.

Configuraciones de dispositivos completamente sin restringir y completamente restringidos

		Completamente sin restringir	Completamente restringidos
Valores del dispositivo	*Control de acceso a función de administración remota* (RM FAC) o contraseña avanzada **Nota:** Encontrará una lista de dispositivos compatibles con RM FAC en "Impresoras Lexmark compatibles con la política de seguridad" en las *notas de la versión*.	Sin seguridad o sin contraseña	RM FAC se ha establecido con una plantilla de seguridad, o se ha configurado una contraseña
	Puertos relevantes	Los siguientes puertos están abiertos: • UDP 161 (SNMP) • UDP 9300/9301/9302 (NPAP)	Cerrado
	Puertos relativos a la seguridad	Los siguientes puertos están abiertos: • UDP 5353 (mDNS) • TCP 6110 • TCP/UDP 6100 (LST)	Los siguientes puertos están abiertos: • UDP 5353 (mDNS) • TCP 6110 • TCP/UDP 6100 (LST)

		Completamente sin restringir	Completamente restringidos
Configuración de Markvision	Perfil de búsqueda	Asegúrese de que la opción **Incluir impresoras con seguridad en la búsqueda** está deseleccionada.	Asegúrese de que la opción **Incluir impresoras con seguridad en la búsqueda** está seleccionada.
	¿Se utilizan los canales seguros en la comunicación entre Markvision y los dispositivos de red?	No **Notas:** • Se recomienda este tipo de configuración, a menos que esté especialmente preocupado por la seguridad de la comunicación de red. • Una excepción sería que hubieran ciertos valores que *solo* se pudieran leer/escribir a través de canales seguros.	Sí
	¿Cómo determinar la configuración de seguridad de los dispositivos de la red?	En la cuadrícula de datos principal de Markvision, se muestra un icono de candado *abierto* junto a la dirección IP de un dispositivo completamente sin restringir.	En la cuadrícula principal de Markvision, se muestra un icono de candado *cerrado* junto a la dirección IP de un dispositivo completamente restringido. **Nota:** Si Markvision no conoce los credenciales de comunicación del dispositivo, entonces una barra roja atraviesa el icono de candado. Esto significa que Markvision no puede comunicarse con el dispositivo más allá de la búsqueda mínima.
	¿Cómo se buscan dispositivos que tienen este tipo de configuración?	**1** En el área “Marcadores y búsqueda avanzada”, seleccione **Todas las impresoras**. **2** En el área de resumen de los resultados de búsqueda, desplácese a la categoría Comunicaciones y seleccione **Sin seguridad**.	**1** En el área “Marcadores y búsqueda avanzada”, seleccione **Todas las impresoras**. **2** En el área de resumen de los resultados de búsqueda, desplácese a la categoría Comunicaciones y seleccione **Seguro**.

Notas:

- Si el dispositivo o el perfil de búsqueda no se adhiere a uno de estos casos, es probable que se produzca un comportamiento inesperado o indefinido.
- Asegúrese de que el dispositivo está en el estado correcto y que se ha configurado correctamente el perfil de búsqueda *antes* de buscar el dispositivo. Si cambia alguno de los dos después de ejecutar el perfil de búsqueda, es probable que se produzca un comportamiento inesperado o indefinido.

Descripción de la configuración para políticas de seguridad

Utilice la política de seguridad para personalizar la configuración de seguridad de un dispositivo de red.

Para que Markvision realice eficazmente funciones de administración remotas en un dispositivo de red, asegúrese de que la política de seguridad se adhiere a los parámetros siguientes:

- En la sección Configuración general de la política de seguridad, la configuración de acceso de los siguientes puertos se ha establecido en **Activada** o en **Proteger y desproteger**:
  - Acceso de puerto: mDNS (UDP 5353)
  - Acceso de puerto: TCP/UDP (6110/6100)
- En la sección Controles de acceso (si existe en el modelo del dispositivo), la configuración de Cambios de configuración del adaptador de red NPA y Actualizaciones de firmware se han establecido en **Sin seguridad**.
- Las siguientes secciones (si existen en el modelo del dispositivo) son de solo lectura y no se pueden editar:
  - Controles de acceso
  - Plantillas de seguridad

    Nota: Los bloques de la columna Configuración de autenticación pueden necesitar los credenciales proporcionados.
  - Otra configuración

  Nota: Las secciones Controles de acceso, Plantillas de seguridad y Otra configuración no están disponibles en todos los modelos de dispositivo. Para obtener más información, consulte “Impresoras Lexmark compatibles con la política de seguridad” en las *notas de la versión*.

Uso de bloques desde una aplicación eSF

Si desea utilizar el bloque desde una aplicación de *Marco de soluciones incrustado* (eSF) para la política de seguridad, asegúrese primero de que la aplicación eSF se haya instalado manualmente en todos los dispositivos afectados. Markvision *no* aplica la instalación de la aplicación cuando aplica una política de seguridad.

Nota: Solo la configuración interna disponible para todas las aplicaciones eSF se duplicará, se comprobará su conformidad o se aplicará mediante la política de seguridad.

Creación de una política de seguridad

Para crear una política de seguridad, duplique primero una política existente de un dispositivo maestro preconfigurado.

Duplicación de una política de seguridad para restringir dispositivos

Paso 1. Configure un dispositivo para restringirlo mediante Embedded Web Server.

Después de configurar un dispositivo para restringirlo, utilice ese dispositivo como dispositivo maestro que duplicará para una política de seguridad.

1. Si el modelo de dispositivo es compatible con el control de acceso de administración remota, establezca dicho control de acceso en una plantilla de seguridad existente. Si el modelo de dispositivo no es compatible con el control de acceso de administración remota, configure una contraseña avanzada. Realice una de las siguientes acciones:

   Nota: Encontrará una lista de dispositivos compatibles con el control de acceso de administración remota, consulte “Impresoras Lexmark compatibles con la política de seguridad” en las *notas de la versión*.

   Configuración del control de acceso de administración remota

   a. Desde Markvision, haga clic en **Servicio de mantenimiento**.
   b. Localice el dispositivo que desea configurar y seleccione su dirección IP.
   c. Haga clic en **Página web incrustada** > **Configuración** >**Seguridad** >**Configuración de seguridad**.

d Desde la sección Configuración de seguridad avanzada, haga clic en **Controles de acceso**.

e Desplácese hasta Administración remota y seleccione una plantilla de seguridad del menú desplegable.

Nota: La plantilla de seguridad debe especificar solo autenticación.

f Haga clic en **Enviar**.

Configuración de contraseñas avanzadas

a Desde Markvision, haga clic en **Servicio de mantenimiento**.

b Localice el dispositivo que desea configurar y seleccione su dirección IP.

c Haga clic en **Página web incrustada** >**Configuración** >**Seguridad**.

d Haga clic en **Crear/Cambiar contraseña** o en **Crear contraseña**.

e Si es necesario, haga clic en **Crear contraseña avanzada** y, a continuación, escriba una contraseña.

f Confirme la contraseña volviendo a escribirla en el campo siguiente y haga clic en **Enviar**.

2 Asegúrese de que los puertos relevantes estén cerrados y los puertos de seguridad estén abiertos.

Nota: Si procede, puede seleccionar **Modo seguro** e ir directamente a paso 3.

a En el servidor Embedded Web Server, haga clic en **Valores** o **Configuración** y, a continuación, en **Seguridad** >**Acceso a puerto TCP/IP**.

b Localice los puertos relevantes siguientes y, si es necesario, desmarque las casillas de verificación situadas junto a ellos o seleccione **Desactivado** en los menús desplegables.

- **UDP 161 (SNMP)**
- **UDP 9300/9301/9302 (NPAP)**

c Localice los siguientes puertos de seguridad y asegúrese de que las casillas de verificación situadas junto a ellos están marcadas, o de seleccionar **Proteger y desproteger** en los menús desplegables.

- **UDP 5353 (mDNS)**
- **TCP 6110**
- **TCP/UDP 6100 (LST)**

d Haga clic en **Enviar**.

3 Configuración de otros ajustes de seguridad.

a En el servidor Embedded Web Server, haga clic en **Valores** o **Configuración** y, a continuación, en **Seguridad**.

b Realice otros cambios en la configuración de seguridad según convenga.

c Tras realizar otros cambios, haga clic en **Valores** o **Configuración** y, a continuación, en **Seguridad** >**Ver resumen de seguridad** (si existen en el modelo del dispositivo).

d Compruebe que los cambios se reflejan en la página de resumen.

Nota: Si usa una contraseña avanzada en lugar del control de acceso de administración remota, no tendrá que usar el servidor Embedded Web Server para restringir el dispositivo maestro. Puede usar Markvision para crear una política de seguridad en cualquier dispositivo y, a continuación, configurar la contraseña avanzada y los valores del puerto en la sección Configuración general de la política.

Paso 2. Asegúrese de que Markvision reconoce su dispositivo restringido maestro.

1 Creación de perfiles de búsqueda. Para obtener más información sobre la creación de un perfil de búsqueda, consulte “Creación de un perfil de búsqueda” en la página 18.

2 Desde el cuadro de diálogo “Perfil de búsqueda: Añadir”, asegúrese de que **Incluir impresoras con seguridad en la búsqueda** está seleccionado.

3 Para ejecutar el perfil de búsqueda, haga clic en ▶.

Nota: En este punto, el dispositivo está "parcialmente descubierto". Esto significa que Markvision ha descubierto el dispositivo con información limitada, pero no podrá realizar funciones adicionales con él, tales como conformidad de política, aplicación de política y auditoría. Para adquirir su información completa, necesita proporcionar los credenciales de comunicación del dispositivo.

Paso 3. Inicie el proceso de duplicado.

1 Desde Markvision, haga clic en **Políticas**.

2 Localice su dispositivo restringido maestro y seleccione la casilla de verificación situada junto a su dirección IP.

3 Si es necesario, haga clic en **Políticas de dispositivo** y, luego, en .

4 En el campo Nombre, escriba el nombre de la nueva política de seguridad.

5 Asegúrese de que se ha seleccionado el tipo de política de Seguridad.

6 Introduzca los credenciales requeridos para autenticarse en el dispositivo y luego haga clic en **Aceptar**.

Nota: Utilice los credenciales de la plantilla de seguridad que ha definido en el control de acceso de administración remota o utilice la contraseña avanzada configurada.

7 Permita que se complete el proceso de duplicación.

Si la política se muestra en texto rojo, significa que faltan credenciales y, por lo tanto, no se puede asignar a un dispositivo en su estado actual. Para hacer que una política se pueda asignar a un dispositivo, introduzca los credenciales correctos para el dispositivo.

8 Edite la configuración de la nueva política de seguridad y asegúrese de que la configuración en la política contiene valores válidos.

a En la sección Políticas de dispositivos, seleccione el nombre de la política y haga clic en .

b Seleccione un valor para cada ajuste que desee incluir al llevar a cabo una comprobación de cumplimiento o tarea de aplicación de política.

c Desactive la casilla de verificación situada junto a un valor para *excluirlo* al llevar a cabo una comprobación de cumplimiento o tarea de aplicación de política.

d Escriba la contraseña de seguridad y haga clic en **Guardar**.

Nota: Para obtener más información sobre configuración válida para una política de seguridad, consulte “Descripción de la configuración para políticas de seguridad” en la página 33.

9 Asigne la política de seguridad a dispositivos sin restringir del mismo modelo que el dispositivo restringido maestro.

Para obtener más información sobre la asignación de una política a varios dispositivos, consulte “Asignación de políticas” en la página 41.

10 Aplique la política de seguridad a los dispositivos seleccionados.

Para obtener más información sobre la aplicación de una política, consulte “Aplicación de políticas” en la página 41.

11 Vuelva a buscar los dispositivos.

Ahora los dispositivos están restringidos. Además, ahora Markvision conoce los credenciales de comunicación del dispositivo y puede utilizarlos para ejecutar tareas en las áreas de servicio Activos y Políticas.

Duplicación de una política de seguridad para quitar la restricción de dispositivos

Paso 1. Configure un dispositivo para quitarle la restricción mediante Embedded Web Server.

Después de configurar un dispositivo para quitarle la restricción, utilice ese dispositivo como dispositivo maestro que duplicará para una política de seguridad.

1 Si el modelo de dispositivo es compatible con el control de acceso de administración remota, establezca dicho control de acceso en **Sin seguridad**. Si el modelo de dispositivo no es compatible con el control de acceso de administración remota, quite la contraseña avanzada. Realice una de las siguientes acciones:

Nota: Encontrará una lista de dispositivos compatibles con el control de acceso de administración remota, consulte “Impresoras Lexmark compatibles con la política de seguridad” en las *notas de la versión*.

Configuración del control de acceso de administración remota

a Desde Markvision, haga clic en **Servicio de mantenimiento**.

b Localice el dispositivo que desea configurar y seleccione su dirección IP.

c Haga clic en **Página web incrustada** > **Configuración** >**Seguridad** >**Configuración de seguridad**.

d Desde la sección Configuración de seguridad avanzada, haga clic en **Controles de acceso**.

e Desplácese hasta **`Administración remota`** y, a continuación, seleccione **Sin seguridad** en el menú desplegable.

f Haga clic en **Enviar**.

Eliminación de la contraseña avanzada

a Desde Markvision, haga clic en **Servicio de mantenimiento**.

b Localice el dispositivo que desea configurar y seleccione su dirección IP.

c Haga clic en **Página web incrustada** >**Configuración** >**Seguridad**.

d Haga clic en **Crear/Cambiar contraseña** o en **Crear contraseña**.

e Si es necesario, haga clic en **Crear contraseña avanzada**.

f Borre los campos de contraseña y haga clic en **Enviar**.

2 Asegúrese de que los puertos relevantes y de seguridad estén abiertos.

a En el servidor Embedded Web Server, haga clic en **Valores** o **Configuración** y, a continuación, en **Seguridad** >**Acceso a puerto TCP/IP**.

b Localice los siguientes puertos y asegúrese de que están seleccionados, o de que están establecidos en **Proteger y desproteger**.

Puertos relevantes

- **UDP 161 (SNMP)**
- **UDP 9300/9301/9302 (NPAP)**

Puertos de seguridad

- **UDP 5353 (mDNS)**
- **TCP 6110**
- **TCP/UDP 6100 (LST)**

c Haga clic en **Enviar**.

3 Configuración de otros ajustes de seguridad.

a En el servidor Embedded Web Server, haga clic en **Valores** o **Configuración** y, a continuación, en **Seguridad**.

b Realice otros cambios en la configuración de seguridad según convenga.

c Tras realizar otros cambios, haga clic en **Valores** o **Configuración** y, a continuación, en **Seguridad** >**Ver resumen de seguridad** (si existen en el modelo del dispositivo).

d Compruebe que los cambios se reflejan en la página de resumen.

Nota: Si usa una contraseña avanzada en lugar del control de acceso de administración remota, no tendrá que usar el servidor Embedded Web Server para quitar la restricción del dispositivo maestro. Puede usar Markvision para crear una política de seguridad en cualquier dispositivo y, a continuación, configurar la contraseña avanzada y los valores del puerto en la sección Configuración general de la política.

Paso 2. Asegúrese de que Markvision reconoce su dispositivo sin restringir maestro.

1 Creación de perfiles de búsqueda. Para obtener más información sobre la creación de un perfil de búsqueda, consulte “Creación de un perfil de búsqueda” en la página 18.

2 En el cuadro de diálogo “Perfil de búsqueda – Añadir”, asegúrese de desmarcar la casilla de verificación **Incluir impresoras con seguridad en la búsqueda**.

3 Para ejecutar el perfil de búsqueda, haga clic en ▶.

Paso 3. Inicie el proceso de duplicado.

1 Desde Markvision, haga clic en **Políticas**.

2 Localice su dispositivo sin restringir y seleccione la casilla de verificación situada junto a su dirección IP.

3 Si es necesario, haga clic en **Políticas de dispositivo** y, luego, en .

4 En el campo Nombre, escriba el nombre de la nueva política de seguridad.

5 Asegúrese de que se ha seleccionado el tipo de política de Seguridad.

6 Introduzca los credenciales requeridos para autenticarse en el dispositivo y luego haga clic en **Aceptar**.

Nota: Utilice los credenciales de la plantilla de seguridad que ha definido en el control de acceso de administración remota o utilice la contraseña avanzada configurada.

7 Permita que se complete el proceso de duplicación.

Si la política se muestra en texto rojo, significa que faltan credenciales y, por lo tanto, no se puede asignar a un dispositivo en su estado actual. Para hacer que una política se pueda asignar a un dispositivo, introduzca los credenciales correctos para el dispositivo.

8 Edite la configuración de la nueva política de seguridad y asegúrese de que la configuración de la política contiene valores válidos.

   a En la sección Políticas de dispositivos, seleccione el nombre de la política y haga clic en .

   b Seleccione un valor para cada ajuste que desee incluir al llevar a cabo una comprobación de cumplimiento o tarea de aplicación de política.

   c Desactive la casilla de verificación situada junto a un valor para *excluirlo* al llevar a cabo una comprobación de cumplimiento o tarea de aplicación de política.

   d Haga clic en **Guardar**.

   Nota: Para obtener más información sobre configuración válida para una política de seguridad, consulte "Descripción de la configuración para políticas de seguridad" en la página 33.

9 Asigne la política de seguridad a dispositivos sin restringir del mismo modelo que el dispositivo sin restringir maestro.

   Notas:

   - Para obtener más información sobre la asignación de una política a varios dispositivos, consulte "Asignación de políticas" en la página 41.
   - Si uno de los dispositivos seleccionados está restringido, se volverá sin restringir después de aplicar la política.

10 Aplique la política de seguridad a los dispositivos seleccionados.

   Para obtener más información sobre la aplicación de una política, consulte "Aplicación de políticas" en la página 41.

11 Vuelva a buscar los dispositivos.

Ahora los dispositivos están sin restringir y se pueden utilizar en todas las áreas de servicio.

Modificación de los credenciales de comunicación de un dispositivo restringido

Los *Credenciales de comunicación* son necesarios para autenticarse en un dispositivo de red mediante Lexmark Secure Transport (LST). Los credenciales de comunicación pueden ser una combinación de las siguientes opciones: nombre de usuario, dominio, contraseña y *número de identificación personal* (PIN).

Nota: Algunos modelos de dispositivos solo admiten contraseñas. Para obtener más información, consulte "Impresoras Lexmark compatibles con la política de seguridad" en las *notas de la versión*.

Hay dos tipos de bloques de credenciales de comunicación:

- **Autoridad final**: el bloque es la autoridad final en lo referente a autorización y autenticación de credenciales. Algunos ejemplos son las contraseñas o los PIN.
- **Autoridad intermedia**: el bloque pasa los credenciales a una autoridad externa de autenticación y autorización. Ejemplos de autoridad externa son *Lightweight Directory Access Protocol* (LDAP) y Kerberos.

Modificación de los credenciales de un bloque de autoridad final

Nota: Las opciones de la política de seguridad Controles de acceso y Plantillas de seguridad no están disponibles en todos los modelos de dispositivo. Para obtener más información, consulte “Impresoras Lexmark compatibles con la política de seguridad” en las *notas de la versión*.

1. Si es necesario, en la ficha de políticas, haga clic en **Políticas de dispositivos** para mostrar la sección Políticas de dispositivos.
2. Seleccione la política de seguridad restringida que desee y haga clic en >**Controles de acceso**.
3. Localice **Administración remota** y anote su valor.
4. Haga clic en **Plantillas de seguridad**.
5. En la columna Configuración de autenticación, seleccione el bloque junto al valor que ha anotado en paso 3.
6. En el campo Contraseña, escriba la nueva contraseña.
7. Confirme la contraseña volviéndola a escribir en el campo siguiente y haga clic en **Guardar**.
8. Aplique la política de seguridad restringida a sus dispositivos asociados.

   Cuando se complete correctamente la tarea de aplicación, se actualizarán los credenciales de comunicación del dispositivo.

Modificación de los credenciales de un bloque de autoridad intermedia

1. Desde la autoridad externa que utilice, realice las modificaciones a los credenciales.
2. En la página web de Markvision, haga clic en **Políticas** >**Políticas de dispositivo** para mostrar la sección Políticas de dispositivos.
3. Seleccione la política de seguridad restringida que desee y haga clic en >**Credenciales de dispositivo**.
4. En la sección Credenciales de dispositivo, actualice los valores actuales a los valores nuevos que ha introducido en la autoridad externa
5. Haga clic en **Guardar**.
6. Aplique la política de seguridad restringida a sus dispositivos asociados.

   Cuando se complete correctamente la tarea de aplicación, Markvision podrá comunicarse con los dispositivos de nuevo.

Edición o eliminación de políticas

1. Si es necesario, en la ficha Políticas, haga clic en **Políticas de dispositivos** para mostrar la sección correspondiente.
2. Seleccione una política y, a continuación, realice una de las siguientes acciones:
   - Para editar la política, haga clic en .
     - **a** En el campo Nombre de política, escriba el nuevo nombre de la política, si corresponde.
     - **b** Seleccione un valor para cada ajuste que desee incluir al llevar a cabo una comprobación de cumplimiento o tarea de aplicación de política.
     - **c** Desactive la casilla de verificación situada junto a un valor para *excluirlo* al llevar a cabo una comprobación de cumplimiento o tarea de aplicación de política.
     - **d** Haga clic en **Guardar**.

- Para eliminar la política, haga clic en — y, a continuación, haga clic en **Sí**.

Asignación de políticas

1 Si es necesario, en la ficha Políticas, haga clic en **Políticas de dispositivos** para mostrar la sección correspondiente.

2 Seleccione una política.

Notas:

- Para seleccionar varias políticas, utilice **Mayús** + **clic** o bien **Ctrl** + **clic**.
- Puede asignar varios tipos de políticas a un dispositivo al mismo tiempo, pero sólo puede utilizar una política para cada tipo.

3 Active la casilla de verificación situada junto a la dirección IP del dispositivo al que desea que se asigne la política.

Nota: también puede seleccionar varios o todos los dispositivos.

4 Haga clic en .

En la columna Tipo de política, aparece un signo de interrogación junto al dispositivo seleccionado.

El signo de interrogación indica que el dispositivo no se ha verificado aún para saber si cumple con la política asignada.

Comprobación de cumplimiento con políticas

1 En la ficha Políticas, active la casilla de verificación situada junto a la dirección IP del dispositivo.

Nota: también puede seleccionar varios o todos los dispositivos.

2 Haga clic en **Cumplimiento**.

3 En el cuadro de diálogo Políticas de comprobación de cumplimiento, seleccione un tipo de política y, a continuación, haga clic en **Aceptar**.

4 En la columna Tipo de política, compruebe que aparece una marca de verificación junto al dispositivo seleccionado.

5 Si aparece un signo de interrogación o una X, haga clic en para ver datos específicos.

Nota: la comprobación de cumplimiento de política se puede programar para que se realice a una hora determinada o de forma regular. Para obtener más información, consulte “Programación de tareas” en la página 56.

Aplicación de políticas

1 En la ficha Políticas, active la casilla de verificación situada junto a la dirección IP del dispositivo.

Nota: también puede seleccionar varios o todos los dispositivos.

2 Haga clic en **Aplicar**.

3 En el cuadro de diálogo Aplicar políticas, seleccione un tipo de política y, a continuación, haga clic en **Aceptar**.

4 Haga clic en para comprobar que la aplicación de política ha terminado.

Nota: la tarea de aplicación de política se puede programar para que se realice a una hora determinada o de forma regular. Para obtener más información, consulte “Programación de tareas” en la página 56.

Eliminación de políticas

1 En la ficha Políticas, active la casilla de verificación situada junto a la dirección IP del dispositivo.

2 Si es necesario, haga clic en **Políticas de dispositivos** para mostrar la sección correspondiente y, a continuación, haga clic en .

3 En el cuadro de diálogo Eliminar política, seleccione una política y, a continuación, haga clic en **Aceptar**.

Nota: También puede seleccionar varias políticas.

Administración de la asistencia técnica

Trabajo con políticas

Antes de intentar resolver un problema en un dispositivo, asegúrese primero de que el dispositivo cumple con las políticas asignadas.

Comprobación del cumplimiento de los dispositivos con las políticas

1. En la pestaña Asistencia técnica, seleccione la casilla de verificación que hay junto a la dirección IP del dispositivo.

   Nota: puede seleccionar varios o todos los dispositivos.

2. Haga clic en **Cumplimiento**.
3. En el cuadro de diálogo Políticas de comprobación de cumplimiento, seleccione un tipo de política y, a continuación, haga clic en **Aceptar**.
4. Espere a que la tarea se complete en la zona de información sobre tareas.
5. Haga clic en para ver los resultados de la comprobación de cumplimiento.

Aplicación de políticas

1. En la pestaña Asistencia técnica, seleccione la casilla de verificación que hay junto a la dirección IP del dispositivo.

   Nota: puede seleccionar varios o todos los dispositivos.

2. Haga clic en **Aplicar**.
3. En el cuadro de diálogo Aplicar políticas, seleccione un tipo de política y, a continuación, haga clic en **Aceptar**.
4. Espere a que la tarea se complete en la zona de información sobre tareas.
5. Haga clic en para comprobar que se ha completado la aplicación de la política.

Trabajo con dispositivos

Comprobación del estado de un dispositivo

1. Busque un dispositivo mediante las opciones Marcadores o Búsqueda avanzada.

   Nota: puede utilizar las categorías del área de resumen de los resultados de búsqueda para limitar la lista de dispositivos encontrados.

2. Active la casilla de verificación situada junto a la dirección IP del dispositivo y, a continuación, haga clic en **Recopilar estado actual**.
3. En las columnas Estado de la impresora y Estado de suministro, observe el icono situado junto al dispositivo.

Icono	Estado
	Correcto: el dispositivo está listo y los suministros son suficientes.
	Advertencia: el dispositivo funciona, pero puede que queden pocos suministros o que éstos requieran atención más adelante.
	Error: el dispositivo o los suministros requieren atención inmediatamente.

4 Haga clic en **Trabajar con dispositivo** para ver detalles sobre el estado del dispositivo.

Visualización de dispositivos de forma remota

Nota: esta característica sólo está disponible para dispositivos que admiten la visualización remota.

1 En la ficha Asistencia técnica, active la casilla de verificación situada junto a la dirección IP del dispositivo.

2 Haga clic en **Trabajar con dispositivo**.

Aparece un cuadro de diálogo que muestra los datos y una imagen del dispositivo.

3 Haga clic en **Panel del operador remoto** > **Haga clic aquí para continuar**.

Aparece otro cuadro de diálogo que muestra, de forma remota, una visualización dinámica del panel de control del dispositivo en su estado actual.

4 En el lateral inferior izquierdo, observe el equivalente a las teclas de un teclado para cada uno de los comandos de botón del dispositivo.

Nota: la ubicación del equivalente a las teclas de un teclado puede diferir según el modelo del dispositivo.

Visualización de la página web incorporada

Nota: esta característica sólo está disponible para dispositivos que admiten la visualización remota de la página web incorporada.

1 En la ficha Asistencia técnica, active la casilla de verificación situada junto a la dirección IP del dispositivo.

2 Haga clic en **Trabajar con dispositivo**.

Aparece un cuadro de diálogo que muestra los datos y una imagen del dispositivo.

3 Haga clic en **Página web incorporada**.

Nota: en la parte inferior del cuadro de diálogo, también puede seleccionar el idioma que desea utilizar.

Administración de eventos de dispositivo

El administrador de eventos permite controlar y administrar de forma proactiva la flota de impresión. Defina un destino donde notificarle o notificar a otros usuarios especificados los incidentes concretos que se produzcan. Crear un evento automatizado cuando un dispositivo envía una alerta a la red.

Creación de un destino

Un destino es una acción predefinida que ejecuta una serie de comandos cuando se produce un determinado evento en un grupo de dispositivos. Puede tratarse de una notificación por correo electrónico o una solicitud de línea de comandos cuando se requiere una acción personalizada.

1. En la ficha Administrador de eventos, haga clic en **Destinos** para acceder a la sección de destinos.
2. Haga clic en ✚ y, a continuación, escriba un nombre único para el destino.
3. Realice uno de los procedimientos siguientes:
   - Seleccione **Comando** y, a continuación, haga clic en **Siguiente**.
     a. Introduzca el nombre de un comando ejecutable en la casilla Ruta de acceso de comandos.
     b. Añada palabras clave a los parámetros del comando seleccionando una palabra clave de la lista Marcadores de posición y, a continuación, haga clic en ▶.
   - Seleccione **Correo electrónico** y, a continuación, haga clic en **Siguiente**.
     a. Asegúrese de haber configurado correctamente los ajustes de correo electrónico en el cuadro de diálogo Configuración del sistema.
     Para obtener más información, consulte “Configuración de los valores del correo electrónico” en la página 48.
     b. Introduzca valores en los campos correspondientes:
     - **De**: escriba la dirección de correo electrónico del remitente.
     - **Para**: escriba la dirección de correo electrónico del destinatario.
     - **CC**: escriba la dirección de correo electrónico de otros destinatarios para que reciban una copia del mensaje.
     - **Asunto**: si lo desea, escriba un título con el asunto del correo electrónico.
     - **Cuerpo**: escriba el mensaje de correo electrónico.

Nota: Puede utilizar los *marcadores de posición* disponibles en la columna Marcadores de posición como parte del asunto o como el asunto completo. También puede utilizarlos como parte del mensaje del correo electrónico. Los marcadores de posición son variables que, al utilizarlas, se sustituyen por el valor real.

4. Haga clic en **Finalizar**.

Editar o eliminar un destino

1 En la ficha Administrador de eventos, haga clic en **Destinos** para mostrar los destinos activos.

2 Seleccione un destino y, a continuación, realice alguna de las siguientes acciones:

- Para editar el destino, haga clic en .
  - **a** Edite el nombre del destino y, a continuación, haga clic en **Siguiente**.
  - **b** También puede editar el nombre del comando ejecutable en la casilla Ruta de acceso de comandos.
  - **c** Para eliminar una palabra clave de la casilla Parámetros del comando, haga doble clic en la palabra clave y, a continuación, pulse **Eliminar**.
  - **d** Para añadir más palabras clave a la casilla Parámetros del comando, seleccione una palabra clave de la lista Marcadores de posición y, a continuación, haga clic en .
- Para eliminar el destino, haga clic en — y, a continuación, haga clic en **Sí**.

  Advertencia—Posibles daños: Al eliminar un destino, los eventos asociados al mismo también desaparecen.

3 Haga clic en **Finalizar**.

Creación de un evento

1 En la ficha Administrador de eventos, haga clic en **Eventos** para acceder a la sección de eventos.

2 Haga clic en + y, a continuación, escriba un nombre único para el evento y su descripción.

3 En la sección Alertas, seleccione una y, a continuación, haga clic en **Siguiente**.

Nota: puede seleccionar varias o todas las alertas

4 Seleccione un destino y, a continuación, realice alguna de las siguientes acciones:

- Para ejecutar el evento cuando se activa la alarma, seleccione **Sólo en Activar**.
- Para ejecutar e evento cuando la alerta se activa y se elimina, seleccione **Sólo en Activar y Borrar**.

5 Haga clic en **Finalizar**.

Edición o eliminación de un evento

1 En la ficha Administrador de eventos, haga clic en **Eventos** para mostrar los eventos activos.

2 Seleccione un evento y, a continuación, realice alguna de las siguientes acciones:

- Para editar el evento, haga clic en .
  - **a** Edite el nombre del evento y su descripción.
  - **b** En la sección Alertas, añada más alertas seleccionándolas o elimine una alerta desmarcando la casilla de verificación que aparece junto a ella.
  - **c** Haga clic en **Siguiente**.
  - **d** En la sección Destinos, añada más destinos seleccionándolos o elimine un destino desmarcando la casilla de verificación que aparece junto a él.
  - **e** Seleccione un destino de activación y, a continuación, haga clic en **Finalizar**.
- Para eliminar un evento, haga clic en — y, a continuación, en **Sí**.

Asignación de un evento a un dispositivo

1 En la pestaña Administrador de eventos, seleccione la casilla de verificación que hay junto a la dirección IP del dispositivo.

2 Haga clic en **Eventos** para mostrar los eventos activos.

3 Seleccione un evento y haga clic en .

Eliminación de eventos de dispositivos

1 En la ficha Administrador de eventos, active la casilla de verificación situada junto a la dirección IP del dispositivo.

2 Si es necesario, haga clic en **Eventos** para mostrar los eventos activos.

3 Seleccione un evento y, a continuación, haga clic en .

Visualización de detalles de eventos

1 En la ficha Administrador de eventos, busque un dispositivo que utilice marcadores o la búsqueda avanzada.

Nota: puede utilizar las categorías del área de resumen de los resultados de búsqueda para limitar la lista de dispositivos encontrados.

2 En el área Resultados de búsqueda, active la casilla de verificación situada junto a la dirección IP de un dispositivo.

Nota: si no conoce la dirección IP del dispositivo, búsquelo en la columna Nombre del sistema.

3 Haga clic en **Propiedades**.

Aparece un cuadro de diálogo que muestra las condiciones activas actuales y los detalles de los eventos asignados al dispositivo.

Realización de otras tareas administrativas

Descarga de archivos genéricos

La aplicación permite descargar varios archivos del servidor de Markvision en uno o más dispositivos de una red. Esto posibilita la distribución instantánea de varios tipos de archivos, incluidos los *archivos de configuración universal* (UCF), a cualquier dispositivo que administre la aplicación.

1. En el área Cabecera, haga clic en .
2. En el menú desplegable Incluir impresoras, seleccione un grupo de dispositivos o un marcador disponible.
3. Haga clic en **Examinar** y, a continuación, desplácese a la carpeta en la que se ha guardado el archivo.
4. Seleccione el archivo que desea descargar y haga clic en **Abrir**.
5. En el menú desplegable Destino, seleccione una de las siguientes opciones:
   - **Configuración (HTTP)**: descarga un archivo UCF de impresora.
   - **Configuración (FTP)**: descarga un archivo UCF de red.
   - **Actualización de firmware**: descarga una actualización de firmware para los dispositivos.
   - **Impresión (FTP)**: descarga un archivo imprimible a través de una red FTP.
   - **Impresión (socket básico)**: descarga un archivo imprimible del ordenador.
6. Haga clic en **Descargar**.

Notas:

- La tarea Descarga de archivos genéricos no estará disponible cuando la opción Bloqueo de impresora esté activada.
- Se puede programar una tarea de descarga de archivo genérico para que se realice en una hora determinada o de forma regular. Para obtener más información, consulte “Programación de tareas” en la página 56.

Configuración de los valores del correo electrónico

Notas:

- debe configurar los valores del protocolo simple de transferencia de correo (SMTP, Simple Mail Transfer Protocol) para que Markvision pueda enviar notificaciones de correo electrónico para alertas y mensajes de error.
- Si activa ahora la configuración de SMTP, Markvision ya no podrá enviarle notificaciones de correo electrónico para alertas y mensajes de error.

1. En el área Cabecera, haga clic en la ficha > **Correo electrónico**.
2. Seleccione la casilla de verificación **Activar configuración de SMTP** y, a continuación, introduzca los valores en los campos correspondientes.
   - **Servidor de correo SMTP**: escriba la información del servidor de correo.
   - **Puerto**: escriba el número de puerto del servidor de correo SMTP.

- **De**: escriba la dirección de correo electrónico del remitente.

3 Si un usuario debe conectarse antes de enviar el correo electrónico, active la casilla de verificación **Es necesario registrarse**.
   a Introduzca la información de inicio de sesión y la contraseña.
   b Vuelva a escribir la contraseña para confirmarla.

4 Haga clic en **Aplicar** > **Cerrar**.

Configuración de los valores del sistema

1 En el área Cabecera, haga clic en > ficha **General**.

2 En la sección Origen de nombre de host, seleccione el origen del sistema en el que se adquirirá el nombre de host para un dispositivo y, a continuación, haga clic en **Aplicar**.

3 En la sección Administrador de eventos, establezca el intervalo de tiempo que debe esperar el sistema antes de volver a registrar dispositivos para alertas y, a continuación, haga clic en **Aplicar**.

Adición, edición o eliminación de usuarios en el sistema

1 En el área Cabecera, haga clic en > ficha **Usuario**.

2 Realice uno de los procedimientos siguientes:
   - Para agregar un usuario, haga clic en ✚.
     a Introduzca los datos necesarios.
     b En la sección Funciones, seleccione la función del nuevo usuario y, a continuación, haga clic en **Aceptar**.

       A un usuario se le pueden asignar una o varias funciones:
       – **Administrador**: el usuario puede acceder y realizar tareas en todas las fichas. Sólo los usuarios a los que se les ha asignado esta función tienen privilegios administrativos, como la posibilidad de agregar más usuarios al sistema o configurar los valores del mismo.
       – **Activos**: el usuario sólo puede acceder y realizar tareas de la ficha Activos.
       – **Administrador de eventos**: el usuario sólo puede acceder y realizar tareas de la ficha Administrador de eventos.
       – **Políticas**: el usuario sólo puede acceder y realizar tareas de la ficha Políticas.
       – **Asistencia técnica**: el usuario sólo puede acceder y realizar tareas de la ficha Asistencia técnica.
   - Seleccione un usuario existente y, a continuación, haga clic en para editarlo o en — para eliminarlo.

3 Siga las instrucciones que aparecen en la pantalla del ordenador.

Nota: la cuenta de usuario se desactiva después de tres intentos fallidos de conexión consecutivos, y sólo la puede volver a activar el administrador. Sin embargo, si el usuario es el único del sistema que dispone de la función Administrador, la cuenta se suspende temporalmente sólo durante unos cinco minutos.

Activación de la autenticación del servidor LDAP

Lightweight Directory Access Protocol (LDAP) es un protocolo basado en estándares, multiplataforma y extensible que se ejecuta directamente sobre TCP/IP y se utiliza para acceder a bases de datos especializadas que se denominan *directorios*.

Los administradores de Markvision pueden utilizar el servidor LDAP para autenticar ID de usuario y contraseñas. De esta forma se elimina la necesidad de que los usuarios mantengan un ID de conexión y contraseña diferentes sólo para Markvision.

Markvision intenta en primer lugar la autenticación con las credenciales de usuario válidas presentes en el sistema. Si Markvision no puede autenticar el usuario en el primer intento, prueba a realizar la autenticación con usuarios registrados en el servidor LDAP. Sin embargo, si un usuario tiene el mismo nombre de usuario tanto en el servidor de Markvision interno como en el servidor de directorio LDAP, Markvision utilizará los credenciales almacenados en el servidor interno. Esto significa que el usuario necesita utilizar la contraseña de Markvision y *no* la de LDAP.

Como requisito, el servidor LDAP debe contener grupos de usuarios que corresponden a las funciones definidas en “Adición, edición o eliminación de usuarios en el sistema” en la página 49.

Paso 1. Configure los ajustes de autenticación

1. En el área Cabecera, haga clic en la ficha >**LDAP**.
2. En la sección de información de autenticación, introduzca los valores en los campos adecuados.
   - **Servidor**: escriba la dirección IP o el nombre de host del servidor de directorio LDAP donde se realizará la autenticación.

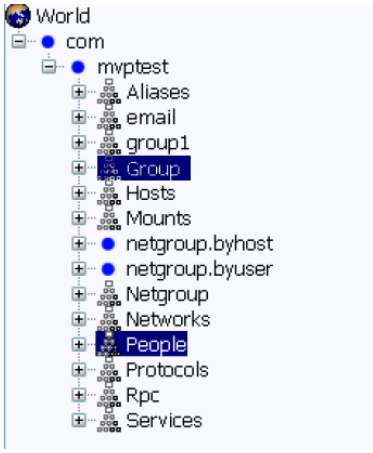
     Si desea utilizar comunicación cifrada entre el servidor MVE y el servidor de directorio LDAP, haga lo siguiente:
     a. Utilice el *nombre de dominio cualificado completo* (FQDN) del host del servidor.
     b. Acceda al archivo de host de red y, a continuación, cree una entrada para asignar el nombre del host del servidor a su dirección IP.

        Notas:

        - En un sistema operativo UNIX/Linux, el archivo de host de red se suele encontrar en **`/etc/hosts`**.
        - En un sistema operativo Windows, el archivo de host de red se suele encontrar en **`%SystemRoot%\system32\drivers\etc`**.
        - El protocolo Transport Layer Security (TLS) requiere que el nombre de host del servidor coincida con el nombre de host "Emitido a" especificado en el certificado de TLS.
   - **Puerto**: Escriba el número de puerto que utilizará el ordenador local para comunicarse con el servidor de comunidad LDAP.

     El núm. de puerto predet. es 389.

- **DN raíz**: escriba el nombre base distinguido del nodo raíz. En la jerarquía del servidor comunitario LDAP, debe ser el ascendente directo del nodo de usuario y del de grupo. En esta ilustración, debe escribir **`dc=mvptest,dc=com`** en el campo DN raíz.

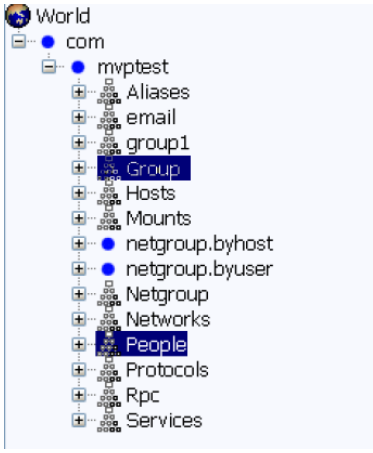


Nota: Cuando se esté especificando el DN raíz, asegúrese de que solo **`dc`** y **`o`** formen parte de la expresión del DN raíz. Si **`ou`** o **`cn`** aparecen como el antecesor común del nodo de usuario y de grupo, utilice **`ou`** o **`cn`** en las expresiones de Base de búsqueda de usuario y Base de búsqueda de grupo.

3 Si desea que Markvision busque *usuarios* anidados en el servidor comunitario LDAP, seleccione **Habilitar búsqueda de usuarios anidados**.

Para afinar más la solicitud de búsqueda, introduzca los valores en los campos adecuados.

- **Base de búsqueda de usuario**: Escriba el nodo en el servidor comunitario LDAP en el que se encuentran el objeto de usuario. Este es también el nodo debajo del DN raíz en el que se enumeran todos los nodos de usuario. En esta ilustración, debe escribir **`ou=people`** en el campo Base de búsqueda de usuario.



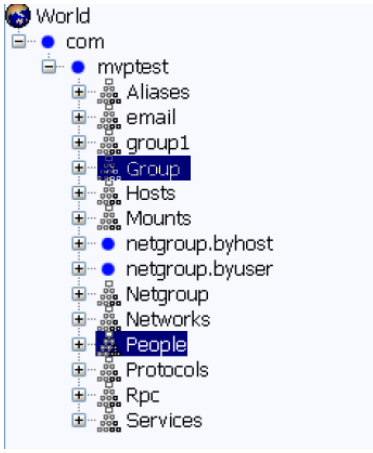
Si los usuarios están en varios niveles de directorio jerarquizados en el servidor comunitario LDAP, haga lo siguiente:

a Calcule cualquier jerarquía ascendente común entre las posibles ubicaciones del nodo de usuario.

b Incluya la configuración en el campo Base de búsqueda de usuario.

Nota: Como alternativa, también puede seleccionar **Habilitar búsqueda de usuarios anidados** y, a continuación, dejar en blanco el campo Base de búsqueda de usuario. Esto indica a Markvision que busque usuarios en todo el árbol LDAP empezando por el DN de base/raíz.

- **Filtro de búsqueda de usuario**: Escriba el parámetro para buscar un objeto de usuario en el servidor comunitario LDAP. En esta ilustración, debe escribir `(uid={0})` en el campo Filtro de búsqueda de usuario.



La función Filtro de búsqueda de usuario puede tener varias condiciones y expresiones complejas, como se muestra en la siguiente tabla.

Si quiere que el usuario inicie sesión con el	Escriba esto en el campo Filtro de búsqueda de usuario
Nombre común	`(CN={0})`
Nombre de inicio de sesión	`(sAMAccountName={0})`
Número de teléfono	`(telephoneNumber={0})`
Nombre de inicio de sesión o nombre común	`(|(sAMAccountName={0})(CN={0}))`

Notas:

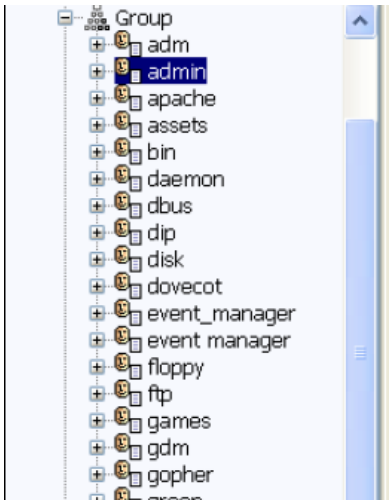
- Estas expresiones se aplican *solo* al servidor LDAP de Windows Active Directory.
- Para el Filtro de búsqueda de usuario, el único patrón válido es `{0}`, lo que significa que MVE buscará el nombre de inicio de sesión del usuario MVE.

4 Si desea que Markvision busque *grupos* anidados en el servidor comunitario LDAP, seleccione **Habilitar búsqueda de grupos anidados**.

Para afinar más la solicitud de búsqueda, introduzca los valores en los campos adecuados.

- **Base de búsqueda de grupo**: escriba el nodo en el servidor de comunidad LDAP en el que están los grupos de usuarios correspondientes a las funciones de Markvision. Este es también el nodo debajo del DN raíz en el que se enumeran todos los nodos de grupo (Función).

En esta ilustración, debe escribir **`ou=group`** en el campo Base de búsqueda de grupo.



Nota: Una Base de búsqueda se compone de múltiples atributos separados por comas, tales como cn (nombre común), ou (unidad organizativa), o (organización), c (país) y dc (dominio).

- **Filtro de búsqueda de grupo**: escriba el parámetro para buscar un usuario dentro de un grupo que corresponda a una función en Markvision.

  Nota: Puede utilizar los patrones **`{0}`** y **`{1}`**, según la configuración esquemática de su servidor comunitario LDAP back-end. Si utiliza **`{0}`**, MVE buscará el DN (nombre distinguido) del usuario LDAP. El DN del usuario se recupera internamente durante el proceso de autenticación del usuario. Si utiliza **`{1}`**, MVE buscará el nombre de inicio de sesión de usuario MVE.

- **Atributo de rol de grupo**: escriba el atributo que contiene el nombre completo del grupo (rol).

  En esta ilustración, debe escribir **`cn`** en el campo Atributo de rol de grupo.

Nota: Al seleccionar **Habilitar búsqueda de usuarios anidados** y **Habilitar búsqueda de grupos anidados** se especifica la profundidad en el servidor comunitario LDAP. De forma predeterminada, la Búsqueda de usuario LDAP y Búsqueda de grupo LDAP se realizan, como máximo, en un nivel por debajo de la Base de búsqueda de usuario y de la Base de búsqueda de grupo, respectivamente. Por lo tanto, la búsqueda anidada (subárbol) se utiliza para indicar que se busquen todas las entradas en los niveles anidados de debajo, incluidas la Base de búsqueda de usuario y la Base de búsqueda de grupo.

Paso 2. Configure los ajustes de vinculación

Esta sección determina el protocolo que debe utilizar el servidor MVE para comunicarse con el servidor de directorio LDAP externo.

1 Haga clic en **Información de vinculación**.

Notas:

- Si no hay ninguna configuración LDAP almacenada en Markvision, se selecciona Vinculación LDAP anónima de forma predeterminada. Esto significa que el servidor MVE no produce su identidad ni credenciales para el

servidor LDAP para utilizar la facilidad de búsqueda del servidor LDAP. La sesión de búsqueda LDAP siguiente será solamente de comunicación sin cifrar.

- El LDAP de Windows Active Directory *no* es compatible con la opción Vinculación anónima.

2 Si desea que el servidor MVE produzca su identidad en el servidor LDAP para poder utilizar la facilidad de búsqueda del servidor LDAP, configure la opción Vinculación simple.

a Seleccione **Vinculación simple**.

b En el campo de DN de vinculación, escriba el nombre distinguido de vinculación.

c Escriba la contraseña de vinculación y, a continuación, confírmela escribiéndola de nuevo.

Notas:

- La contraseña de vinculación depende de los valores de Usuario de vinculación del servidor del directorio LDAP. Si el Usuario de vinculación se ha establecido como **`No vacío`** en el LDAP, se requiere una contraseña de vinculación. Si el Usuario de vinculación se ha establecido como **`Vacío`** en el LDAP, *no* se requiere una contraseña de vinculación. Para obtener más información sobre los valores del Usuario de vinculación en LDAP, contacte con su administrador de LDAP.
- La opción Vinculación simple utiliza comunicación sin cifrar entre MVE y LDAP.

3 Si quiere utilizar comunicación cifrada entre el servidor MVE y el servidor del directorio LDAP, seleccione **TLS** (Transport Layer Security) o **Kerberos V5 (Windows Active Directory)**.

Si ha seleccionado **TLS**, el servidor MVE deberá autenticarse completamente en el servidor de directorio LDAP utilizando la identidad (DN de vinculación) y los credenciales (contraseña de vinculación) del servidor MVE.

a En el campo de DN de vinculación, escriba el nombre distinguido de vinculación.

b Escriba la contraseña de vinculación y, a continuación, confírmela escribiéndola de nuevo.

Nota: Se requiere la contraseña de vinculación.

Para certificados auto-firmados, la huella TLS debe ser disponible para el almacén de claves de todo el sistema *Máquina virtual Java* (JVM) llamado **`cacerts`**. Este almacén de claves se encuentra en la carpeta [mve.home]/jre/lib/security, donde [mve.home] es la carpeta de instalación de Markvision.

Si ha seleccionado **Kerberos V5 (Windows Active Directory)**, realice las acciones siguientes:

a En el campo Nombre de usuario de KDC, escriba el nombre del Centro de distribución de clave (KDC).

b Escriba la contraseña de KDC y, a continuación, confírmela escribiéndola de nuevo.

c Haga clic en **Examinar**, a continuación, desplácese a la carpeta en la que se almacena el archivo *krb5.conf*.

Notas:

- Para obtener más información sobre el archivo de configuración de Kerberos, consulte la documentación suministrada con el protocolo de seguridad Kerberos.
- El protocolo de seguridad de Kerberos *solo* es compatible en Windows Active Directory que admita GSS--API.

d Seleccione el archivo y haga clic en **Abrir**.

Paso 3. Configure los ajustes de asignación de funciones

1 Haga clic en **Asignación de funciones**.

2 Introduzca los valores en los campos apropiados.

- **Admin**: escriba la función existente en LDAP que dispondrá de derechos de administración en MVE.
- **Activos**: Escriba la función existente en LDAP que gestionará el módulo de activos en MVE.

- **Políticas**: Escriba la función existente en LDAP que gestionará el módulo de políticas en MVE.
- **Servicio de mantenimiento**: Escriba la función existente en LDAP que gestionará el módulo de servicio de mantenimiento en MVE.
- **Gestión de eventos**: Escriba la función existente en LDAP que gestionará el módulo de gestión de eventos en MVE.

Notas:

- MVE asignará de forma automática el Grupo LDAP (Función) especificado a su función en MVE.
- Puede asignar un grupo LDAP a varias funciones de MVE y también puede introducir más de un grupo LDAP en un campo de función de MVE.
- Si introduce varios grupos LDAP en los campos de funciones, utilice el carácter de la barra vertical (|) para separar varios grupos LDAP. Por ejemplo, si quiere incluir los grupos **`administrador`** y **`activos`** para la función Administrador, introduzca **`administrador`** | **`activos`** en el campo Administrador.

3 Si decide *no* utilizar algunas de las funciones MVE, puede dejar los campos correspondientes en blanco.

Nota: Esto se aplica a todas las demás funciones, *excepto* a la función de administrador.

4 Para validar la configuración, haga clic en **Probar**.

5 Escriba el nombre de usuario y la contraseña de LDAP y haga clic en **Probar conexión**.

Aparece el cuadro de diálogo Resultados de la configuración de LDAP de prueba. Si hubiera algún error, haga lo siguiente:

a Revise la información del cuadro de diálogo para determinar la causa de los errores.

b Actualice las entradas que hizo en las fichas Información de autenticación, Información vinculante y Asignación de funciones.

c Repita los pasos de paso 4 a paso 5 hasta que no haya más errores en el cuadro de diálogo Resultados de la configuración de LDAP de prueba.

6 Haga clic en **Aplicar** >**Cerrar**.

Generación de informes

1 En el área Cabecera, haga clic en .

2 En el menú desplegable Incluir impresoras, seleccione un grupo de dispositivos basándose en las búsquedas que se han marcado anteriormente.

3 En el menú desplegable Tipo de informe, seleccione el tipo de datos que desea ver.

Seleccione	Para ver
Estado de duración - Resumen	Un informe resumido de los estados de duración de los dispositivos.
Fabricante - Resumen	Un informe resumido de los fabricantes de dispositivos.
Modelo de impresora - Resumen	Un informe resumido de nombres y números de modelos de dispositivos.
Capacidades	Una hoja de cálculo que muestra las capacidades de los dispositivos.
Capacidades - Resumen	Un informe resumido de las capacidades de los dispositivos.
Estado del ciclo de vida	Una hoja de cálculo que muestra los estados de duración de los dispositivos.
Número total de páginas impresas	Una hoja de cálculo que muestra el número de páginas de duración de los dispositivos.

Seleccione	Para ver
Contador de mantenimiento	Una hoja de cálculo que muestra el número de mantenimiento de los dispositivos.
Versiones de firmware	Una hoja de cálculo que muestra las versiones de firmware de los dispositivos.
Soluciones eSF	Una hoja de cálculo que muestra las distintas soluciones Embedded Server Framework (eSF) instaladas en los dispositivos.
Estadísticas:Trabajos por hojas impresas	Una hoja de cálculo que muestra el número de trabajos de impresión realizados por los dispositivos.
Estadísticas:Trabajos por número de papel	Una hoja de cálculo que muestra el número de cargas de papel para los trabajos de impresión, fax y copia realizados por los dispositivos.
Estadísticas:Trabajos por uso de digitalización	Una hoja de cálculo que muestra el número de trabajos de digitalización realizados por los dispositivos.
Estadísticas:Trabajos por uso de fax	Una hoja de cálculo que muestra el número de trabajos de fax realizados por los dispositivos.
Estadísticas:Trabajos por información de suministro	Una hoja de cálculo que muestra detalles importantes de cada elemento de suministro en los dispositivos.

4 En el menú desplegable Formato de informe, seleccione **PDF** o **CSV**.

5 Si selecciona PDF, en el campo Título podrá elegir personalizar el título del informe.

6 Si es necesario, en el menú desplegable Grupo, seleccione un grupo.

7 Haga clic en **Generate (Generar)**.

Programación de tareas

1 En el área Cabecera, haga clic en .

2 En el menú desplegable Agregar, realice una de las siguientes acciones:
- Seleccione **Auditoría** y, a continuación, seleccione un grupo de dispositivos.
- Seleccione **Búsqueda** y, a continuación, seleccione un perfil de búsqueda.
- Seleccione **Cumplimiento** y, a continuación, seleccione un grupo de dispositivos y un tipo de política.
- Seleccione **Aplicación** y, a continuación, seleccione un grupo de dispositivos y un tipo de política.
- Seleccione **Descarga de archivos genéricos** y, a continuación, seleccione un grupo de dispositivos, un archivo y una destinación. Solo los usuarios del rol Administrador pueden utilizar esta opción.

3 Haga clic en **Siguiente**.

4 En el campo Nombre, escriba el nombre del nuevo evento programado.

5 Seleccione los valores y, a continuación, haga clic en **Finalizar**.

Visualización de registros del sistema

1. En el área Cabecera, haga clic en .

   De forma predeterminada, la última actividad de la base de datos aparece en primer lugar.

2. Si desea ver las actividades por categoría, realice las siguientes acciones:
   - **a** Haga clic en **Filtrar**.
   - **b** En la sección Período de tiempo, seleccione las fechas de inicio y finalización.
   - **c** En el campo ID, escriba los números del ID de la tarea.

     Nota: este campo es opcional.
   - **d** En la sección Nombre de la tarea, desactive la casilla de verificación situada junto a la tarea que no desee incluir en el archivo de registro.
   - **e** En la sección Categorías, desactive la casilla de verificación situada junto a la categoría que no desee incluir en el archivo de registro.
   - **f** Haga clic en **Aceptar**.
3. Haga clic en **Preparar para exportar** > **Finalizar exportación**.
4. En el menú desplegable “Guardar en”, desplácese a la carpeta en la que desea guardar el archivo de registro.
5. En el campo “Nombre de archivo”, escriba el nombre del archivo y, a continuación, haga clic en **Guardar**.
6. Desplácese a la carpeta en la que desea que se guarde el archivo de registro y, a continuación, ábralo para ver el registro del sistema.

Preguntas más frecuentes

¿Qué dispositivos admite la aplicación?

Si desea obtener la lista completa de dispositivos admitidos, consulte las notas de la versión.

Cómo cambiar la contraseña

En el área Cabecera, haga clic en **Cambiar contraseña** y, a continuación, siga las instrucciones de la pantalla del ordenador.

¿Por qué no puedo seleccionar dispositivos en la lista Modelos admitidos del cuadro de diálogo Crear nueva política?

Los valores de configuración y los comandos difieren entre los distintos modelos. Un comando de ajuste que funciona en un modelo puede no funcionar en otro. Las políticas se restringen a un único modelo con el fin de evitar la creación de políticas que no funcionen correctamente.

La mejor forma de evitar la creación de una política no efectiva es crear primero una nueva política y asignarla, a continuación, a varios dispositivos.

¿Pueden acceder otros usuarios a mis marcadores?

Sí. Los marcadores son globales y cualquier usuario puede verlos y administrarlos.

¿Dónde se encuentran los archivos de registro?

Navegue hasta este directorio para encontrar los archivos de registro del instalador siguientes: **`%TEMP%\`**

- *mve-*.log*
- **.isf*

Navegue hasta este directorio para encontrar los archivos de registro de aplicación siguientes:

`<INSTALL_DIR>`*`\tomcat\logs`**, donde ***`<INSTALL_DIR>` es la carpeta de instalación de Markvision.

Los archivos de este directorio que tienen el formato **.log* son archivos de registro de aplicación.

Solución de problemas

El usuario ha olvidado la contraseña

Para restablecer la contraseña de usuario, debe tener privilegios de administrador.

1. En el área Cabecera, haga clic en .
2. En la ficha Usuario, seleccione un usuario y, a continuación, haga clic en .
3. Cambie la contraseña.
4. Haga clic en **Aceptar** y, a continuación, haga clic en **Cerrar**.
5. Pida al usuario que se conecte de nuevo.

La aplicación no encuentra ningún dispositivo de red

Compruebe las conexiones de la impresora

- Asegúrese de que el cable de alimentación se encuentra enchufado de forma segura a la impresora y a una toma de alimentación debidamente conectada a tierra.
- Asegúrese de que la impresora está encendida.
- Asegúrese de que el resto de equipo eléctrico conectado a la toma de corriente funcione correctamente.
- Asegúrese de que el cable de LAN está conectado al servidor de impresión y a la LAN.
- y que funciona correctamente.
- Reinicie la impresora y el servidor de impresión.

Asegúrese de que el servidor de impresión interno está correctamente instalado y activado

- Imprima una página de configuración para la impresora. El servidor de impresión debería aparecer en la lista de conexiones de la página de configuración.
- Asegúrese de que TCP/IP está activado en el servidor de impresión. El protocolo debe estar activo para que el servidor de impresión y la aplicación funcionen. Asegúrese de que el protocolo esté activo en el panel de control de la impresora.
- Consulte la documentación del servidor de impresión.

Asegúrese de que el nombre del dispositivo en la aplicación es el mismo que el establecido en el servidor de impresión

1. Compruebe el nombre de dispositivo establecido en la aplicación.

   En el área Resultados de búsqueda, busque la dirección IP de la impresora.

   El nombre del dispositivo aparece junto a su dirección IP. Éste es el nombre de dispositivo de la aplicación y *no* el nombre de dispositivo del servidor de impresión.

2. Compruebe el nombre de dispositivo establecido en el servidor de impresión. Para obtener más información, consulte la documentación del servidor de impresión.

Asegúrese de que el servidor de impresión se comunica en la red

1. Aplique PING al servidor de impresión.
2. Si el comando ping funciona, verifique la dirección IP, la máscara de red y el gateway del servidor de impresión para asegurarse de que sean correctos.
3. Apague la impresora y, a continuación, vuelva a aplicar el comando ping para comprobar si hay direcciones IP duplicadas.

   Si el comando ping no funciona, imprima una página de configuración y compruebe si la IP está activada.

4. Si TCP/IP está activado, compruebe la dirección IP, la máscara de red y el gateway para asegurarse de que son correctos.
5. Asegúrese de que los puentes y los encaminadores funcionan y están configurados correctamente.
6. Asegúrese de que todas las conexiones físicas entre el servidor de impresión, la impresora y la red funcionan.

La información del dispositivo es incorrecta

Si la aplicación muestra información del dispositivo que parece incorrecta, realice una auditoría en el dispositivo.

Glosario de términos de seguridad

Autenticación	Método por el cual un sistema identifica de forma segura a un usuario.
Autorización	Método para especificar qué funciones están disponibles para un usuario, por ejemplo, lo que se le permite hacer al usuario.
Bloques	Herramientas de Autenticación y Autorización utilizadas en el Embedded Web Server. Se incluye: contraseña, PIN, cuentas internacionales, LDAP, LDAP +GSSAPI, Kerberos 5 y NTLM.
Controles de acceso	Están disponibles las configuraciones que controlan tanto los menús, las funciones y los valores de cada dispositivo y a quién. En algunos dispositivos también son denominados como Funciones de los controles de acceso.
Grupo	Un conjunto de usuarios que comparten características comunes.
Plantilla de seguridad	Un perfil creado y guardado en el Embedded Web Server, utilizado en conjunto con Controles de acceso para controlar las funciones de los dispositivos.

Índice alfabético

A
activación de autenticación de servidor LDAP 50
Activos, ficha
  utilizar 12
actualización a la última versión de Markvision 9
administrador de eventos, ficha
  utilizar 12
admitidos, lista de modelos 58
agregación de un usuario 49
aplicación de políticas 41, 43
aplicación, archivos de registro
  ubicar 58
archivos
  descargar 48
asignación de palabras clave a un dispositivo 28
asignación de políticas 41
asignación de un evento a un dispositivo 47
Asistencia técnica, ficha
  utilizar 12
auditoría de un dispositivo 21
avisos 2

B
bases de datos, servidores
  compatible 8
búsqueda avanzada, uso 24
búsqueda de dispositivos 18, 24
búsqueda, perfil
  crear 18
  editar 19
  eliminar 19

C
Cabecera, área 14
cambio de contraseñas 58
categorías
  agregar 28
  editar 28
  eliminar 28
  utilizar 27
compatibles, dispositivos 58
compatibles, servidores de bases de datos 8
comprobación de cumplimiento con políticas 41
comprobación del cumplimiento de los dispositivos con las políticas 43
comprobación del estado del dispositivo 43
configuración de los valores del sistema 49
contraseña, usuario
  restablecer 59
copia de seguridad de la base de datos Firebird 9
creación de marcadores 27
creación de nuevas políticas 30
creación de perfiles de búsqueda 18
creación de políticas desde dispositivos 31
creación de un evento 46

D
descarga de archivos genéricos 48
descripción de la pantalla de inicio 14
descripción de protocolos 15
descripción de puertos 15
descripción general 7
destino
  crear 45
  editar 46
  eliminar 46
dispositivo
  asignar palabras clave 28
  asignar un evento 47
  auditar 21
  comprobar estado 43
  eliminar eventos 47
  eliminar palabras clave asignadas 29
  importar desde un archivo 20
  ver de forma remota 44
  visualizar detalles de eventos 47
  visualizar propiedades 22
dispositivo, alertas
  recibir 49
dispositivo, estado
  comprobar 43
dispositivo, nombre de host
  adquirir 49
dispositivo. estado de duración
  Administrado 21
  Administrado (encontrado) 21
  Administrado (falta) 21
  Administrado (modificado) 21
  Administrado (normal) 21
  configurar 21
  No administrado 21
  Retirado 21
dispositivos
  buscar 18, 24

E
edición de destinos 46
edición de políticas 40
edición de un evento 46
edición de un perfil de búsqueda 19
edición de usuarios 49
eliminación de eventos de dispositivos 47
eliminación de marcadores 27
eliminación de palabras clave asignadas de dispositivos 29
eliminación de políticas 40, 42
eliminación de un destino 46
eliminación de un evento 46
eliminación de un perfil de búsqueda 19
eliminación de usuarios 49
equipo, RAM 8
evento
  crear 46
  editar 46
  eliminar 46
  eliminar de dispositivos 47
  visualizar detalles 47

F
Firebird, base de datos
  hacer una copia de seguridad 9
  restaurar 10

G
generación de informes 55

General, ficha
  utilizar 49

I

importación de dispositivos desde un archivo 20
impresora, estado 43
incorporada, página web
  visualizar 44
incorrecta, información del dispositivo 60
Información de la tarea, área 14
informes
  generar 55
inicio, pantalla
  describir 14
instalador, archivos de registro
  ubicar 58

L

LDAP, servidor
  activar autenticación 50

M

marcadores
  acceder 27
  crear 27
  eliminar 27
marcadores de posición 45
marcadores predeterminados, uso 24
Marcadores y búsqueda avanzada, área 14
Markvision
  acceder 10
  instalar 8
  utilizar 12
Markvision Enterprise
  actualizar a la última versión 9
  definición 7
MarkVision Professional
  migrar a Markvision Enterprise 11
migración de MarkVision Professional a Markvision Enterprise 11
MVE
  migrar a 11
MVP
  importar a Markvision Enterprise 11
  migrar a Markvision Enterprise 11

N

no se puede detectar un dispositivo en red 59

O

olvidada, contraseña de usuario 59

P

palabras clave
  agregar 28
  asignar a un dispositivo 28
  editar 28
  eliminar 28
  eliminar de dispositivos 29
  utilizar 27
política
  aplicar 41
  asignar 41
  comprobar cumplimiento 41
  crear 30
  crear desde un dispositivo 31
  editar 40
  eliminar 40
  extraer 42
  tipos 30
políticas
  aplicar 43
  comprobar cumplimiento de los dispositivos 43
  gestionar 30
Políticas, ficha
  utilizar 12
procesador, velocidad 8
programación de tareas 56
propiedades de dispositivos
  visualizar 22
protocolos
  describir 15
puertos
  describir 15
puesta en marcha
  pantalla de inicio 14

R

recepción de alertas de dispositivos 49
registro, archivos
  ubicar 58
restablecimiento de contraseña de usuario 59
restauración de la base de datos Firebird 10
Resultados de búsqueda, área 14
Resumen de los resultados de búsqueda, área 14

S

sistema, nombres
  comprobar 59
sistema, registro
  visualizar 57
sistema, requisitos
  espacio disponible en el disco duro del equipo 8
  RAM 8
  resolución de pantalla 8
  velocidad del procesador 8
sistema, valores
  configurar 49
solución de problemas
  información del dispositivo incorrecta 60
  no se puede detectar un dispositivo en red 59
  restablecer contraseña de usuario 59
Suministro, estado 43

T

tareas
  programar 56

U

uso de categorías 27
uso de palabras clave 27
usuario
  agregar 49
  editar 49
  eliminar 49

V

visualización de detalles de eventos 47
visualización de dispositivos de forma remota 44
visualización de la página web incorporada 44
visualización de propiedades de dispositivos 22
visualización de registros del sistema 57