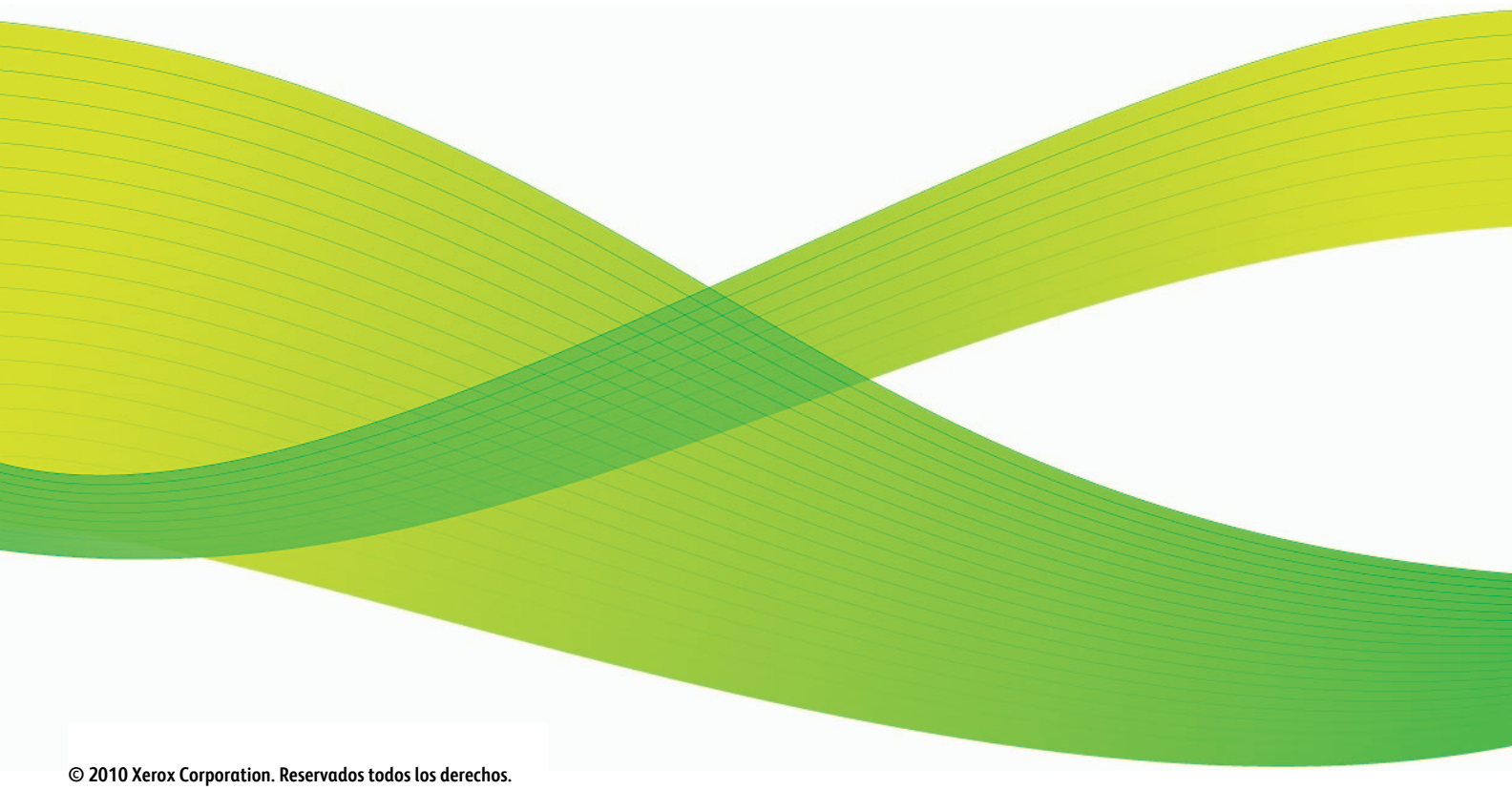
Versión 1.6, octubre de 2010

Xerox Secure Access Unified ID System®

Guía de instalación



Traducción a cargo de:

Xerox
CTC European Operations
Bessemer Road
Welwyn Garden City
Hertfordshire
AL7 1BU
Reino Unido

Contenido

Notas de seguridad

1

Lea detenidamente estas notas de seguridad para cerciorarse de utilizar el equipo de un modo seguro y de acuerdo con la legislación aplicable.

El equipo ha sido diseñado y probado con el fin de cumplir estrictos requisitos de seguridad. Entre estos requisitos, se incluyen la aprobación del equipo por parte de agencias de seguridad y el cumplimiento de los estándares medioambientales establecidos.

Lea atentamente las instrucciones siguientes antes de utilizar el equipo y consúltelas cuando sea necesario con el fin de garantizar un uso continuado y seguro del mismo.

AVISO: cualquier modificación no autorizado, como la incorporación de funciones nuevas o la conexión de dispositivos externos, podría afectar a la certificación del producto. Para obtener más información, póngase en contacto con un distribuidor local autorizado.

Suministro eléctrico

La fuente de alimentación suministrada con el equipo debe utilizarse con el tipo de suministro eléctrico indicado en la placa de características del equipo. Si no está seguro de si el suministro eléctrico satisface los requisitos, consulte a su compañía eléctrica.

AVISO: información sobre seguridad eléctrica

- Utilice únicamente la fuente de alimentación suministrada con el equipo.
- No coloque el equipo en lugares donde la gente pueda pisar el cable o la fuente de alimentación, o bien tropezar con ellos.
- No coloque objetos sobre el cable de la fuente de alimentación.
- Si se produce alguna de las siguientes situaciones, apague el equipo inmediatamente, desconecte el cable de alimentación de la toma eléctrica y llame a un servicio técnico autorizado para resolver el problema:
  - El equipo desprende olores extraños.
  - El cable de alimentación está dañado o deshilachado.
  - Ha saltado un interruptor, un fusible o algún otro mecanismo de seguridad.
  - El equipo está expuesto al agua.
  - Algún componente del equipo está dañado.

Dispositivo de desconexión

El cable de alimentación de la fuente de alimentación es el dispositivo de desconexión del equipo. Para interrumpir el suministro eléctrico del equipo, desconecte el cable de alimentación de la toma eléctrica.

Información sobre la normativa

Emisiones de radiofrecuencia

Estados Unidos y Canadá

Nota: este equipo ha sido probado y cumple con los límites establecidos para los dispositivos digitales de Clase B, conforme a la sección 15 de las normas de la FCC. Estos límites se han establecido para proporcionar una protección razonable frente a interferencias perjudiciales cuando el equipo se utiliza en un entorno residencial. Este equipo genera, utiliza y puede emitir energía radioeléctrica, y si no se instala y utiliza de acuerdo con las instrucciones, puede producir interferencias perjudiciales en las radiocomunicaciones. Sin embargo, no se puede garantizar que no se vayan a producir interferencias en una instalación determinada. Si el equipo produce interferencias perjudiciales en la recepción de radio o televisión, lo que puede determinarse apagando y encendiendo el equipo, el usuario puede corregir las interferencias tomando una o más de las medidas siguientes:

- Cambiar la orientación o la ubicación de la antena receptora
- Separar más el equipo y el receptor
- Conectar el equipo a una toma eléctrica de un circuito distinto al utilizado por el receptor
- Consultar al distribuidor o a un técnico en radio y televisión

Con el fin de garantizar el cumplimiento de las normas de la FCC en los Estados Unidos, es necesario utilizar cables blindados con el equipo.

Canadá

Este aparato de clase "B" cumple con la norma ICES-003 de Canadá.

Cet appareil Numérique de la classe "B" est conforme à la norme NMB-003 du Canada.

Europa

La marca CE que aparece en este producto representa la declaración de conformidad por parte de Xerox con las siguientes directivas de la Unión Europea a partir de las fechas indicadas:

12 de diciembre de 2006:	Directiva del Consejo 2006/95/CE (conforme a sus modificaciones). Aproximación de las legislaciones de los Estados miembros relativas a los equipos de baja tensión.
15 de diciembre de 2004:	Directiva del consejo 2004/108/CE (conforme a sus modificaciones). Aproximación de las legislaciones de los Estados miembros relativas a la compatibilidad electromagnética.
9 de marzo de 1999:	Directiva del Consejo 99/5/CE sobre equipos radioeléctricos y equipos terminales de telecomunicación y reconocimiento mutuo de su conformidad.

Para obtener una declaración de conformidad completa, con la definición de las directivas pertinentes y las normas a las que se hace referencia, póngase en contacto con el distribuidor autorizado de Xerox más cercano.

AVISOS:

- Para que este equipo funcione cerca de equipos médicos, científicos o industriales, puede que sea preciso limitar la radiación externa de estos últimos o tomar medidas especiales para mitigarla.
- Con el fin de garantizar el cumplimiento de la Directiva del Consejo 89/336/CEE, es necesario utilizar cables blindados con este producto.

"Información sobre la normativa referente a la identificación de los dispositivos de radiofrecuencia"

Los lectores que se proporcionan junto con este producto generan 13.56 MHz al utilizar un sistema de bucle inductivo como dispositivo de identificación de radiofrecuencia. Dicho dispositivo cumple con los requisitos especificados por la Directiva del Consejo Europeo 99/5/CE, así como con todas las leyes y normas aplicables de cada país.

El uso de este dispositivo está sujeto a las siguientes condiciones: (1) no debe causar ninguna interferencia perjudicial y (2) debe admitir cualquier interferencia recibida, incluidas las que provoquen un funcionamiento no deseado.

Los cambios o modificaciones que se realicen al equipo sin la autorización específica de Xerox Corporation pueden anular el derecho de uso del equipo por parte del usuario.

Reciclaje y eliminación del producto

Si usted se ocupa de la eliminación del equipo, tenga en cuenta que el producto contiene plomo, mercurio y otros materiales cuya eliminación puede estar regulada en algunos países o estados debido a cuestiones medioambientales. La presencia de plomo y mercurio cumple con las normas internacionales aplicables en el momento de la comercialización del producto.

Unión Europea

Información sobre la eliminación del producto para usuarios comerciales

Si el equipo tiene este símbolo, quiere decir que se debe eliminar de acuerdo con los procedimientos nacionales acordados.

De acuerdo con la legislación europea, la eliminación de equipos eléctricos y electrónicos que hayan llegado al final de su vida útil está sujeta a los procedimientos acordados.

Antes de eliminar el equipo, póngase en contacto con su distribuidor local o representante de Xerox para obtener información relativa a la retirada de equipos que han llegado al final de su vida útil.

Norteamérica (Estados Unidos y Canadá)

Xerox tiene un programa internacional de retirada y reciclaje o reutilización de equipos viejos. Llame al servicio de atención al cliente de Xerox (1-800-ASK-XEROX) para saber si este producto Xerox forma parte del programa. Para más información sobre los programas medioambientales de Xerox, visite http://www.xerox.com/environment

Si usted se encarga de la eliminación del producto Xerox, tenga en cuenta que el producto puede contener plomo, mercurio, perclorato y otros materiales cuya eliminación puede estar regulada en algunos países o estados debido a consideraciones medioambientales. La presencia de estos materiales cumple con las normas internacionales aplicables en el momento de la comercialización del producto. Para obtener información acerca del reciclaje y la eliminación del producto, póngase en contacto con los responsables locales. En los Estados Unidos, también puede consultar la página web de Electronic Industries Alliance: http://www.eiae.org

Perclorato: este producto puede incluir uno o varios dispositivos que contengan perclorato, como, por ejemplo, las baterías. Es posible que se deban seguir instrucciones específicas de uso. Consulte http://www.dtsc.ca.gov/hazardouswaste/perchlorate

Información sobre la eliminación del producto para usuarios particulares

Si el equipo exhibe este símbolo, quiere decir que no se debe eliminar junto con otros residuos domésticos.

De acuerdo con la legislación europea, los equipos eléctricos y electrónicos que hayan llegado al final de su vida útil deberán eliminarse por separado y no junto a otros residuos domésticos.

Los usuarios particulares de los Estados Miembros de la Unión Europea pueden entregar los equipos eléctricos y electrónicos usados en los puntos de recogida designados de forma gratuita. Para obtener información, póngase en contacto con los responsables locales.

En algunos Estados Miembros, al adquirir un equipo nuevo, es posible que el distribuidor local tenga la obligación de retirar el equipo antiguo de forma gratuita. Solicite información a su distribuidor.

Otros países

Póngase en contacto con los responsables locales para solicitar información acerca de la eliminación del equipo.

Información de contacto sobre cuestiones medioambientales, de salud y de seguridad

Información de contacto

Para obtener más información acerca de cuestiones medioambientales, de salud y de seguridad en relación con este producto Xerox y sus suministros, póngase en contacto con las siguientes líneas de atención al cliente:

Estados Unidos: 1-800 828-6571

Canadá: 1-800 828-6571

Europa: +44 1707 353 434

www.xerox.com/environment información de seguridad EE. UU. (información de seguridad del producto para EE. UU.)

www.xerox.environment_europe información de seguridad UE (información de seguridad del producto para la UE)

Pasos de instalación 2

Las guías de instalación y administración de Xerox Secure Access contienen instrucciones detalladas sobre la instalación y configuración del servidor Secure Access y las impresoras multifunción. Este capítulo ofrece una tabla que indica el orden de instalación de acuerdo con el tipo de configuración del hardware de Secure Access, empezando por la Guía de instalación.

Pasos (*) indica que el paso es obligatorio	Xerox Secure Access con un lector de tarjetas USB	Xerox Secure Access con un dispositivo de autenticación y lector de tarjetas
Guía de instalación		
1. Lea el capítulo 3: Descripción general de la instalación	*	*
2. Capítulo 4: Instalación del servidor Secure Access; Preparación de la red y la base de datos	*	*
3. Capítulo 4: Instalación del servidor Secure Access; Ejecución del asistente para la instalación	*	*
4. Capítulo 5: Configuración del hardware; Paso 1: Configuración de la dirección IP del dispositivo de autenticación	Omitir	*
5. Capítulo 5: Configuración del hardware; Paso 2: Montaje del dispositivo de autenticación de Secure Access	Omitir	*
6. Capítulo 5: Configuración del hardware; Paso 3: Conexión del hardware	Omitir	*
7. Capítulo 5: Configuración del hardware; Paso 4: Montaje y conexión del lector de tarjetas USB de Secure Access	*	Omitir
Guía de administración		
8. Lea el capítulo 3: Descripción general de Secure Access	*	*
9. Capítulo 4: Flujo de trabajo de configuración; Paso1: Configurar el dispositivo multifunción de Xerox para aceptar la autenticación de red a través del mecanismo Xerox Secure Access	*	*
10. Capítulo 4: Adición de dispositivos multifunción a la base de datos de Secure Access	*	*
11. Capítulo 4: Asociación del dispositivo multifunción a un dispositivo de autenticación de Secure Access	Omitir	*
12. Capítulo 4: Configuración de la impresión Follow-You (opcional)	*	*
13. Capítulo 4: Establecimiento de los parámetros de autenticación	*	*
14. Capítulo 4: Importación y sincronización de cuentas de usuario	*	*
15. Capítulo 4: Configuración del servicio personalizado Release My Documents (liberar documentos)	*	*

3 Descripción general de la instalación

Contenido del capítulo:

Esta guía incluye instrucciones que le ayudarán a instalar el software del servidor Xerox Secure Access Unified ID System™ y a realizar la instalación física de los dispositivos de autenticación. Antes de configurar los dispositivos de autenticación, es necesario instalar el servidor.

Una vez que haya instalado correctamente el software del servidor Secure Access, consulte la Guía de administración de Secure Access para obtener instrucciones detalladas acerca de la instalación física del dispositivo y la configuración del software.

Este capítulo proporciona la información siguiente:

- Componentes que forman parte del servidor Secure Access
- Requisitos del sistema

Componentes de Secure Access

Xerox Secure Access Unified ID System™ (de aquí en adelante "Secure Access") es una solución de hardware y software que consta de los siguientes componentes:

- El software del servidor Secure Access, que gestiona la base de datos de usuarios y proporciona servicios que se comunican con los dispositivos (impresoras) multifunción y los dispositivos de autenticación de Secure Access.
- Un dispositivo de autenticación de Secure Access, que incluye un lector de tarjetas y controla el acceso a los dispositivos multifunción de Xerox.

  O bien
- Un lector de tarjetas USB de Secure Access

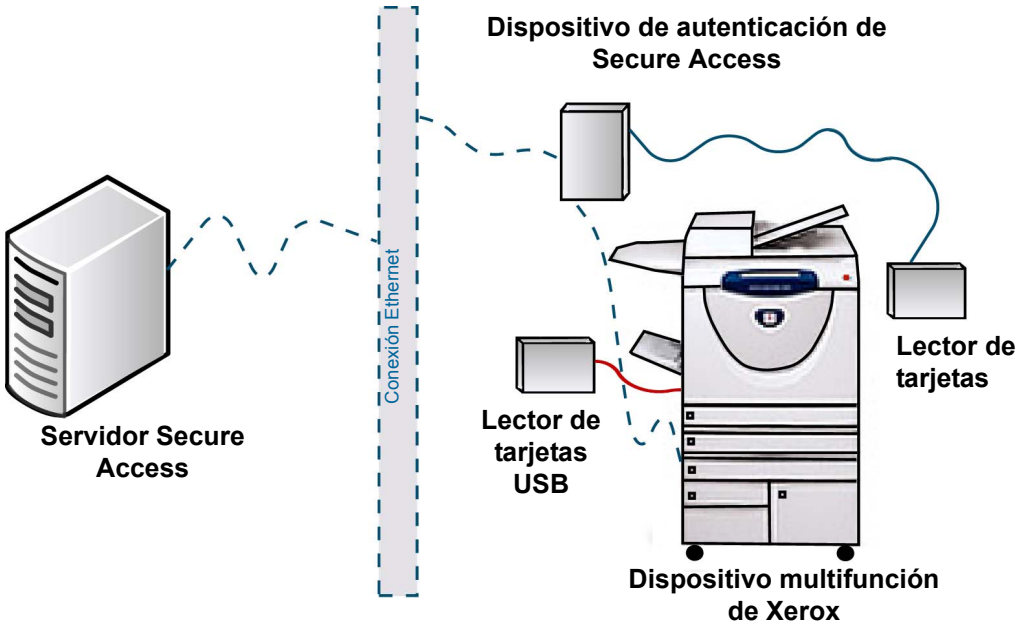


Figura 3-1: Componentes de Secure Access

Cada instalación del software del servidor Secure Access requiere al menos tres servicios:

- Core Authentication Server (CAS)
- Motor de control de dispositivos (DCE)
- Motor de enrutamiento de documentos (DRE)

Además, también es necesario instalar Secure Access Manager, una herramienta administrativa utilizada para establecer comunicación entre los distintos componentes de Secure Access.

Core Authentication Server (CAS)

El servidor CAS (servidor de autenticación principal) alberga la base de datos que contiene todos los datos de usuarios y dispositivos multifunción.

Para realizar una instalación de Secure Access, es necesario haber instalado previamente una base de datos. El servidor CAS utiliza la instancia de base de datos para crear una base de datos de cuentas que contiene toda la información de usuarios y dispositivos. Consulte Requisitos del sistema para el servidor Secure Access en la página 18 para obtener información sobre las bases de datos compatibles.

Motor de control de dispositivos (DCE)

El motor de control de dispositivos gestiona todas las comunicaciones con los dispositivos multifunción. Si un usuario desea utilizar la funcionalidad de copia, escaneado o fax en un dispositivo multifunción, primero debe activar el lector de tarjetas. La lectura de una tarjeta de banda magnética o de proximidad inicia una petición de acceso.

El dispositivo de autenticación reenvía la petición de inicio de sesión al DCE, que se comunica con el CAS para verificar los datos de cuenta de usuario asociados a la tarjeta.

Motor de enrutamiento de documentos (DRE)

El motor DRE es el servidor de impresión. Su función principal es la de permitir el flujo de documentos de las estaciones de trabajo a los dispositivos multifunción. A continuación, se describe un flujo de trabajo DRE típico:

1. Un usuario genera una petición de impresión a un dispositivo multifunción que está registrado en la base de datos de Secure Access Manager.
2. Si el usuario imprime en una cola de impresión que utiliza un puerto de Secure Access Manager, el DRE almacenará el trabajo en el servidor de impresión.
3. Cuando el usuario inicia una sesión en el dispositivo multifunción, el DRE busca los trabajos en la cola de dicho dispositivo (o grupo de extracción) y libera los que fueron enviados por el usuario que ha iniciado sesión.

Si el dispositivo no tiene instalado un puerto de Secure Access, el trabajo se imprimirá sin validación.

Si desea que los trabajos de impresión sean retenidos en una cola segura, se puede configurar la impresión Follow-You. Para activar esta funcionalidad, debe configurar el dispositivo multifunción para que utilice un puerto de Secure Access, en lugar de uno convencional. El supervisor de puertos se integra con las funciones y con el subsistema de impresión de Windows como parte del servicio de administración de trabajos de impresión. Esto permite que el supervisor pueda recibir trabajos de impresión y, a continuación, retenerlos en una cola virtual segura hasta que un usuario verificado los libere en un dispositivo multifunción determinado.

Asimismo, puede incorporar el servicio personalizado Release My Documents al dispositivo multifunción. Este servicio permite a los usuarios acceder a la cola de impresión segura directamente desde el panel frontal del dispositivo multifunción. Consulte la Guía de administración de Xerox Secure Access para obtener las instrucciones de configuración.

Instalación en varios servidores

La instalación mediante la que todos los servicios se instalan en el mismo servidor se denomina instalación 'local'. No obstante, algunas instalaciones pueden necesitar más de un servidor para distribuir la carga de gestión. Las instalaciones en las que los servicios se distribuyen entre dos o más servidores se denominan instalaciones "remotas".

Tanto si se realiza la instalación en un solo servidor como si se realiza en varios, los servicios DRE y DCE siempre deberán instalarse en el mismo servidor.

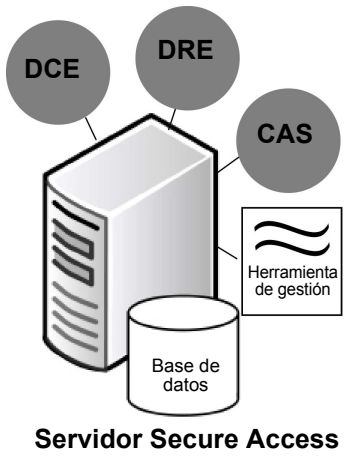


Figura 3-2: Instalación local

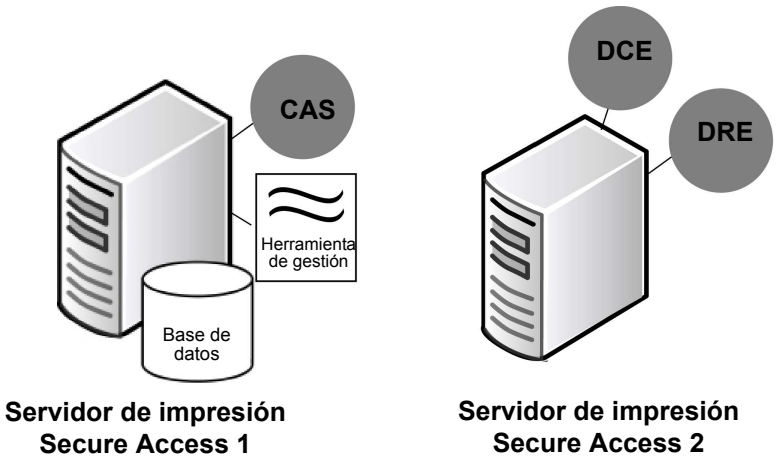


Figura 3-3: Instalación remota

Además, si Secure Access va a gestionar muchos dispositivos multifunción, es posible instalar varios servidores de impresión DRE para equilibrar la carga de comunicaciones.

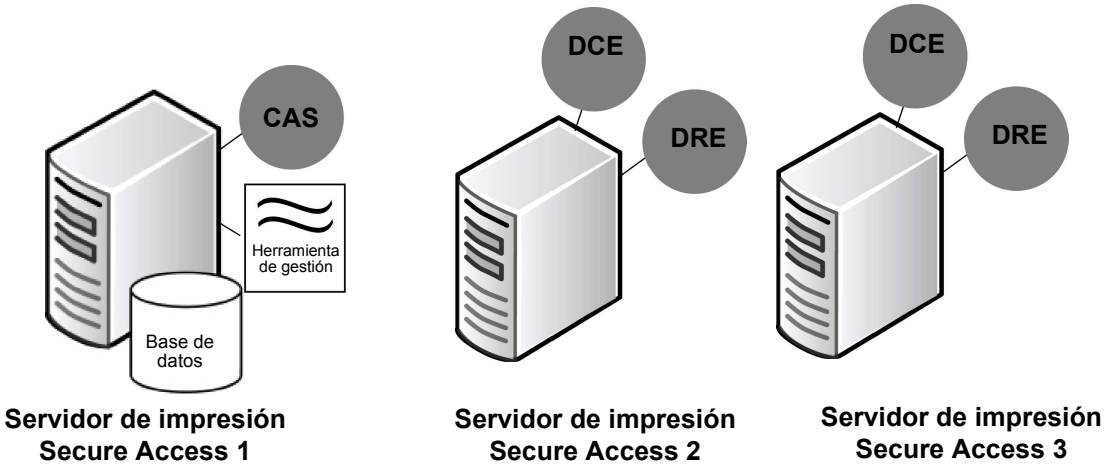


Figura 3-4: Instalación en varios servidores de impresión

Consulte Ejecución del asistente para la instalación en la página 23 para obtener detalles acerca de la instalación y configuración en varios servidores. El asistente para la instalación permite seleccionar únicamente los componentes que desea instalar en cada servidor. Los servicios DRE y DCE se pueden instalar para una configuración de varios servidores, pero siempre deberán ir instalados en el mismo servidor.

Requisitos del sistema para el servidor Secure Access

Antes de instalar Secure Access asegúrese de que los servidores que tiene previsto utilizar cumplan los requisitos de funcionamiento mínimos que se describen a continuación.

En la tabla siguiente, se enumeran únicamente los requisitos de funcionamiento mínimos. Para maximizar el rendimiento en entornos donde se gestionan grandes volúmenes de impresión, necesitará más espacio en disco y más memoria, además de un procesador más rápido.

Componente	Requisitos mínimos
Hardware	• Procesador: Pentium III, Athlon o superior • Memoria del sistema: 512 MB como mínimo • Espacio en disco para aplicaciones: 100 MB • Espacio en disco para la base de datos: 20 MB • Resolución de pantalla: 1024 x 768
Sistema operativo de CAS/DCE/DRE	Uno de los siguientes: • Windows Server 2003 (32 bits) • Windows XP Professional (solo 32 bits)[1] • Windows Server 2008 (32 y 64 bits), 2008 R2 (64 bits) Nota: antes de instalar el software del servidor Secure Access, es necesario haber instalado todas las actualizaciones esenciales del sistema operativo.
Bases de datos	• Microsoft SQL Server 2005 Express[2] • Microsoft SQL Server 2008 Express (64 bits) Nota: Nota: Secure Access no puede instalarse en un servidor que ejecute una aplicación MSDB (como FreeFlow™ SMARTsend™) puesto que estas bases de datos entran en conflicto con la base de datos SQL Server.

[1] Si piensa instalar el servicio CAS en un servidor Windows XP Professional que no esté asociado a un dominio, siga las instrucciones de la página 15 para configurar los parámetros de autenticación de usuarios.

[2] SQL Server 2005 Express requiere Windows Service Pack 2 (SP2) o una versión superior para ejecutarse en Windows Server 2008 o 2008 R2.

Parámetros de autenticación de usuarios en Windows XP Pro

Si piensa instalar el servicio CAS de Secure Access en la plataforma Microsoft Windows XP Professional, y la máquina no está asociada a un dominio, debe cambiar las opciones de seguridad de XP para que los inicios de sesión se adapten a las cuentas de usuario con nombre.

En Windows XP Pro, los inicios de sesión en red que utilizan las cuentas locales se asignan automáticamente a la cuenta de invitado de forma prefijada. Si desea que los usuarios se autentiquen como ellos mismos, debe cambiar este parámetro.

Realice estos pasos antes de ejecutar el asistente de instalación de Secure Access.

1. Abra la ventana Configuración de seguridad local en la máquina donde va a instalar el servicio CAS.
2. En el panel de exploración de la izquierda, haga doble clic en **Directivas locales** y luego en **Opciones de seguridad**.
3. En el panel de la derecha, desplácese hacia abajo hasta la entrada **Acceso de red: modelo de seguridad y para compartir para cuentas locales**.
4. Haga doble clic en esta entrada y elija **Clásico: usuarios locales autenticados como ellos mismos**.
5. Haga clic en **Aplicar** y luego en **Aceptar** para cerrar la ventana.
6. Cierre la ventana Configuración de seguridad local.

Requisitos de los componentes de hardware de Secure Access

Asegúrese de que dispone de todo el hardware que se le ha proporcionado:

Configuración 1:

- Fuente de alimentación
- Cable de alimentación
- Llave especial (llave metálica utilizada para restaurar los valores prefijados del dispositivo). Consulte Restablecimiento de un dispositivo de autenticación en los apéndices de la Guía de administración.
- Cable de red Ethernet 10/100 Base-T
- Lector de tarjetas

O bien

Configuración 2:

- Lector de tarjetas USB de Secure Access

Lectores de tarjetas compatibles

Secure Access es compatible con los siguientes lectores de tarjetas:

- ABA Magstripe
- Mifare (incluidos los lectores HID iCLASS)
- Legic
- HID 125 kHz
- Indala
- EM Marin
- Hitag

4 Instalación del servidor Secure Access

Contenido del capítulo:

Esta sección incluye instrucciones acerca del uso del asistente que permite instalar el servidor Secure Access. Siga atentamente las instrucciones y asegúrese de que los servidores cumplen los requisitos de funcionamiento mínimos descritos en Requisitos del sistema para el servidor Secure Access en la página 18.

Este capítulo proporciona información acerca de:

- Preparación de la red y de la base de datos antes de la instalación
- Utilización del asistente para la instalación con el fin de seleccionar componentes de instalación para cada servidor Secure Access

Preparación de la red y de la base de datos

Aunque el procedimiento de instalación de Secure Access es muy sencillo, es necesario realizar las tareas que se incluyen a continuación antes de ejecutar el asistente:

1. Planifique las funciones del sistema.
2. Active Xerox Secure Access en el dispositivo multifunción mediante Servicios de Internet de CentreWare.

   Notas:

   - Abra el navegador web y conéctese a Servicios de Internet de CentreWare. Acceda a la página donde se activa Xerox Secure Access. Esta configuración requiere la activación de SSL y la creación de un certificado. Para más información, consulte el CD de administración del sistema de la impresora.
   - Para los lectores de tarjetas USB, puede que el dispositivo multifunción requiera una actualización del software. Póngase en contacto con un distribuidor local de Xerox o visite la página web de asistencia del dispositivo multifunción concreto en la sección "Asistencia y controladores" de www.xerox.com
3. Determine el destino de la instalación para cada uno de los componentes de Secure Access.

   Nota: antes de instalar Secure Access en la red, asegúrese de que tiene privilegios de administrador para todas las máquinas donde haya que instalarlo y configurarlo.
4. Verifique que la configuración de la red está preparada para gestionar la comunicación entre los componentes de Secure Access.
5. Utilice las actualizaciones de Windows para instalar todas las actualizaciones críticas que requiera el sistema operativo.
6. Instale Microsoft .NET Framework 2.0.

   Nota: consulte en el sitio web de Microsoft la lista completa de requisitos previos para la instalación de SQL Server 2005 ó 2008 Express Edition.
7. Instale y configure la base de datos.

   Nota: si utiliza SQL Server 2005 ó 2008 Express, tiene que configurar la base de datos para utilizar el modo de autenticación de Windows. Secure Access no admite la autenticación en modo mixto.

Ejecución del asistente para la instalación

Durante la instalación de Secure Access, el asistente permite seleccionar las características que desea instalar en cada servidor. Si va a distribuir los componentes entre varios servidores, tiene que ejecutar el asistente en cada máquina y seleccionar únicamente los componentes necesarios. Si la instalación se va a realizar en un solo servidor, sólo tendrá que ejecutar el asistente una vez.

Cada instalación requiere al menos un componente CAS, DCE, DRE y Secure Access Manager.

1. Antes de realizar la instalación, asegúrese de que se han completado los pasos de la sección "Preparación de la red y de la base de datos".
2. Cierre todas las demás aplicaciones del servidor antes de realizar la instalación de Secure Access.
3. Ejecute el asistente para la instalación de Secure Access.
   - Si realiza la instalación desde el CD de Secure Access, seleccione el archivo **32-bit Setup.exe** para iniciar la instalación para una máquina de 32 bits, o bien seleccione **64-bit Setup.exe** para iniciar la instalación para una máquina de 64 bits.

   O bien

   - Si realiza la instalación a través de una distribución electrónica, descargue el archivo ZIP y ejecute el archivo **Setup.exe** de 32 ó 64 bits.

   Nota: si al ejecutar el archivo setup.exe recibe un mensaje de error, puede que tenga que actualizar la versión de Microsoft Installer. Visite el sitio web de Microsoft y descargue e instale la versión más reciente de Microsoft Installer para el sistema operativo.
4. En la pantalla de bienvenida, haga clic en **Siguiente** para iniciar el proceso de instalación.
5. Examine el contrato de licencia del software y haga clic en **Acepto**; seguidamente, haga clic en **Siguiente**.
6. Seleccione las opciones que desea instalar en la máquina y haga clic en **Siguiente**.

   De forma prefijada, se seleccionan todos los componentes. Seleccione solamente los componentes que necesite para este servidor concreto. Por ejemplo, si esta máquina es el servidor de impresión, instale únicamente los componentes DRE y DCE. Ejecute el instalador en otro servidor para instalar el resto de componentes, según las necesidades.

   Nota: lea las descripciones de los componentes que se ofrecen en Componentes de Secure Access en la página 14 antes de instalar cualquier componente. Esta información le ayudará a determinar la forma de instalar los componentes que mejor se adapten a las necesidades de su empresa.
7. Seleccione el idioma de la interfaz en la pantalla **Seleccionar el idioma**. Este es el idioma que se utilizará en Secure Access Manager únicamente. El idioma que se utilizará en todos los mensajes del panel frontal de los dispositivos multifunción vendrá determinado por la configuración del dispositivo.
8. En la pantalla **Instance for SQL Express** (Instancia para SQL Express), escriba el nombre de la instancia que creó para la base de datos SQL Express. Haga clic en **Next** (Siguiente).

   Nota: el nombre de la instancia que introduzca en este campo debe coincidir con el nombre que creó para la base de datos de Secure Access al instalar SQL Express. La instalación no puede continuar sin el nombre de instancia correcto. Si ha realizado una instalación estándar de SQL Express y no ha cambiado los parámetros prefijados, deje este valor como SQLEXPRESS y, a continuación, haga clic en Siguiente.

9. Especifique valores para **UserID** (ID de usuario) y **Password** (Clave) para los servicios de la pantalla **User Name for Services** (Nombre de usuario para servicios).

   Si los componentes se instalan en más de una máquina, debe introducir las mismas credenciales de usuario en cada instalación. Estas credenciales se utlizan para iniciar y ejecutar todos los servicios. Si no introduce las mismas credenciales para todos los componentes, el servidor CAS no responderá a las solicitudes del componente DCE o DRE.

   Las cuentas de dominio deben utilizar el nombre de dominio (por ejemplo, dominio\nombre_de_usuario).

   Aunque esta cuenta no requiere privilegios administrativos en el servidor Secure Access, sí debe tener privilegios de operador de impresión para permitir que el DRE procese las solicitudes de impresión.

10. Escriba el nombre del servidor de autenticación Xerox Secure Access.

    Cuando inicie Secure Access Manager, tendrá que identificar el servidor CAS con el nombre que haya especificado aquí.

11. Haga clic en **Install** (Instalar) para iniciar el proceso de instalación. El asistente para la instalación copia los archivos, configura los servicios y crea los accesos directos a Secure Access Manager.

12. Cuando finalice el proceso, haga clic en **Finish** (Finalizar) para salir del asistente para la instalación.

13. La instalación del servidor Secure Access ha finalizado. Para configurar el hardware de Secure Access, consulte el capítulo 5.

Actualización de Secure Access

Si realiza una actualización por etapas o actualiza todos los componentes durante un periodo de inactividad programado, las instrucciones que se facilitan más abajo lo guiarán a través del asistente para la instalación con el fin de que pueda actualizar Secure Access.

Nota: se recomienda hacer una copia de seguridad de la base de datos antes de realizar la actualización.

Durante la instalación de Secure Access, el asistente detecta los componentes de Secure Access que ya están instalados en la máquina (por ejemplo, la base de datos). Estos componentes se seleccionarán automáticamente en el asistente. Puede conservar las opciones prefijadas o seleccionar más componentes para instalar.

Para actualizar Secure Access, realice los pasos siguientes:

1. Cierre todas las demás aplicaciones del servidor antes de realizar la instalación de Secure Access.
2. Ejecute el asistente para la instalación de Secure Access.
   - Si realiza la instalación desde el CD de Secure Access, seleccione el archivo **32-bit Setup.exe** para iniciar la instalación para una máquina de 32 bits, o bien seleccione **64-bit Setup.exe** para iniciar la instalación para una máquina de 64 bits.

   O bien

   - Si realiza la instalación a través de una distribución electrónica, descargue el archivo ZIP y ejecute el archivo **Setup.exe** de 32 ó 64 bits.

   Nota: si al ejecutar el archivo setup.exe recibe un mensaje de error, puede que tenga que actualizar la versión de Microsoft Installer. Visite el sitio web de Microsoft y descargue e instale la versión más reciente de Microsoft Installer para el sistema operativo.
3. En la pantalla de bienvenida, haga clic en **Siguiente** para iniciar el proceso de instalación.
4. Examine el contrato de licencia del software y haga clic en **Acepto**; seguidamente, haga clic en **Siguiente**.
5. Seleccione las opciones que desea instalar en la máquina y haga clic en **Siguiente**.

   De forma prefijada, se seleccionan todos los componentes. Seleccione solamente los componentes que necesite para este servidor concreto. Por ejemplo, si esta máquina es el servidor de impresión, instale únicamente los componentes DRE y DCE. Ejecute el instalador en otro servidor para instalar el resto de componentes, según las necesidades.
6. Escriba el nombre del servidor de autenticación Xerox Secure Access.
7. Haga clic en **Finish** (Finalizar) para salir del asistente.

La actualización del servidor Secure Access ha finalizado. Para configurar el hardware de Secure Access, consulte el capítulo 5.

5 Configuración del hardware de Secure Access

Contenido del capítulo:

En este capítulo, se incluyen instrucciones para realizar la configuración física del hardware de Secure Access. Antes de empezar, debe tener instalado el software del servidor Secure Access. Siga las instrucciones que se proporcionan en el capítulo 4 para realizar la instalación del servidor Secure Access.

Si utiliza un lector de tarjetas USB para Secure Access, vaya directamente al paso 4.

1. Configure la dirección IP para cada dispositivo de autenticación.
2. Instale el hardware del dispositivo de autenticación de Secure Access en el dispositivo multifunción o cerca de él.
3. Realice las conexiones eléctricas, serie, de expansión y del lector de tarjetas.

Configuración de la dirección IP del dispositivo de autenticación

PRECAUCIÓN: Si no utiliza un servidor DHCP para asignar direcciones IP, NO CONECTE EL DISPOSITIVO DE AUTENTICACIÓN A LA RED hasta que haya configurado la dirección IP de forma manual. Consulte Asignación manual de la dirección IP en la página 29.

De forma prefijada, los dispositivos de autenticación de Secure Access están configurados para la comunicación DHCP. Es necesario asignar una dirección IP a cada dispositivo de autenticación y configurar la dirección IP del servidor del componente DCE. Existen dos métodos para asignar la dirección IP:

- Mediante un servidor DHCP. Siga las instrucciones descritas en Configuración del servidor DHCP para la detección de dispositivos de autenticación en la página 28.
- Si no utiliza un servidor DHCP o prefiere no configurar la opción 230 en el servidor DHCP, tendrá que utilizar la aplicación Authentication Device Web Admin para configurar las direcciones de forma manual. Siga las instrucciones descritas en Asignación manual de la dirección IP en la página 29.

Configuración del servidor DHCP para la detección de dispositivos de autenticación

Las instrucciones que se proporcionan más abajo son específicas para servidores DHCP de Windows. Si utiliza un servidor que funcione en una plataforma distinta (por ejemplo: UNIX, Linux, OS X, OpenVMS o AS/400), configúrelo para que transfiera la dirección del servidor DCE con el valor 230.

Nota: Para obtener más información técnica acerca de cómo utilizar DHCP para asignar direcciones IP a los dispositivos de autenticación de Secure Access, consulte el documento titulado "Setting the Secure Access Authentication Device IP Address White Paper", que está disponible en www.xerox.com.

1. En Herramientas administrativas de Windows, abra la consola de gestión de DHCP de Windows.
2. Seleccione el nodo raíz del servidor DHCP.
3. En el menú **Acción**, seleccione **Configurar opciones predeterminadas**.
4. En la lista desplegable **Clase de opción**, seleccione **Opciones estándar de DHCP**.
5. En la sección **Nombre de opción**, haga clic en **Agregar**.
   a. En el campo **Nombre**, escriba: Xerox Secure Access.

   Nota: La utilidad de la etiqueta del campo **Nombre** tiene únicamente fines de identificación.

   b. En la lista desplegable **Tipo de datos**, seleccione Cadena.
   c. En el campo **Código**, escriba 230.
   d. En el campo **Descripción**, escriba: Secure Access.
6. Haga clic en **Aceptar**.

7. En la sección **Valor de cadena**, escriba EQ;A;<dirección IP servidor DCE> en el campo **Cadena**, donde <dirección IP servidor DCE> es la dirección IP del servidor DCE.
8. Expanda el nodo **Ámbito** y seleccione **Opciones de ámbito**.
9. En el menú **Acción**, seleccione **Configurar opciones**.
10. Seleccione **230**.
11. Haga clic en **OK** para guardar los cambios.

Asignación manual de la dirección IP

Siga estas instrucciones solamente si no utiliza un servidor DHCP para configurar la dirección IP del dispositivo de autenticación, o bien si utiliza un servidor DHCP, pero prefiere utilizar una dirección IP estática en lugar de utilizar la opción 230.

La primera vez que se enciende, el dispositivo de autenticación busca un servidor DHCP para obtener una dirección IP. Si no detecta ningún servidor DHCP, el dispositivo cambia al modo de comunicación estática y adopta la dirección IP estática prefijada: 192.168.2.1. Es posible utilizar un cable Ethernet para conectar un sistema (por ejemplo, un PC portátil) a cada dispositivo de autenticación y, posteriormente, utilizar una herramienta de administración web para cambiar la dirección IP e introducir la dirección IP del servidor DCE.

Antes de empezar, imprima la hoja separable de configuración de la página 35. Utilice esta hoja para anotar las direcciones IP asignadas a todos los dispositivos de autenticación.

Configuración del PC portátil

El sistema en que se ejecuta la herramienta de administración web debe reconocer la dirección IP estática para poder acceder a la herramienta.

1. En el sistema (PC portátil) que ejecutará la herramienta de administración web, seleccione **Conexiones de red** > **Conexión de área local** > **Propiedades**.
2. Haga doble clic en **Propiedades de Internet** (TCP/IP) y, a continuación, haga clic en **Avanzadas**.
3. En la sección Direcciones IP, haga clic en **Agregar**.
4. Escriba lo siguiente:
   Dirección IP: 192.168.2.x (la "x" representa una dirección IP que no está asignada)
   Máscara de subred: 255.255.255.0
5. Haga clic en **Agregar** para guardar los cambios.

Utilización de la herramienta de administración web para configurar direcciones IP

Siga el procedimiento siguiente para cada dispositivo de autenticación.

1. Utilice un cable Ethernet normal para conectar un PC portátil al puerto Downlink del dispositivo de autenticación de Secure Access.
2. Para encender el dispositivo de autenticación, conecte un extremo del cable de alimentación al dispositivo de autenticación y el otro extremo a una toma que esté libre.

3. Abra el navegador web y escriba 192.168.2.1 en el campo de dirección.
   Esta es la dirección IP prefijada que está asignada al dispositivo de autenticación de Secure Access.

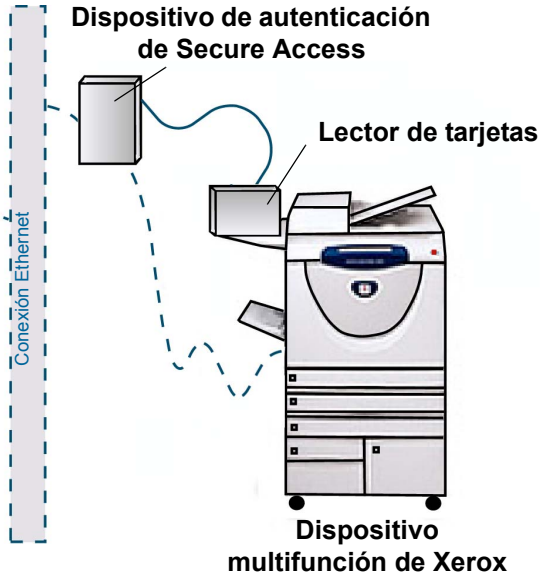
   Nota: En el caso del idioma francés, seleccione el enlace suministrado.
4. Haga clic en el enlace **Configure** (Configurar) situado en la parte superior de la página.
5. Escriba lo siguiente para conectarse:
   Nombre de usuario: deviceadmin
   Clave: pc_passwd
6. Cambie la clave utilizada para acceder a la herramienta de administración web. Puede cambiar la clave en cualquier momento, pero asegúrese de cambiar el valor prefijado antes de que el sistema de Secure Access esté en funcionamiento.
7. En la sección **Configure Xerox Secure Access Authentication Device** (Configurar el dispositivo de autenticación de Xerox Secure Access), elija Static IP (IP estática) en el campo **Addressing mode** (Modo de direccionamiento).
8. Introduzca una dirección IP estática en el campo **IP Address** (Dirección IP) para configurar la dirección de este dispositivo de autenticación.
9. En la sección **Configure Server** (Configurar servidor), escriba la dirección IP del servidor DCE en el campo correspondiente.
10. Haga clic en el botón **Update Configuration** (Actualizar configuración), situado debajo de los campos Configure Server.
11. Haga clic en el enlace **Restart** (Reiniciar) de la parte superior de la página y luego en "Click here to confirm restart" (Haga clic aquí para confirmar el reinicio) para reiniciar el terminal.

Repita las instrucciones para todos los dispositivos de autenticación de Secure Access que vaya a distribuir.

Nota: Recuerde volver a configurar las propiedades de Internet del PC portátil cuando acabe.

Montaje del dispositivo de autenticación de Secure Access

Imprima la Hoja separable de configuración en la página 35. A medida que realice el montaje, rellene las columnas de esta hoja. Necesitará esta información cuando configure la comunicación entre los dispositivos en el servidor Secure Access.



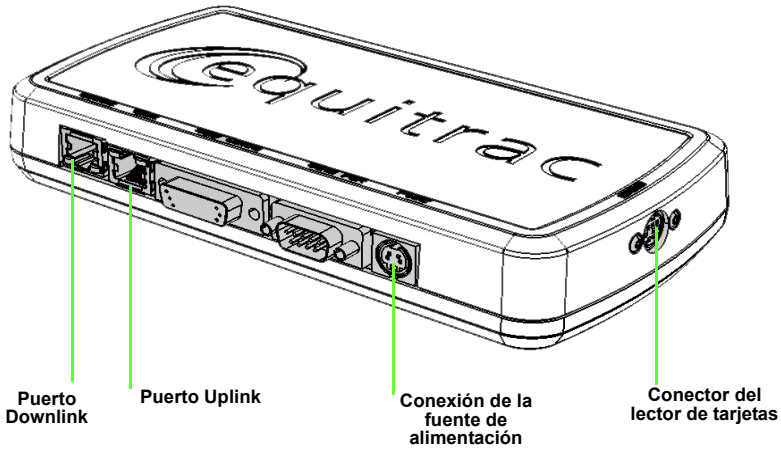
1. Coloque el dispositivo de autenticación en el suelo, detrás del dispositivo multifunción y en el lado de entrada del mismo. **Coloque el dispositivo en un lugar de fácil acceso y asegúrese de que el cable sea lo suficientemente largo para conectarlo al lector de tarjetas**.
2. Coloque el lector de tarjetas en el estante situado en el lado izquierdo del panel frontal del dispositivo multifunción mediante la tira de velcro suministrada. Si tiene instalada la grapadora auxiliar, coloque el lector de tarjetas a la derecha de la grapadora de modo que éste quede entre la grapadora y el dispositivo multifunción. **Antes de adherir la tira de velcro, asegúrese de que la cubierta superior del alimentador de documentos puede abrirse sin que el lector de tarjetas lo impida**.
3. Utilice la hoja de configuración para registrar las direcciones IP y MAC del dispositivo de autenticación, así como la dirección IP y el nombre de host del dispositivo multifunción que controlará dicho dispositivo.

   Nota: Consulte el CD de administración del sistema del dispositivo multifunción para conocer otras sugerencias de montaje.

Conexión del hardware

Asegúrese de realizar las tareas de configuración descritas en Configuración de la dirección IP del dispositivo de autenticación en la página 28 antes de conectar el hardware del dispositivo de autenticación de Secure Access.

Consulte el gráfico que se incluye a continuación para conectar los componentes. Observe que el dispositivo de autenticación dispone de un puerto serie y un puerto de control de copias que no se utiliza en esta configuración.



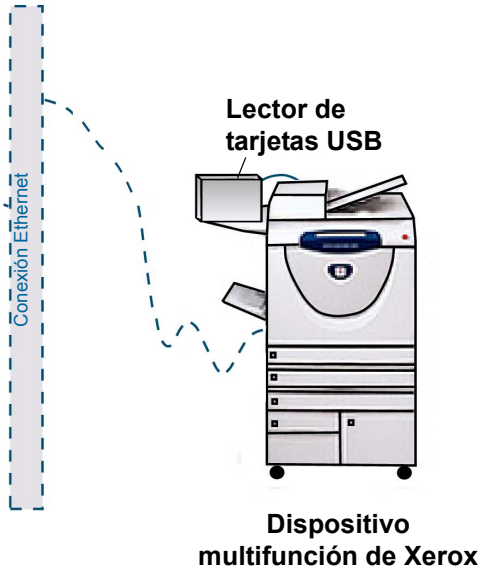
1. Utilice la hoja de configuración para anotar la dirección MAC del dispositivo de autenticación. Escriba esta dirección en la misma fila que el dispositivo multifunción que controlará.
2. Enchufe el cable serie del lector de tarjetas en el conector del lector de tarjetas del dispositivo de autenticación.

3. Conecte un extremo del cable Ethernet al conector de red y el otro extremo al puerto Uplink del dispositivo de autenticación de Secure Access.
4. Conecte el cable Ethernet de los dispositivos multifunción al puerto Downlink del dispositivo de autenticación.

   Nota: Cuando el dispositivo de autenticación está apagado, no hay conexión Ethernet disponible en el puerto Downlink. Como alternativa, puede conectar el cable Ethernet del dispositivo multifunción directamente a otro puerto Ethernet. El dispositivo de autenticación incorpora el puerto Downlink por si no hay otro puerto Ethernet disponible.
5. Conecte la fuente de alimentación al dispositivo de autenticación y, a continuación, enchufe el otro extremo del cable a una toma eléctrica próxima.

La configuración del hardware ha finalizado. Siga las instrucciones de la Guía de administración de Secure Access para configurar el servidor Secure Access y permitir la comunicación entre los dispositivos de autenticación y los dispositivos multifunción.

Montaje/conexión del lector de tarjetas USB de Secure Access



1. Coloque el lector de tarjetas en el estante situado en el lado izquierdo del panel frontal del dispositivo multifunción mediante la tira de velcro suministrada. Si tiene instalada la grapadora auxiliar, coloque el lector de tarjetas a la derecha de la grapadora de modo que éste quede entre la grapadora y el dispositivo multifunción. **Antes de adherir la tira de velcro, asegúrese de que la cubierta superior del alimentador de documentos puede abrirse sin que el lector de tarjetas lo impida**.
2. Conecte el cable del lector en algún puerto USB que esté disponible en la parte trasera del dispositivo multifunción.

   Consulte el CD de administración del sistema del dispositivo multifunción para conocer otras sugerencias de montaje.

Hoja separable de configuración

Arranque esta hoja y utilícela cuando realice la configuración física de los dispositivos de autenticación. Debe mantener registradas las direcciones IP y MAC de cada dispositivo de autenticación, así como el dispositivo multifunción que controlará.

	Dispositivo de autenticación		Dispositivo multifunción	
	Dirección MAC	Dirección IP	Dirección IP	Nombre del host
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				