Version 1.6, October 2010

Xerox Secure Access Unified ID System®

Guía de administración

© 2010 Xerox Corporation. Reservados todos los derechos.

Copyright© 2007-2010 de Xerox Corporation. Reservados todos los derechos. XEROX©, Secure Access Unified ID System, SMARTsend y FreeFlow son marcas comerciales o con licencia de Xerox Corporation en los Estados Unidos y otros países.

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 autorizada, 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

CE	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

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

http://www.xerox.com/environment_europe información de seguridad EU (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; Sección 1: Preparación de la red y la base de datos	*	*
3. Capítulo 4: Instalación del servidor Secure Access; Sección 2: 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; Paso 1: Configuración del 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	*

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
12. Capítulo 4: Configuración de la impresión Follow-You (opcional)	*	*
13. Capítulo 4: Configuración de 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 Secure Access

Contenido del capítulo:

Una vez que haya instalado el servidor Xerox Secure Access Unified ID System® y haya realizado la instalación física de los dispositivos de autenticación o del lector de tarjetas USB de Secure Access, utilice esta guía para añadir dispositivos multifunción a la base de datos de Secure Access, lo que permitirá la comunicación entre el servidor y los dispositivos de autenticación. Utilice esta guía para llevar a cabo tareas de configuración avanzadas de todos los componentes y funciones de Secure Access.

Este capítulo proporciona la información siguiente:

- Componentes de hardware y software que forman parte de Xerox Secure Access
- Acceso a Secure Access Manager para administrar el sistema

¿Qué es Secure Access?

Secure Access Unified ID System® permite controlar el acceso a las funciones de impresión, fax, copia y escaneado de los dispositivos multifunción de Xerox. Cuando un usuario se disponga a utilizar un dispositivo controlado por Secure Access, deberá pasar la tarjeta por la ranura correspondiente o por el lector de tarjetas de proximidad. El panel frontal del dispositivo multifunción únicamente se activa cuando el servidor Secure Access ha autenticado la información de cuenta del usuario.

Mediante un protocolo propietario (Convenience Authentication Protocol), el dispositivo de autenticación de Secure Access se comunica con el servidor Secure Access a través de una conexión de red Ethernet para verificar la información de usuario obtenida de una tarjeta de banda magnética o una tarjeta de proximidad. Si se utiliza un lector de tarjetas USB, el dispositivo multifunción se comunicará directamente con el servidor Secure Access. Si el servidor Secure Access verifica al usuario, el panel del dispositivo multifunción se desbloqueará para que pueda utilizarse. Si no se verifica al usuario, el dispositivo multifunción permanecerá bloqueado y el usuario no podrá llevar a cabo ninguna tarea en el dispositivo.

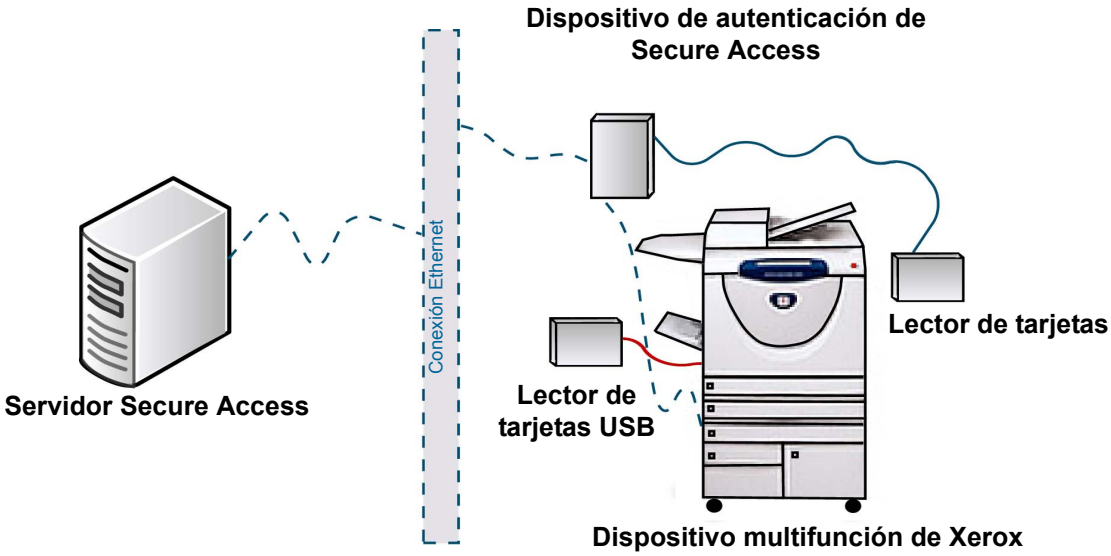


Figura 3-1: Componentes de la solución Secure Access

Si el usuario desea escanear documentos, el servidor Secure Access proporciona el ID de usuario de red para el dispositivo multifunción compatible. A continuación, el dispositivo puede utilizar el ID para implementar la funcionalidad de inicio de sesión único y realizar automáticamente la autenticación para el escaneado.

Componentes de Secure Access

La solución requiere dos componentes principales:

1. El **dispositivo de autenticación de Secure Access**, que consta de un terminal de autenticación y un lector de tarjetas externo. Los usuarios no acceden al terminal de autenticación.

   El lector de tarjetas se conecta al dispositivo de autenticación únicamente a través de un cable serie y no se conecta directamente al dispositivo multifunción. Consulte la *Guía de instalación* para obtener instrucciones de montaje e instalación.

Figura 3-2: Componentes del dispositivo de autenticación de Secure Access

O bien

1. El **lector de tarjetas USB del servidor Secure Access**, que está conectado al dispositivo multifunción. Consulte la Guía de instalación para obtener instrucciones de montaje e instalación.
2. El **servidor Secure Access**, que consta de los componentes siguientes:
   - Core Authentication Server (CAS)
   - Motor de control de dispositivos (DCE)
   - Motor de enrutamiento de documentos (DRE)
   - Secure Access Manager (Herramientas administrativas)

   Nota: puede instalar estos componentes en un mismo servidor o distribuirlos en varios servidores. En algunas instalaciones, es posible que también necesite más de un DCE o DRE. Consulte la *Guía de instalación* para obtener información detallada.

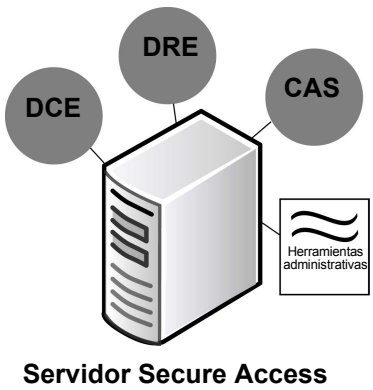


Figura 3-3: Componentes del servidor Secure Access

Los componentes del servidor principal se comunican a través de los puertos designados. Cada componente "escucha" a través de un puerto específico la información o las peticiones de otros componentes. Consulte la sección Asignaciones de puerto en la página 47 para obtener una lista completa de las asignaciones de puerto por componente.

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 contenga toda la información de usuarios y dispositivos. Consulte los requisitos del sistema en la *Guía de instalación* para obtener información acerca de 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. Este proceso se describe en las figuras 3-4 y 3-5.

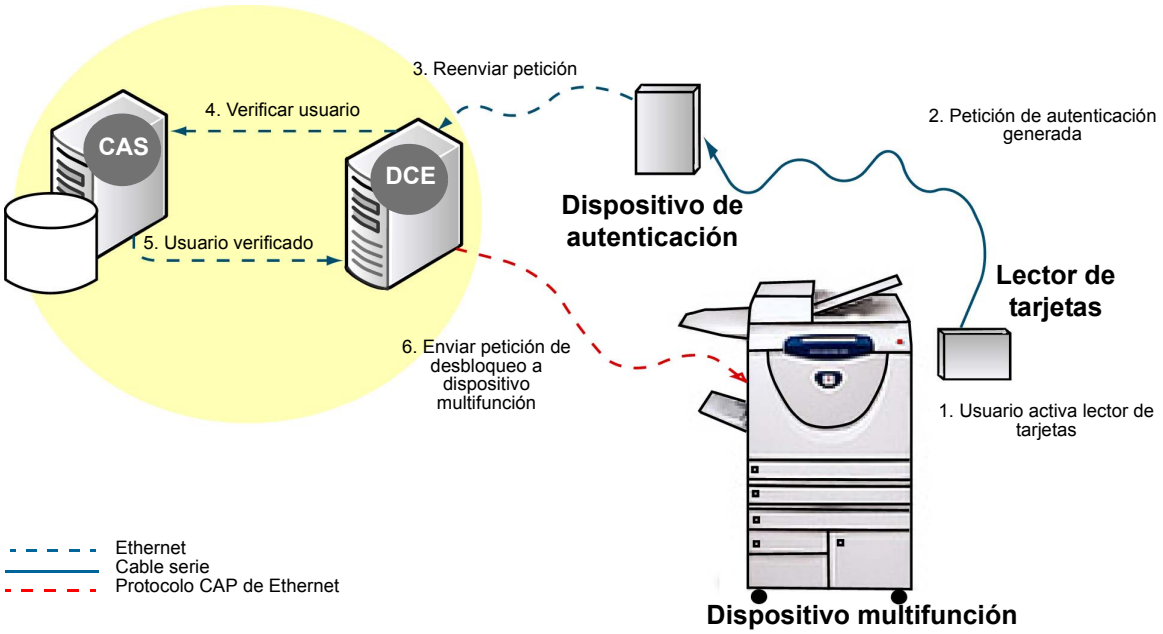


Figura 3-4: Flujo de trabajo de autenticación de usuarios

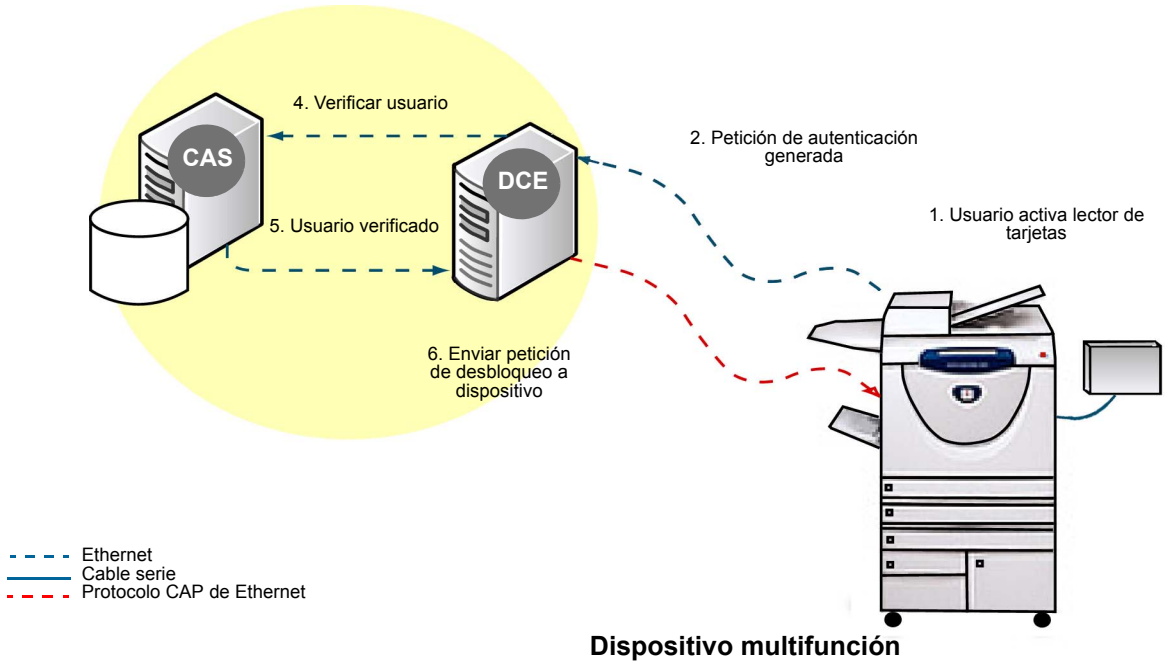


Figura 3-5: Flujo de trabajo de la autenticación de usuario con el lector de tarjetas USB

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.

   Nota: si el servicio personalizado Release My Documents está instalado, los usuarios pueden acceder a la pantalla correspondiente para ver la cola de impresión segura y liberar los documentos que sea necesario. Consulte Configuración del servicio personalizado Release My Documents en la página 41.

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

Si desea que los trabajos de impresión se retengan en una cola segura, puede configurar la impresión Follow-You. Si desea activar esta funcionalidad, debe configurar el dispositivo multifunción para utilizar un puerto de Secure Access, en lugar de un puerto convencional. El supervisor de puertos se integra con las funciones y 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.

Cuando se activa la impresión Follow-You, el usuario debe autenticarse primero en el dispositivo multifunción que desee, como muestra la Figure 3-4: Flujo de trabajo de autenticación de usuarios en la página 16. Si la autenticación se realiza correctamente, y el servicio personalizado Release My Documents está instalado, el usuario puede acceder al panel frontal del dispositivo multifunción para ver la cola de impresión. El usuario puede liberar uno o todos los trabajos (según la configuración).

Realización de cambios en los componentes del servidor

Si en Secure Access Manager se realizan cambios de configuración de cualquiera de los componentes principales del servidor Secure Access (CAS, DRE, DCE), por ejemplo, añadir dispositivos nuevos, se debe esperar al menos 30 segundos para que los cambios surtan efecto.

La demora a la hora de actualizar los componentes del servidor es una función de la característica de sondeo de CAS. Esto significa que la demora podría ser mayor en el caso de que CAS no esté disponible por algún motivo durante el período de sondeo posterior a la modificación del servidor. CAS enviará los datos modificados a los componentes relevantes una vez que se haya restablecido la conexión.

Compatibilidad con el lector de datos y flujo de trabajo de usuarios

Las funciones del dispositivo multifunción permanecen bloqueadas hasta que un usuario proporciona información de autenticación válida. Para ello, el usuario debe pasar su tarjeta inteligente o de proximidad por el lector de tarjetas de proximidad o por un lector de banda magnética.

Una vez que el servidor CAS haya validado los datos del usuario, el dispositivo multifunción se desbloqueará y estará listo para su utilización. Cuando el usuario haya terminado, debe pulsar los botones **Borrar todo** o **Acceso** del teclado del dispositivo multifunción para desconectarse y bloquear el dispositivo.

Secure Access admite varios tipos de lectores externos: de banda magnética, EM Marin, de proximidad HID, Hitag, Indala, Legic y Mifare. Todos los lectores vienen configurados de fábrica y no es necesario realizar ajustes adicionales.

Lector de banda magnética

Secure Access es compatible con lectores de banda magnética externos. Los usuarios pueden introducir datos de validación pasando la tarjeta magnética codificada por el lector de tarjetas. El lector de banda magnética lee virtualmente cualquier tipo de tarjeta magnética convencional en la ranura 2 y acepta datos codificados de tipo estándar o personalizados. Los datos de la ranura 1 están disponibles con los lectores de tarjeta USB de banda magnética.

Utilización de un lector de dispositivos de banda magnética

Pida a los usuarios que sigan los pasos que se incluyen a continuación para introducir datos mediante un dispositivo lector de tarjeta de banda magnética:

1. Inserte la tarjeta en la ranura con la banda magnética hacia la parte externa del terminal. Asegúrese de que la tarjeta presione firmemente la ranura.
2. Deslice la tarjeta hacia abajo por la guía de la ranura y extráigala.

   Nota: no deslice la tarjeta en ángulo o el terminal no aceptará los datos.

   Si el terminal no puede leer los datos, el indicador LED se pondrá rojo. Vuelva a insertar la tarjeta en la ranura y deslice la tarjeta por el lector.

Tarjetas inteligentes sin contacto y tarjetas de proximidad

Secure Access admite tarjetas inteligentes sin contacto Legic y Mifare, así como tarjetas de proximidad EM Marin, HID, Hitag e Indala. Para introducir los datos de validación, los usuarios deben pasar la tarjeta de proximidad a una distancia máxima de 2,5 cm respecto al lector externo.

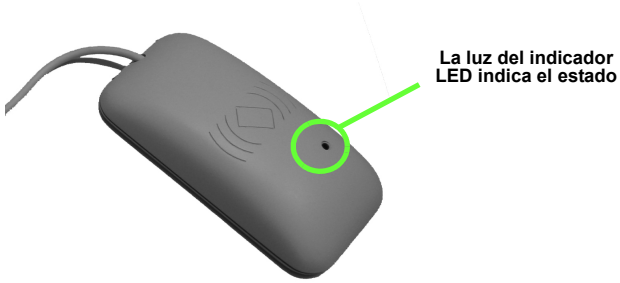
Utilización de una tarjeta de proximidad o una tarjeta inteligente

Para introducir datos mediante una tarjeta de proximidad o una tarjeta inteligente, pase la tarjeta a una distancia de unos 2,5 cm con respecto al símbolo de proximidad que figura en la parte superior del dispositivo lector de tarjetas. Para localizar el lector de tarjetas de proximidad en el módulo del lector de datos, busque el símbolo siguiente:

Si la tarjeta se pasa incorrectamente, el indicador LED se pondrá rojo y parpadeará.

Señales y modos de lectores de tarjetas

Secure Access muestra los mensajes a través de un indicador LED que se encuentra en el módulo del lector de tarjetas.



El comportamiento del indicador LED es el mismo para ambos tipos de lectores de tarjetas, salvo que se indique otra cosa. Es posible que se muestren las señales siguientes:

Comportamiento del indicador LED	Significado
Rojo fijo	El subsistema de autenticación se encuentra en modo Inactivo; está preparado, pero no hay ninguna sesión activa.
Verde fijo	El dispositivo de autenticación se encuentra en modo Preparado y hay una sesión activa. Este estado también se muestra si se utiliza un lector de tarjetas USB mientras se enciende el dispositivo multifunción y el controlador de red aún no se ha inicializado.

Comportamiento del indicador LED	Significado
Luz verde que parpadea lentamente	Se han recibido los datos del lector de tarjetas y el dispositivo está a la espera de que se autentique la sesión activa o el usuario introduzca datos (por ejemplo, el autorregistro de la tarjeta o un mensaje para liberar todos los trabajos).
Luz roja que parpadea lentamente	El subsistema de autenticación no está conectado al servidor.
Luz roja que parpadea rápidamente	Tarjeta no válida; acceso denegado.

El subsistema de autenticación tiene dos modos de funcionamiento: Inactivo y Preparado.

Un subsistema de autenticación que está listo para ser utilizado se encuentra en modo Inactivo. Cuando se pasa una tarjeta con banda magnética, el dispositivo cambia al modo Preparado. El dispositivo vuelve al modo Inactivo cuando un usuario completa una transacción o después de un período de inactividad configurable, que se haya definido en el dispositivo multifunción, en el modo Preparado.

Nota: el subsistema de autenticación vuelve al modo Inactivo si se activa el temporizador del modo de reposo del dispositivo multifunción.

Cuando el dispositivo se encuentra en el modo Inactivo, el indicador LED del lector de tarjetas emite una luz roja fija.

Durante el modo Preparado, el color del indicador LED del lector de tarjetas es verde fijo, y el usuario puede empezar a utilizar el dispositivo controlado para llevar a cabo una transacción.

Administración de Secure Access

Todas las tareas de administración se realizan en Secure Access Manager. De forma prefijada, el programa de instalación instala Secure Access Manager en el menú Inicio.

Vaya a **Inicio** > **Todos los programas** > **Xerox Secure Access** > **Secure Access Manager**

> Nota: debe tener privilegios administrativos en el servidor Secure Access para iniciar Secure Access Manager.

Para poder abrir Secure Access Manager, debe seleccionar el servidor CAS con el que desee trabajar. El servidor CAS se valida en una base de datos de autenticación exclusiva, por lo que no es necesario escribir el nombre de la base de datos correspondiente ni seleccionarlo en la lista.

La interfaz de Secure Access Manager se divide en cinco áreas. Cuando seleccione una tarea de las herramientas, el contenido del panel derecho se actualizará para mostrar las opciones disponibles.

Idiomas disponibles

Durante la instalación de Secure Access, el asistente de instalación le solicitó que especificara el idioma que utilizarán los componentes de la instalación. Esta configuración se aplica solamente a la interfaz de Secure Access Manager.

El idioma que se muestra en el panel frontal del dispositivo multifunción depende de la configuración del dispositivo. El servidor Secure Access comprueba la configuración de idioma del dispositivo multifunción cada vez que un usuario pasa su tarjeta. Si se activa en el dispositivo multifunción algún idioma que no sea inglés, francés, alemán, italiano o español, los mensajes de Secure Access aparecerán en inglés de forma prefijada.

Configuración y gestión 4

Contenido del capítulo:

La configuración hace referencia a los parámetros de software necesarios para establecer comunicación entre los dispositivos multifunción, los dispositivos de autenticación y el servidor Secure Access. Asegúrese de seguir los pasos descritos en la página 24 para obtener los mejores resultados.

Este capítulo proporciona información acerca de:

- La realización de todos los pasos de la configuración inicial
- La adición de los dispositivos multifunción a la base de datos de Secure Access
- La asociación de un dispositivo de autenticación de Secure Access a un dispositivo multifunción cuando no se utiliza un lector de tarjetas USB
- La aplicación de la autenticación y la configuración de las opciones de autenticación adicionales
- La importación y sincronización de cuentas de usuario con la sincronización de Active Directory
- La supervisión de eventos de autenticación

Flujo de trabajo de configuración

Siga los pasos en el orden en que se presentan a continuación. De lo contrario, la instalación será incompleta.

Antes de empezar, asegúrese de haber instalado correctamente el servidor Secure Access. Siga las instrucciones que se proporcionan en la Guía de instalación de Xerox Secure Access Unified ID System®. Instale el servidor CAS y al menos un motor DCE y un motor DRE.

1. **Configuración del dispositivo multifunción de Xerox para aceptar la autenticación de red a través del mecanismo Xerox Secure Access**

   Este paso se realiza a través de Servicios de Internet de CentreWare, funcionalidad que está disponible mediante un navegador web. Consulte el CD de administración del sistema del dispositivo multifunción para obtener información sobre cómo instalar y configurar Xerox Secure Access en el dispositivo.

2. **Adición de dispositivos multifunción a la base de datos de Secure Access**

   Cree una entrada para cada dispositivo multifunción en Secure Access Manager. Asigne cada dispositivo multifunción a un servidor de impresión DRE específico (si es necesario).

3. **Configuración de la impresión Follow-You**

   Nota: este paso es opcional y solo debe configurarse cuando es necesario utilizar la impresión Follow-You en el sitio.

   Para configurar la impresión Follow-You, cree grupos de extracción que agrupan dispositivos de características similares. Cuando el usuario envíe un documento a un dispositivo multifunción de un grupo de extracción, puede autenticarse en cualquier dispositivo multifunción del grupo de extracción y "extraer" el trabajo en cola que debe imprimirse en dicho dispositivo multifunción.

4. **Configuración de parámetros de autenticación**

   Configure los parámetros que Secure Access necesitará para autenticar las peticiones de acceso por parte de los usuarios, incluidas la activación de mensajes secundarios y la configuración de datos de tarjeta.

5. **Importación y sincronización de cuentas de usuario**

   Configure los parámetros de sincronización de Active Directory y, a continuación, importe las cuentas de usuario existentes a la base de datos de Secure Access.

6. **Instalación del servicio personalizado Release My Documents**

   Para permitir que los usuarios puedan ver y liberar uno o varios documentos de la cola de impresión segura directamente desde el panel frontal del dispositivo multifunción, instale el servicio personalizado Release My Documents.

7. **Configuración del autorregistro de tarjetas de usuario**

   Para permitir que los usuarios puedan autorregistrar sus tarjetas de banda magnética.

Adición de dispositivos multifunción a la base de datos de Secure Access

Todos los dispositivos multifunción deben registrarse en la base de datos de Secure Access. Debe asignar un nombre exclusivo a cada dispositivo multifunción y para ello necesita la dirección IP de red de cada dispositivo.

Este paso consta de dos pasos secundarios con el fin de facilitar las tareas de administración: la especificación de parámetros para los dispositivos y la asociación de los dispositivos multifunción al dispositivo de autenticación de Secure Access.

Especificación de parámetros para los dispositivos

1. En Secure Access Manager, haga clic en **Devices** (Dispositivos).
2. En Settings (Configuración), haga clic en **Add...** (Agregar) en la lista de dispositivos.
3. En el cuadro de diálogo Physical Device Summary (Resumen de dispositivos físicos) que aparece, escriba la información necesaria, tal como se describe en la tabla siguiente.

   Nota: los campos del fabricante y del modelo se rellenan automáticamente la primera vez que el dispositivo se comunica con el motor DRE. La próxima vez que abra este cuadro de diálogo, se mostrará esta información.

Valor	Descripción
Name (Nombre)	Escriba un nombre único para este dispositivo multifunción. Este nombre se utilizará para identificar el dispositivo en Secure Access Manager.
Hostname/IP address (Nombre de host/Dirección IP)	Escriba la dirección IP o el nombre de host. Asegúrese de que puede determinar el nombre de host si no conoce la dirección IP.
Description (Descripción)	Introduzca una descripción que ayude a otros administradores a identificar el dispositivo, normalmente por la ubicación. Por ejemplo: "segundo piso, RR. HH.".
Authentication Device (Dispositivo de autenticación)	Seleccione el dispositivo de autenticación de Secure Access (a partir de la dirección MAC) que controlará el acceso a este dispositivo multifunción. Nota: si utiliza un lector de tarjetas USB Secure Access, no se asocia ningún dispositivo de autenticación, por lo que deberá dejarlo como "<lector USB>".
Secure Access compatibility	• **MFP with Secure Access capability** (Dispositivo multifunción con Secure Access): seleccione esta opción si utiliza un lector de tarjetas USB o un dispositivo multifunción de Xerox que funciona con Secure Access. Especifique también el **ID del administrador** y la **clave** asociados a este dispositivo multifunción. • **Other type of MFP or printer** (Otro tipo de dispositivo multifunción o impresora): seleccione esta opción si el dispositivo de autenticación se utiliza para la impresión Follow-You con cualquier dispositivo multifunción o impresora que no sea compatible con Secure Access.

Valor	Descripción
Server (Servidor)	Introduzca el nombre del servidor que tiene DCE instalado y que controlará este dispositivo multifunción o impresora.
Initialize Secure Access device (Inicializar el dispositivo de Secure Access)	El dispositivo de Secure Access se inicializa de forma automática la primera vez que se configura. Si se cambia de dispositivo multifunción, inicialice el dispositivo de Secure Access haciendo clic en este botón. Aparecerá una ventana emergente para confirmar que la inicialización se ha llevado a cabo correctamente. Nota: puede utilizar este botón para instalar el servicio personalizado Release My Documents. Para obtener más información, consulte Configuración del servicio personalizado Release My Documents en la página 41.
Behavior (Comportamiento)	Si utiliza el supervisor de puertos de Secure Access para activar la impresión Follow-You, puede seleccionar una de las dos opciones de liberación siguientes: • **At assigned control terminal** (En el terminal de control asignado): el usuario debe pasar la tarjeta por el dispositivo multifunción para liberar los documentos enviados a dicho dispositivo. • **Release documents from pull group** (Liberar documentos desde el grupo de extracción): después de la autenticación, el usuario puede seguir las instrucciones del panel frontal para seleccionar los documentos en cola desde un grupo de extracción específico. Para obtener más detalles, consulte Configuración de la impresión Follow-You en la página 32. Si utiliza los supervisores de puertos de Windows, estos valores no tendrán efecto.

4. Haga clic en **OK** para guardar los cambios.

   Nota: si Secure Access detecta que el dispositivo tiene habilitados los servicios personalizados y usted ha realizado cambios en la ventana Devices (dispositivos), se abrirá otra ventana:

   - Si la extensión Release My Documents no está instalada en el dispositivo, aparecerá el mensaje: "Do you want to enable Follow-You printing?" ("¿Desea activar la impresión Follow-You?").
   - Si está instalada, aparecerá el mensaje: "Do you want to keep Follow-You printing enabled?" ("¿desea mantener activada la impresión Follow-You?")

Asociación del dispositivo multifunción a un dispositivo de autenticación de Secure Access

Nota: si utiliza un lector de tarjetas USB de Secure Access, puede omitir este paso.

Cuando se enciende por primera vez un dispositivo de autenticación conectado a la red, el motor DCE registra el dispositivo. El dispositivo aparece en Secure Access Manager como un dispositivo de autenticación de Secure Access sin asignar. Posteriormente, debe asociar el dispositivo multifunción a un dispositivo de autenticación de Secure Access específico. Utilice la hoja separable (consulte la Guía de instalación) que rellenó durante la configuración del hardware para asignar cada dispositivo de autenticación al dispositivo multifunción correspondiente.

1. En Secure Access Manager, haga clic en **Devices** (dispositivos) y, a continuación, seleccione el dispositivo multifunción que desea configurar.
2. En el cuadro de diálogo Physical Device Summary (Resumen del dispositivo físico), muestre la lista de direcciones de hardware.
3. Utilice la hoja separable para localizar la dirección MAC del dispositivo de autenticación que controlará el acceso a este dispositivo multifunción específico.
4. Haga clic en **OK** para guardar los cambios.

Configuración de parámetros de autenticación

Antes de poder importar cuentas de usuario, debe configurar el servidor CAS para validar las cuentas con los PIN de cuentas principales y secundarias. La información de PIN conecta una cuenta de usuario de Secure Access con la información de una tarjeta de banda magnética.

El PIN principal es la secuencia numérica que identifica al usuario de forma exclusiva y suele ser el número de la tarjeta. Para introducir el PIN principal, el usuario debe pasar la tarjeta.

Si prefiere añadir un nivel más de seguridad, puede activar números PIN secundarios. Si se activan, el usuario debe pasar la tarjeta en primer lugar y, a continuación, introducir una "clave" adicional en el panel frontal del dispositivo multifunción. El usuario tendrá acceso al dispositivo multifunción solo cuando se hayan autenticado los datos de la tarjeta de banda magnética y la clave del PIN secundario.

1. En Secure Access Manager, seleccione **Configuration** > **Authentication device settings**.
2. En el área **Authentication mechanisms** (Mecanismos de autenticación) seleccione uno o varios mecanismos de autenticación:
   - Mantenga seleccionado **Secure Access PINs** (PIN de Secure Access) solo si desea conectar una cuenta de impresión de Secure Access con información de inicio de sesión.
   - Active **External user ID and password** (ID de usuario y clave externos) solo si utiliza tarjetas de banda magnética para verificar toda la información de usuario fuera de Secure Access.
   - Active **Secure Access PIN with external password** (PIN de Secure Access con clave externa) si los usuarios van a pasar sus tarjetas para identificarse, pero también deberán proporcionar su clave de cuenta de usuario en el dominio de Secure Access. Secure Access comprobará el nombre de cuenta en la base de datos y, a continuación, verificará la cuenta con la autoridad externa seleccionada para el inicio de sesión de red.

   Nota: si selecciona un mecanismo de autenticación externo, el campo **Enable secondary prompt** (Activar mensaje secundario) se activará automáticamente. La autenticación externa no se puede realizar si no se ha proporcionado la información del PIN secundario.
3. En el área **External authorities** (Autoridades externas), seleccione una o varias autoridades externas solo si seleccionó un método de autenticación correspondiente:
   - Seleccione **Windows** para validar las cuentas con un dominio de Windows prefijado. Escriba el nombre del dominio en el campo **Default domain** (Dominio prefijado).
   - Seleccione **NetWare** para validar las cuentas con un contexto NetWare prefijado. Escriba el nombre en el campo **Default context** (Contexto prefijado).

   Nota: debe instalar el cliente de Novell NetWare para Windows en el servidor CAS si va a realizar una validación con un contexto NetWare.

   - Seleccione **LDAP** para validar las cuentas con un servidor LDAP prefijado. Escriba el nombre del servidor LDAP y, a continuación, seleccione un tipo LDAP de la lista. Seleccione Force SSL encryption (Forzar cifrado SSL) si desea utilizar el cifrado Capa de sockets seguros.

4. En el área **Card setup** (Configuración de la tarjeta), realice los pasos siguientes:
   a. Especifique la posición de inicio y parada de los datos en los campos correspondientes. Los datos recuperados desde estas posiciones se utilizarán como el PIN principal.
   b. Haga clic en **<None>** (Ninguno), junto a **HID decoding** (Descodificación HID) si utiliza un lector de tarjetas de proximidad HID. Es necesario configurar los dispositivos de autenticación para mostrar la información de tarjeta en formato convencional.

   Para obtener más detalles acerca de la especificación de parámetros de descodificación, consulte Descodificación HID en la página 30.
   c. Seleccione **Auto-register primary PINs** (Autorregistrar PIN principales) para que los usuarios puedan registrar una tarjeta de banda magnética no reconocida con el fin de utilizarla en el futuro. Consulte Autorregistro de tarjetas de banda magnética en la página 31 para obtener más detalles.
5. En el área de **Secure Access device prompts** (Mensajes de dispositivo de Secure Access), introduzca el texto prefijado que aparecerá en el panel frontal del dispositivo multifunción:
   a. Introduzca el **título** que se mostrará en todos los mensajes.
   b. Introduzca el texto del **mensaje de inicio de sesión** que se mostrará para solicitar al usuario que inicie sesión. Por ejemplo: "Please swipe your card to login" (Pase la tarjeta para iniciar sesión).
   c. Seleccione **Enable secondary prompt** (Activar mensaje secundario) para que aparezca un mensaje en el panel frontal del dispositivo multifunción de Xerox para solicitar al usuario que introduzca un código PIN secundario (o una clave).
   d. Seleccione **Enable release all jobs prompt** (Activar mensaje para liberar todos los trabajos) para mostrar un mensaje en el panel frontal del dispositivo multifunción de Xerox para preguntar al usuario si desea liberar todos los trabajos que están en la cola de impresión.
6. En el área **SNMP**, especifique los **nombres de comunidad Get** y **Set**.

   Nota: si cambia los nombre prefijados en Secure Access, deberá cambiarlos también en todos los dispositivos físicos para que la comunicación SNMP funcione. Consulte la documentación del dispositivo multifunción para obtener información acerca de cómo cambiar estas opciones.
7. Introduzca el número **JBA Account ID** (Identificación de cuenta JBA) si desea utilizar Secure Access con una aplicación de contabilidad JBA de otro fabricante.
8. Especifique una **hora** para **Job Expiry** (Caducidad del trabajo) después de la cual los trabajos que queden en la cola de impresión caducarán y serán eliminados de la cola. El valor prefijado es 1 hora.
9. Si utiliza nombres de comunidad SNMP ("público" para el acceso de lectura y "privado" para el acceso de escritura) no prefijados en su red, especifíquelos en los campos correspondientes del cuadro de diálogo. Tenga en cuenta que todos los dispositivos deben utilizar los mismos nombres de comunidad.

   Nota: si no escribe los nombres de comunidad, el servidor Secure Access no podrá detectar automáticamente los tipos de dispositivos cuando usted cree puertos nuevos, pero podrá crear los puertos si especifica manualmente los datos de conexión.
10. Haga clic en **OK** para guardar los valores.

Descodificación HID

Para configurar la descodificación HID, realice los pasos siguientes:

1. En Secure Access Manager, seleccione **Configuration** > **Authentication device settings**.
2. Haga clic en **<None>** (Ninguno), junto a **HID decoding** (Descodificación HID) en el área Card Setup (Configuración de la tarjeta).
3. En el cuadro de diálogo **HID decoding** (Descodificación HID), realice los pasos siguientes:
   - Si conoce el tipo de codificación, introduzca la información de codificación de tarjeta HID que se especifica a continuación. Si no conoce el tipo de codificación, póngase en contacto con su proveedor de tarjetas HID para determinar cuál es la codificación que utilizan sus tarjetas de proximidad.
   - En el caso de que no tenga que extraer información de código de recurso, seleccione únicamente el **ID code** (Código de ID). Si tiene que extraer el código de recurso y el código de ID, seleccione ambas opciones.

   a. En el campo **Facility Start**, introduzca la posición en la secuencia de bits sin formato (basada en 0, de izquierda a derecha, inclusiva) donde empieza el código de recurso.
   b. En el campo **Facility End**, introduzca la posición en la secuencia de bits sin formato (basada en 0, de izquierda a derecha, inclusiva) donde finaliza el código de recurso.
   c. En el campo **Facility Width**, introduzca el número de dígitos decimales de la porción del recurso del valor que el dispositivo de autenticación mostrará. Todos los números se completarán con ceros a la izquierda, según corresponda. Si su sitio o el formato de la tarjeta HID no utiliza un código de recurso, o si no necesita que se devuelva como parte del valor de tarjeta, introduzca una anchura de 0 para desactivar la extracción del número de recurso.
   d. En el campo **ID Start**, introduzca la posición en la secuencia de bits sin formato (basada en 0, de izquierda a derecha, inclusiva) donde empieza el código de ID.
   e. En el campo **ID End**, introduzca la posición en la secuencia de bits sin formato (basada en 0, de izquierda a derecha, inclusiva) donde finaliza el código de ID.
   f. En el campo **ID Width**, introduzca el número de dígitos decimales de la parte del código de ID del valor que mostrará el dispositivo de autenticación. Todos los números se completarán con ceros a la izquierda, según corresponda. El dispositivo de autenticación devolverá un valor único cada vez que se pase la tarjeta. Este valor es el código de recurso descodificado seguido del ID descodificado.
   g. Haga clic en **OK** para guardar los cambios.

Autorregistro de tarjetas de banda magnética

Si desea que los usuarios puedan autorregistrar sus tarjetas de banda magnética, debe activar esta opción en Secure Access.

1. En Secure Access Manager, seleccione **Configuration > Authentication device settings**.
2. Seleccione **Auto-register primary PINs** (Autorregistrar PIN principales) en el área **HID decoding** (Descodificación HID).
3. Haga clic en **OK** para guardar los cambios.

Cuando un usuario pase una tarjeta no registrada, deberá iniciar sesión en el dispositivo multifunción con unas credenciales de usuario válidas (ID de usuario y clave). Las credenciales de usuario deben existir previamente en el servidor CAS para permitir el autorregistro.

Una vez que el usuario registra su tarjeta, la siguiente vez que la pase, la información de su cuenta se asociará inmediatamente a la tarjeta y podrá iniciar sesión sin necesidad de introducir sus credenciales de usuario manualmente. Si se ha configurado un PIN secundario, es posible que se le solicite al usuario.

> Nota: si se selecciona la opción **Secure Access PIN with external password** (PIN de Secure Access con clave externa) al configurar el autorregistro de tarjetas, el PIN de Secure Access se sobrescribirá con los datos de la tarjeta de banda magnética al autenticarla y registrarla. El PIN de Secure Access PIN dejará de ser válido para iniciar sesión.

Configuración de la impresión Follow-You

La impresión Follow-You permite al usuario enviar un trabajo de impresión a un dispositivo multifunción específico, pero realizar la autenticación en otro dispositivo multifunción y, a continuación, ver una lista de los trabajos retenidos en una cola segura. A continuación, el usuario puede "extraer" el trabajo de impresión en el dispositivo multifunción en el que se haya autenticado, aunque no sea el dispositivo original seleccionado para la impresión.

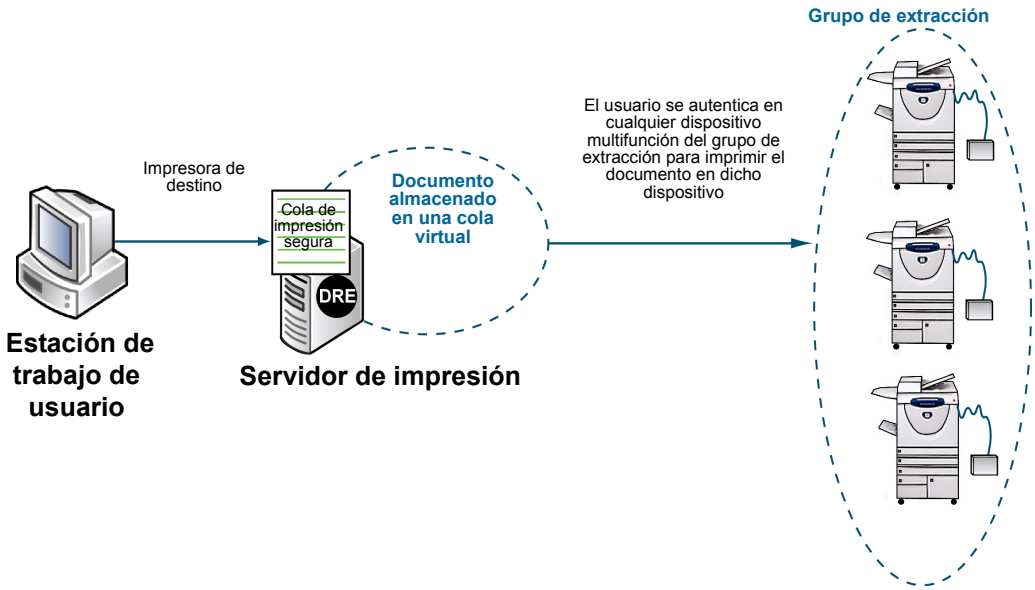


Figura 4-1: Flujo de trabajo de usuarios de impresión Follow-You

Para configurar la impresión Follow-You, debe realizar dos pasos:

1. Utilice el supervisor de puertos de Secure Access para activar la configuración entre el servidor de impresión y todos los dispositivos multifunción controlados. Puede convertir los puertos Windows existentes en puertos de Secure Access. El supervisor de puertos intercepta todos los documentos enviados a los dispositivos de un grupo de extracción y los almacena en la cola segura hasta que son liberados por el usuario autenticado. Consulte Conversión de puertos para utilizar el supervisor de puertos de Secure Access en la página 33 para obtener instrucciones al respecto.
2. Cree los grupos de extracción con Secure Access Manager. Consulte Creación de grupos de extracción en la página 34.

Si desea permitir que el usuario pueda ver los trabajos que tiene en espera en la cola de impresión segura directamente en el panel frontal del dispositivo multifunción, actualícelo para que incluya el servicio personalizado Release My Documents. Consulte Configuración del servicio personalizado Release My Documents en la página 41 para obtener instrucciones al respecto.

Conversión de puertos para utilizar el supervisor de puertos de Secure Access

Secure Access utiliza puertos especializados para activar la impresión Follow-You. Cada dispositivo que forme parte de un grupo de extracción debe utilizar un supervisor de puertos de Secure Access. Si dispone de dispositivos ya configurados para utilizar Windows, podrá convertir fácilmente los puertos.

1. Asegúrese de que los dispositivos que desea convertir están encendidos, conectados a la red y configurados para imprimir.
2. Desde **Mi PC**, desplácese hasta la ubicación donde ha instalado Secure Access.
3. Abra la carpeta **Tools** (Herramientas) y haga doble clic en **SAPrinterConversionWizard.exe**.
4. En la pantalla de bienvenida del asistente para conversión de la impresora, haga clic en Next (Siguiente).
5. Seleccione la **ubicación del servidor de impresión**.

   Si el servidor de impresión (DRE) se encuentra en la máquina local, seleccione **Local machine**; de lo contrario, seleccione **Remote server** (Servidor remoto).
6. Seleccione **Convert printers to use the Secure Access Port Monitor** (Convertir impresoras para utilizar el supervisor de puertos) y, a continuación, haga clic en **Next** (Siguiente).
7. Seleccione o desmarque las impresoras en la lista **Convert Printers** (Convertir impresoras) y, a continuación, haga clic en **Next** (Siguiente).
8. Haga clic en **Finish** (Finalizar) para completar la conversión.

Creación de una cola de impresión con un puerto de Secure Access

En función del hardware de impresión, es posible que necesite más de un puerto que utilice el supervisor de puertos de Secure Access en un servidor de impresión. Puede configurar una nueva definición de impresora que utilice el supervisor de puertos de Secure Access.

1. Mediante la interfaz de Windows estándar, abra el **Asistente para agregar impresoras** de Windows.
2. Siga los mensajes para agregar una impresora local y crear un puerto nuevo.
3. Cuando se le solicite, seleccione el **puerto de Secure Access** como el tipo de puerto que desea crear y haga clic en Siguiente. Se abrirá el asistente para agregar puertos de impresora de Secure Access para solicitarle que se asegure de que la impresora está encendida, conectada a la red y configurada correctamente.
4. Haga clic en **Siguiente** y seleccione **Impresora física** como el **tipo de dispositivo** de la lista desplegable.
5. Especifique un **nombre de impresora** o una **dirección IP**.
6. El asistente proporciona un **nombre de puerto** basado en el nombre de impresora o en la dirección IP. Cambie el nombre manualmente si lo desea.
7. Haga clic en **Siguiente** para continuar con las opciones de configuración del puerto. Aparece la pantalla de configuración de puertos. La **información del dispositivo detectado** aparece automáticamente si el asistente puede recopilar datos de la impresora.

8. Especifique si se utilizará una configuración estándar o personalizada para este puerto.

   Si selecciona la opción de **configuración personalizada**:

   a. Si selecciona la comunicación mediante un **puerto sin formato**, identifique el número de **puerto** TCP y especifique si el supervisor de puertos debe mantener la conexión abierta.
   b. Si selecciona **LPR**, especifique el nombre de la **cola** de impresión en el dispositivo físico (por ejemplo, PORT1).
   c. Si selecciona un **dispositivo específico**, seleccione el **fabricante** y el **modelo** adecuados en las listas desplegables. El dispositivo utiliza los parámetros de comunicación prefijados relevantes basados en dichas selecciones.

9. Haga clic en **Siguiente** y especifique el **nombre del dispositivo físico**. Este será el nombre del dispositivo tal como aparece en Secure Access.
10. Revise los detalles para el puerto nuevo y el registro del dispositivo, y haga clic en **Finalizar** para cerrar el asistente para agregar puertos de impresora de Secure Access o en **Atrás** para cambiar cualquiera de estas opciones. Cuando se cierra el asistente para agregar puertos de Secure Access, aparece nuevamente el Asistente para agregar impresoras de Windows.
11. Complete los pasos restantes en el asistente para agregar impresoras. Cuando se le solicite, seleccione **Sí** para imprimir una página de prueba.
12. Confirme los detalles de la impresora de Windows y haga clic en **Terminar** para salir del asistente o en **Atrás** para cambiar las opciones según convenga.

Creación de grupos de extracción

Los grupos de extracción que cree deben reflejar las necesidades de su empresa. Por ejemplo, puede agrupar dispositivos compatibles según la ubicación física, el departamento, el fabricante, etc. También puede crear grupos de extracción que incluyan una selección de dispositivos de un solo servidor de impresión.

El controlador de dispositivos seleccionado para un grupo de extracción debe ser compatible con todos los dispositivos asociados a ese grupo. Si desea que un trabajo de impresión generado para un dispositivo multifunción se imprima correctamente en otro dispositivo multifunción, asegúrese de que el otro dispositivo pueda interpretar todos los comandos incluidos en la secuencia de datos del controlador.

1. En Secure Access Manager, haga clic en los dispositivos multifunción existentes que desee asignar al mismo grupo de extracción.
2. En el cuadro de diálogo Physical Device Summary (Resumen del dispositivo físico), seleccione **Release documents from pull group** (Liberar documentos del grupo de extracción). Escriba el nombre del grupo de extracción (puede ser cualquier nombre significativo) y, a continuación, haga clic en **OK** para aplicar el cambio.

   Nota: solo tiene que escribir el nombre del grupo de extracción la primera vez que lo utilice. A continuación, se mostrará en la lista de forma automática.
3. Repita los pasos 1 y 2 para seleccionar dispositivos y crear otros grupos de extracción.

Importación y sincronización de cuentas de usuario

Para activar la autenticación, deberá crear cuentas de usuarios que coincidan con los atributos utilizados a la hora de pasar la tarjeta de banda magnética por la ranura. Cuando un usuario pasa su tarjeta por la ranura, el dispositivo de autenticación reenvía la petición de acceso al DCE, que seguidamente reenvía los detalles de la tarjeta al servidor CAS. Si el servidor CAS localiza una cuenta de usuario con atributos que coinciden con los de la tarjeta, el dispositivo multifunción se desbloquea y el usuario puede seguir adelante con la tarea de fax, escaneado, copia o liberación de un trabajo de impresión.

En Secure Access, hay tres métodos para importar cuentas de usuario:

- Utilice Active Directory para importar cuentas (y si lo desea, sincronizarlas).
- Importe cuentas de usuario desde un archivo CSV.
- Cree cuentas manualmente en Secure Access Manager.

Utilización de ADS para importar usuarios existentes

Si dispone de un servidor de Active Directory, puede seleccionar la información de cuenta que desea importar y sincronizar. La sincronización minimizará la sobrecarga administrativa y permitirá que las actualizaciones de cuenta se realicen de forma automática.

Si se realizan los pasos descritos a continuación, se ejecutará una tarea en segundo plano. En Secure Access Manager, haga clic en la herramienta Users para ver el resultado de la tarea. La lista de usuarios se rellenará automáticamente cuando la tarea finalice.

> Nota: los servicios de Secure Access deben iniciarse mediante una cuenta de dominio que tenga acceso al servidor de Active Directory de contacto. Asegúrese de que ha iniciado sesión como administrador del dominio. Si los servicios se inician con una cuenta administrativa local, la sincronización con Active Directory no se llevará a cabo correctamente.

Es importante seleccionar las opciones en el orden correcto en el cuadro de diálogo de sincronización de Active Directory. Por tanto, siga cuidadosamente los pasos descritos a continuación.

1. En Secure Access Manager, haga clic en **Configuration** > **Active Directory Synchronization**.
2. En el área **Domain controllers** (Controladores de dominio), haga clic en **Add** (Agregar). Un controlador de dominio es un servidor que proporciona acceso a Active Directory a los PC que forman parte de dicho dominio. Escriba el nombre del controlador en el campo.
3. En el área **Containers** (Contenedores), haga clic en **Add** (Agregar). Un contenedor es una carpeta en la estructura de árbol de Active Directory que contiene usuarios, grupos o equipos PC.

> ⚠ **PRECAUCIÓN:** asegúrese de que los contenedores OU que seleccione contengan datos de cuenta de usuario únicamente. Si los OU contienen otros datos (por ejemplo, información del sistema o de contacto), se obtendrán resultados inesperados. Es posible que tenga que crear contenedores OU específicos con el fin de utilizarlos únicamente para realizar importaciones y sincronizaciones.

4. Ajuste la opción **Synchronization interval** (Intervalo de sincronización) para cambiar la frecuencia con la que Secure Access sincroniza su base de datos con el servidor de Active Directory especificado. El valor del intervalo de sincronización debe ser al menos de 15 minutos.
5. Seleccione o elimine la selección de las opciones de **actualización de Active Directory que deben aplicarse** (**adiciones**, **eliminaciones** o **modificaciones**) para especificar las cuentas de Active Directory que Secure Access recibirá y aplicará a la base de datos de cuentas en sincronizaciones sucesivas.

   Puede optar por importar usuarios añadidos o modificados, o eliminar cuentas inactivas de la base de datos de Secure Access. Mantenga los valores prefijados de estas opciones para garantizar que las cuentas se actualicen y se mantengan sincronizadas con el servidor de Active Directory.
6. Los atributos de **Assign Values from Active Directory** (Asignar valores de Active Directory) ahorran tiempo y esfuerzo mediante la asignación de atributos particulares a todos los usuarios del contenedor seleccionado. Tenga en cuenta que debe especificar el nombre de atributo de Active Directory y no la etiqueta de campo. Aunque es posible actualizar cuentas de usuario individuales más adelante, seleccione estos atributos antes de importar para agilizar la creación de cuentas.

   Los atributos **Primary PIN** (PIN principal) y **Secondary PIN** (PIN secundario) asignan los valores de PIN numéricos encontrados en el servidor de Active Directory a los campos PIN principal y PIN secundario de Secure Access. Seleccione el valor de PIN secundario si desea importar dichos campos, que el usuario puede introducir en el panel frontal del dispositivo multifunción (un mensaje secundario es como una clave que añade otro nivel de seguridad) si el mensaje secundario está activado en **Configuration** > **User Authentication Device Settings**. Escriba el nombre de atributo de los campos PIN1 (normalmente el número de tarjeta) y PIN2 que se utiliza en el servidor de Active Directory.

   Los atributos **Primary PIN** (PIN principal) y **Secondary PIN** (PIN secundario) también pueden asignarse a una dirección de email.
7. Haga clic en **Import** (Importar) para iniciar inmediatamente la tarea de importación por primera vez. La tarea de importación se ejecuta en segundo plano y puede tardar unos minutos en función del tamaño del servidor de Active Directory que esté importando.
8. Puede hacer clic en **OK** para salir del cuadro de diálogo. La tarea continuará ejecutándose aunque se cierre el cuadro de diálogo.
9. Después de unos minutos, actualice Secure Access Manager y, a continuación, compruebe la lista de usuarios para asegurarse de que las cuentas se han importado correctamente. Abra también las propiedades de una cuenta de usuario y asegúrese de que los ajustes sean correctos.

Adición de usuarios desde una importación de un archivo plano

Utilice la utilidad **SACmd.exe** para añadir, eliminar, modificar y realizar consultas de cuentas de usuario desde un archivo plano.

> Nota: este método consiste en una operación de importación que se realiza una sola vez y no sincroniza datos más allá de la importación.

Secure Access instala esta utilidad en el directorio del servidor de autenticación de forma prefijada: **Archivos de programa** > **Xerox** >**Secure Access** > **Tools**

Esta utilidad de línea de comandos acepta comandos con el formato siguiente:

```
SACmd  -s(Servidor) (Acción) (Obj_ID)| [(Opciones)]
Ejemplo: -sServidorPrueba add usuario1 "Pedro Sanz" pedros@casa.com pin1
pin2
```

Ejecute el comando con un archivo por lotes:

```
SACmd  -s(Servidor) -f(Archivo_lotes)
```

Proceso de archivo por lotes SACmd

SACmd utiliza un modo por lotes y admite un archivo CSV como archivo por lotes (un archivo por servidor). La operación por lotes permite ejecutar acciones de comandos, salvo el comando de consulta.

Nota: copie el archivo .csv en la carpeta **Secure Access** > **Tools**.

```
[ruta de Secure Access\Tools ]\SACmd –s(Servidor) –f
Nombre_archivo_lotes.csv
```

Formato archivo CVS: `(Acción), (Obj_ID)|All,  [(Detalles)]`

Los parámetros que aparecen entre paréntesis "( )" son obligatorios y los parámetros que aparecen entre corchetes "[ ]" son opcionales. Utilice la tabla siguiente para rellenar los parámetros.

Parámetro	Variables
Server	Especifique el nombre o dirección IP del servidor CAS.
Acción	Especifique la acción que deba aplicarse. Utilice una de las siguientes: • add: añadir usuario • delete: eliminar usuario • query: consultar la base de datos • modify: modificar un atributo de objeto
ID_objeto	Aplica la acción solo al ID de objeto especificado. Utilice las comillas dobles con los ID de objeto que tengan un espacio (por ejemplo, Pedro Lagos).
Opciones para el comando Acción	Especifique valores adicionales. Utilice las comillas dobles para los valores de detalle que tengan espacios o valores vacíos. Especifique las cantidades con un punto como separador decimal. Para la acción de modificación, coloque un signo de exclamación "!" para los campos necesarios que no desee modificar. (ID_usuario): ID de usuario (nombre_usuario): nombre de usuario (email): email del usuario

Add

Add (Agregar) permite añadir cuentas de usuario. Requiere valores hasta el campo final necesario (incluido).

Añadir un usuario:

```
add(ID_usuario) [(nombre_usuario) (email) (PINprincipal) (PINsecundario)]
```

Ejemplo:

```
SACmd -SMiServidor add PedroL "Pedro Lagos" "pedrol@casa.com" 123 Password
```

Delete

Delete (Eliminar) permite eliminar cuentas de usuario.

Eliminar un usuario:

```
delete (ID_usuario)
```

Ejemplo:

```
SACmd -SMiServidor delete PedroL
```

Modify

Modify (Modificar) permite al usuario modificar la configuración de la base de datos de usuarios. Requiere valores hasta el campo final necesario (incluido).

Modificación de un usuario:

```
modify (ID_usuario) [(nombre_usuario) (email) (PINprincipal)
(PINsecundario)]
```

Ejemplo: actualiza la dirección de email del usuario pedrol y mantiene el resto de la información:

```
SACmd -SMiServidor modify pedrol! pedrol@espacio.com
```

Creación de cuentas de forma manual

Puede utilizar Secure Access Manager para añadir cuentas de usuario individuales según las necesidades.

1. Seleccione Users (Usuarios), haga clic con el botón secundario en el panel Settings (Configuración) y seleccione **Add User** (Agregar usuario) en el menú.

2. En el cuadro de diálogo User Properties (Propiedades de usuario), escriba la información necesaria, tal como se describe en la tabla siguiente.

Campo	Description
ID de usuario	ID conectado a la base de datos para supervisar la cuenta.
Nombre completo	El nombre completo del usuario. Especifique un nombre completo para identificar fácilmente al usuario en la administración de cuentas o la administración del departamento. Este nombre también aparece en los estados de cuenta e informes.
Dirección de email	La dirección de email se proporciona al dispositivo multifunción para los distintos tipos de tareas como el escaneado a email.
PIN principal	El PIN principal suele ser el número de la tarjeta.
PIN secundario	El PIN secundario se utiliza como clave, y el usuario debe introducir este PIN en el panel frontal del dispositivo multifunción después de pasar la tarjeta para llevar a cabo la autenticación.
Confirmar PIN secundario	Vuelva a escribir el PIN secundario para confirmar la clave.

Supervisión de eventos de autenticación

Secure Access registra cada evento de autenticación en la base de datos de Secure Access. Puede generar un registro de autenticación para cualquier fecha y ver el historial de eventos con la información siguiente, por ejemplo:

- Error de autenticación
- Inicio de sesión (autenticación correcta)

Cada evento registrado contiene la información siguiente:

- Dirección IP de origen
- PIN principal
- Resultado de la validación
- Tipo de servidor
- Nombre de usuario
- Dirección de email
- Nombre de servidor

Para ver un registro de autenticación en Secure Access Manager, haga clic en **Authentication log** (Registro de autenticación) y, a continuación, haga clic con el botón secundario en **View log by date** (Ver registro por fecha). Seleccione la fecha y, a continuación, haga clic en **OK**.

Configuración del servicio personalizado Release My Documents

El servicio personalizado Release My Documents actualiza la impresora para que añada la opción correspondiente a la pantalla Servicios personalizados del panel frontal. Dicha pantalla (que se muestra más abajo) incluye los trabajos de impresión que están en cola para el usuario actual. El usuario puede seleccionar uno o más trabajos y liberarlos o eliminarlos directamente desde el panel frontal del dispositivo multifunción.

> Nota: la impresión Follow-You también debe ser configurada para habilitar esta funcionalidad. Consulte Configuración de la impresión Follow-You en la página 32 para obtener instrucciones al respecto.

Cuando el servicio personalizado Release My Documents no está instalado, la pantalla correspondiente no está disponible en el panel de control del dispositivo multifunción y, por lo tanto, el usuario no puede seleccionar trabajos individuales para liberarlos. En su lugar, inmediatamente después de autenticarse, el usuario recibirá un mensaje para liberar todos los trabajos pendientes en el servidor de impresión.

Cuando un usuario se autentica, se le notifica al DCE y éste conecta con el servidor de impresoras DRE para obtener una lista de todos los documentos que están en cola para ese usuario. La pantalla Release My Documents del panel frontal del dispositivo multifunción mostrará la información.

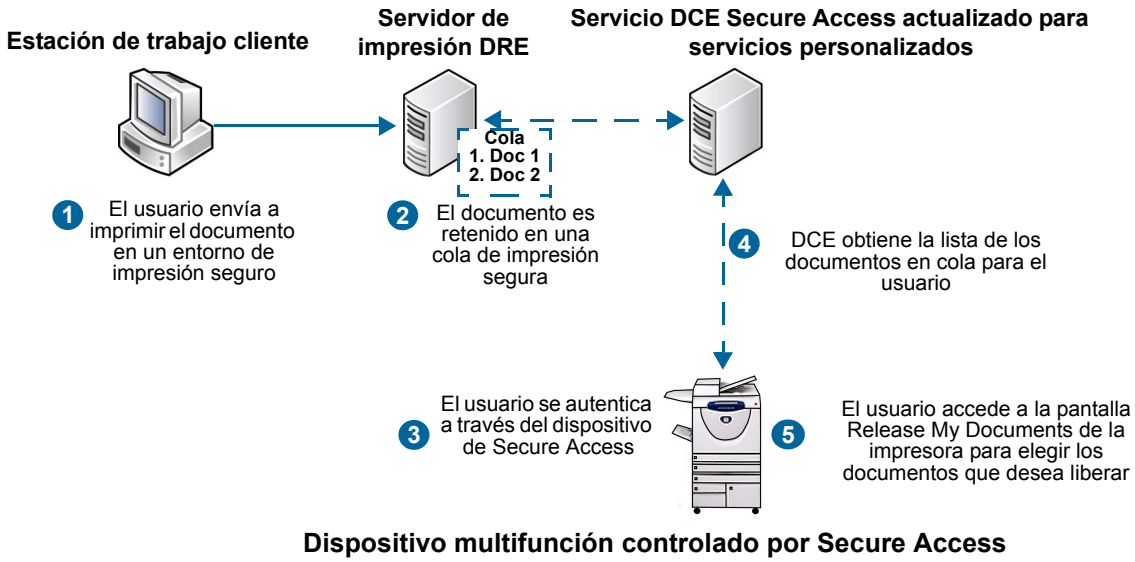


Figura 4-2: Arquitectura de Release My Documents

Incorporación del servicio Release My Documents al dispositivo

Si incorpora nuevos dispositivos a Secure Access Manager, se le solicitará que instale el servicio Release My Documents cuando haga clic en Aceptar después de hacer cambios en la ventana Device (Dispositivo). Consulte Especificación de parámetros para los dispositivos en la página 25 para obtener más detalles.

> Nota: añadir el servicio personalizado es opcional. Si no se añade, se solicitará al usuario que libere todos los documentos durante el proceso de autenticación.

Para incluir el servicio personalizado en un dispositivo ya configurado en Secure Access Manager, siga los pasos siguientes:

1. En Secure Access Manager, haga clic en **Devices** (Dispositivos).
2. Seleccione el dispositivo que desea actualizar de la lista.
3. En el cuadro de diálogo Physical Device Summary (Resumen del dispositivo físico), haga clic en el botón **Initialize Secure Access device** (Inicializar el dispositivo Secure Access)
4. Cuando aparezca el mensaje "Do you want to enable Follow-You printing?" ("¿Desea activar la impresión Follow-You"?, haga clic en **Yes** (Sí).

   Un archivo de instalación se ejecutará en segundo plano para actualizar el servició DCE con el fin de que muestre la pantalla Release My Documents en los servicios personalizados del panel frontal del dispositivo multifunción.

Para determinar si la instalación se ha realizado correctamente, autentíquese en el dispositivo multifunción y, a continuación, pulse **All Services** (Todos los servicios). Debería ver un botón llamado **Release my documents** (Liberar mis documentos). En función del modelo de dispositivo multifunción, puede que necesite pulsar el botón **Custom Services** (Servicios personalizados) para acceder a esta función.

Si la instalación no se ha realizado correctamente, el botón se llamará **Servicex**, donde "x" es un número (por ejemplo, Service4 o Service5). Para resolver el problema, consulte Solución de problemas de instalación del servicio personalizado Release My Documents en la página 52.

Pasos que debe seguir el usuario con Release My Documents

El diagrama que se presenta más adelante muestra los pasos que debe seguir el usuario. Después de enviar el trabajo de impresión, el usuario se dirige a un dispositivo multifunción controlado, se autentica a través del dispositivo de autenticación de Secure Access y, a continuación, selecciona **Custom Services** > **Release My Documents** (Liberar mis documentos) en el panel frontal para acceder a las funciones seguras de liberación de documentos.

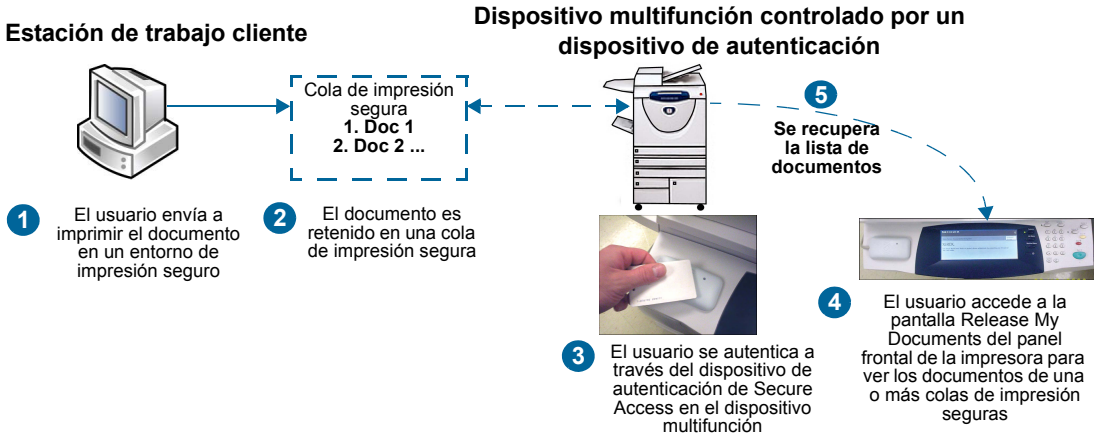


Figura 4-3: Pasos que debe seguir el usuario cuando está instalada la extensión Release My Documents

Apéndices

A

Contenido del capítulo:

Permisos de acceso de sincronización de directorios

SAModifyDeletedContainerSecurity.exe modifica los permisos de acceso administrativo en el contenedor de objetos eliminados en un servidor Active Directory de Windows para que Secure Access pueda acceder a los objetos durante las sincronizaciones de directorios.

De forma prefijada, solo los administradores de Active Directory tienen permiso de acceso. La cuenta de Windows que ejecuta los servicios de Secure Access necesitará este acceso si desea sincronizar las cuentas eliminadas entre Active Directory y Secure Access.

La cuenta que ejecute este comando deberá ser un administrador en el dominio de Active Directory.

Consulte Utilización de ADS para importar usuarios existentes en la página 35 para obtener más información sobre la configuración de las opciones de sincronización de Active Directory.

Secure Access instala esta utilidad de forma prefijada en el directorio del servidor de autenticación: **Archivos de programa > Xerox > Secure Access > Tools**.

Esta utilidad de línea de comandos acepta comandos con el formato siguiente:

```
SAModifyDeletedContainerSecurity.exe (-s servidor) [-p | {-r} -a
nombre_cuenta]
```

Los parámetros que aparecen entre paréntesis "( )" son obligatorios y los parámetros que aparecen entre corchetes angulares "[ ]" son opcionales.

Parámetro	Description
-s servidor	Nombre del servidor del controlador del dominio de Active Directory.
-p	Muestra los permisos actuales en el contenedor.
-r	Elimina los permisos de acceso para el nombre de cuenta especificado.
- a nombre_cuenta	Cuenta que obtendrá acceso al contenedor. El permiso de acceso se eliminará si se ha especificado con la opción -r.

Restablecimiento de un dispositivo de autenticación

Utilice la llave especial para restablecer los ajustes prefijados del dispositivo de autenticación. Esta llave se proporciona con el dispositivo y debe almacenarse en un lugar seguro.

1. Asegúrese de que el dispositivo de autenticación esté encendido.
2. Inserte la llave especial en la ranura de la llave.
3. Gire la llave un cuarto de vuelta hacia usted.
4. Vuelva a girar la llave a su posición original.
5. Extraiga la llave.

   Nota: el dispositivo emitirá un sonido cada 10 segundos si la llave no se gira a la posición original antes de extraerla.

Asignaciones de puerto

Secure Access se comunica en los puertos siguientes

Componente	Puerto
CAS	TCP 2910
DRE	TCP 2938
DCE	TCP 1824, TCP 2939, UDP 2613
Dispositivo de autenticación de Secure Access	TCP 1234

Al instalar Secure Access, estos puertos se abren de manera automática. Sin embargo, si tiene que modificar los ajustes del servidor de seguridad de Windows, puede añadir los puertos a la lista de confianza de cada máquina donde haya instalado algún componente del servidor de Secure Access.

Solución de problemas

Antes de solicitar ayuda, compruebe los síntomas e instrucciones relativos a la solución de problemas siguientes a la hora de corregir el problema.

	Síntoma	Instrucción
1	¿Está apagado el indicador del lector?	**Dispositivo de autenticación**: si el indicador del lector de tarjetas está apagado, significa que el lector no está encendido. Dispositivo de autenticación: compruebe que el cable del lector está conectado y que el conector está correctamente acoplado en el conector pequeño DIN de la unidad de control. Si el cable está colocado correctamente y sigue sin encenderse el indicador, prosiga con el paso siguiente. **Lector USB**: compruebe que tiene la versión de software adecuada instalada en el dispositivo multifunción. Asegúrese de que el lector esté correctamente enchufado a la impresora. Si el LED sigue apagado una vez comprobada la conexión y después de apagar y volver a encender la impresora, deberá intentarlo con otro lector.
2	¿Está conectada la unidad de control?	**Dispositivo de autenticación**: compruebe la parte posterior (lado del conector) de la unidad de control. Si hay suministro eléctrico, se iluminará el indicador amarillo situado junto a la toma identificada como "Ethernet". Compruebe que el cable del suministro eléctrico está bien acoplado y que el cable de alimentación está conectado a la toma de la fuente de alimentación y al enchufe de pared. Verifique que la toma de la pared tiene alimentación eléctrica.
3	¿El indicador del lector se ha puesto rojo y parpadea lentamente?	**Dispositivo de autenticación**: si el indicador del lector parpadea lentamente, significa que el lector está conectado correctamente a la unidad de control, pero esta no ha podido conectarse al servidor. Compruebe que el cable Ethernet esté conectado a la toma de la unidad de control identificada como "Ethernet" y a la toma Ethernet de la pared. **Lector USB**: el módulo lector del dispositivo multifunción no se puede comunicar con el servidor. Compruebe si hay conectividad de red con el dispositivo multifunción y que el dispositivo se inicializó correctamente en Secure Access Manager.
4	¿Está apagada la luz del enlace Ethernet?	**Dispositivo de autenticación**: si el indicador verde situado junto a la toma identificada como "Ethernet" está apagado, significa que no hay conexión Ethernet. Para asegurarse de que el cable de conexión Ethernet está en buen estado, compárelo con otro cable y verifique que la toma de la pared de Ethernet está activa.

	Síntoma	Instrucción
5	¿?Es verde y fija la luz del enlace Ethernet?	**Dispositivo de autenticación**: si el indicador verde situado junto a la toma identificada como "Ethernet" está fijo, significa que hay conexión Ethernet pero no hay actividad. Compruebe que la toma de la pared de Ethernet está conectada al concentrador o conmutador adecuado.
6	¿Aparece el dispositivo en la lista del servidor Secure Access?	**Dispositivo de autenticación**: compruebe la lista desplegable de dispositivos de autenticación en la consola de Secure Access y verifique que contiene la dirección MAC del dispositivo con problemas. Si la dirección MAC del dispositivo (tal como se encuentra en la etiqueta de número de serie de la unidad de control) no aparece en la lista, significa que no ha podido establecer contacto con el servidor. **Lector USB**: no aparece ningún dispositivo de autenticación en la lista si se utiliza un lector USB.
7	¿Ha recibido el dispositivo una dirección IP?	**Dispositivo de autenticación**: si utiliza DHCP para configurar los dispositivos, compruebe el servidor DHCP para verificar que se le ha asignado una dirección IP. Utilice la dirección MAC para llevar a cabo la verificación. Si no se ha asignado ninguna dirección IP, será porque el dispositivo no se puede comunicar con el servidor DHCP o porque se ha configurado mediante la configuración IP manual.
8	¿Ha recibido el dispositivo una dirección de servidor del DHCP?	**Dispositivo de autenticación**: si ha utilizado DHCP para configurar los dispositivos, compruebe que el servidor DHCP especifique el valor 230 para la dirección IP del servidor. Verifique que el valor es la dirección IP correcta del servidor. Tenga en cuenta que el servidor Secure Access no debe configurarse mediante DHCP. Si no se especificó el valor 230 o se especificó incorrectamente, el dispositivo no podrá establecer contacto con el servidor.
9	¿Se ha especificado la dirección IP de forma manual?	**Dispositivo de autenticación**: si la dirección IP se especificó de forma manual, compruebe los registros para determinar la dirección IP del dispositivo y conéctese al dispositivo mediante un navegador web. Si no puede conectarse a la página web en la dirección IP del dispositivo, se deberá a uno de los motivos siguientes: el dispositivo no se ha conectado correctamente, el dispositivo no puede comunicarse o la dirección IP se ha registrado de forma incorrecta. Para eliminar la primera posibilidad, conecte el dispositivo directamente al PC mediante un cable cruzado e intente realizar la conexión de nuevo. Una vez que haya establecido la conexión, verifique que los ajustes de red y la dirección IP del servidor son correctos.

	Síntoma	Instrucción
10	¿Es imposible acceder al dispositivo mediante su dirección IP?	**Dispositivo de autenticación**: si no consigue conectarse al dispositivo con su dirección IP mediante un cable Ethernet conectado al puerto Downlink, restablezca las opciones prefijadas de fábrica del dispositivo. Para ello, desconecte la alimentación de la unidad de control, inserte la llave y gírela hacia la posición de encendido. A continuación, vuelva a conectar la alimentación. Después de 30 segundos, desconecte la alimentación, extraiga la llave y vuelva a conectar la alimentación. Ahora debería poder conectarse con la dirección IP 192.168.2.1. Compruebe que los parámetros de red de su PC son los correctos para poder llegar a dicha dirección. Si ahora puede acceder a la página web del dispositivo, podrá configurar la información de red de forma manual o intentar la configuración DHCP volviendo a conectar el dispositivo a la red. Si sigue sin poder acceder a la página web, es posible que la unidad de control esté defectuosa.
11	¿Se ha puesto rojo el indicador del lector y parpadea rápidamente al pasar la tarjeta?	Si el indicador del lector se pone rojo y parpadea rápidamente, indica que se ha pasado la tarjeta incorrectamente por el lector. El servidor Secure Access ha determinado que el ID de tarjeta no coincide con un usuario válido de la red. Verifique el lector con una tarjeta de usuario que funcione en otros lectores. Si las tarjetas no se leen correctamente en ningún lector, es posible que se deba a la configuración del servidor. Póngase en contacto con el centro de asistencia técnica para verificar la configuración del servidor.
12	¿Se ha puesto rojo el indicador del lector y permanece fijo al pasar la tarjeta?	Si la luz del indicador no cambia al pasar la tarjeta, indica que no la ha detectado. Es posible que la tarjeta magnética se haya codificado con un estándar diferente o que se haya pasado al revés o en la dirección incorrecta. O puede que la tarjeta de proximidad o la tarjeta inteligente sin contacto no se haya colocado lo suficientemente cerca del lector o que sea del tipo incorrecto. Verifique que se ha pasado correctamente la tarjeta. Si la misma tarjeta funciona en otros lectores del mismo sitio, es posible que falle el módulo lector. Si la tarjeta no funciona en otros lectores, verifique la tecnología de la tarjeta con el proveedor de la tarjeta y compárela con la lista de compatibilidad de la tarjeta del lector.
13	¿Se pone verde la luz del indicador del lector al pasar la tarjeta?	Si el indicador se pone rojo, significa que la sesión de Secure Access está activa. Esto quiere decir que la tarjeta se leyó correctamente y coincide con un usuario de Secure Access válido. Si la luz cambia a verde, pero el dispositivo multifunción sigue desactivado, es posible que el dispositivo de Secure Access se haya asociado con un dispositivo multifunción incorrecto. Compruebe la configuración del dispositivo en la consola de Secure Access para verificar que el dispositivo de Secure Access está asociado con el dispositivo multifunción adecuado.

	Síntoma	Instrucción
14	¿Está el panel frontal del dispositivo multifunción desbloqueado siempre?	El panel frontal del dispositivo multifunción solo puede bloquearse en dispositivos que admiten Xerox Secure Access. Verifique que el modelo que intenta utilizar es compatible y que tiene la versión correcta de firmware instalada.
15	¿Qué significan los mensajes de error: "Failed to enable Follow-You printing" (Error al activar la impresión Follow-You) y "Failed to enable Follow-You printing: no site specified" (Error al activar la impresión Follow-You: no se especificó ningún sitio)?	Estos mensajes pueden aparecer si no se instala correctamente el servicio personalizado Release My Documents. Consulte Solución de problemas de instalación del servicio personalizado Release My Documents en la página 52.
16	Los mensajes del dispositivo (Título/Inicio de sesión) no se muestran en el panel frontal del dispositivo multifunción.	Abra el dispositivo en Secure Access Manager. Haga clic en el botón **Initialize Secure Access device** (Inicializar el dispositivo de Secure Access). Ahora deberían aparecer los mensajes en el panel frontal.
17	¿El indicador del lector se pone verde fijo después de reiniciar la impresora?	**Lector de tarjetas USB**: compruebe que tiene la versión de software adecuada instalada en el dispositivo multifunción.

Solución de problemas de instalación del servicio personalizado Release My Documents

Si en la pantalla Servicios personalizados del dispositivo multifunción no aparece el botón "Release my documents", es posible que necesite ejecutar la instalación con parámetros específicos. Si su DNS no permite que la impresora determine el nombre de host del servidor que ejecuta el DCE, la herramienta no es capaz de registrar los dispositivos correctamente. Consulte la tabla que se presenta a continuación para ver los parámetros que debe ejecutar en su lugar.

El ejecutable de Release My Documents se encuentra en la carpeta Tools de la máquina que alberga el Core Authentication Server. Asegúrese de que tiene permisos de administrador en el servidor que alberga el servicio CAS y DCE para poder instalar los archivos necesarios.

1. Abra una línea de comandos y escriba la ruta a la carpeta Tools. Por ejemplo:
   c:\Archivos de programa\Xerox\SecureAccess\Tools\
2. Ejecute el archivo con los parámetros que se detallan en la tabla siguiente:
   saxeroxeipregistration.exe

   Nota: puede ejecutar el comando con los parámetros siguientes para sobrescribir la instalación que ha fallado; no es necesario que primero elimine el registro de la extensión.

Parámetro	Resultado
-i	Identifica la dirección IP de la impresora que recibirá la extensión de Release My Documents.
-r	Registra el servidor DCE especificado en el dispositivo multifunción especificado.
-d	Elimina el registro de la extensión de Release My Documents del dispositivo multifunción correspondiente.
-v	Permite ver la información registrada. Ejecute este comando para confirmar la instalación de la extensión.
-u	Nombre de usuario para la autorización de actualización del dispositivo.
-p	Clave de usuario para la autorización de actualización del dispositivo.
-c	Enumera los dispositivos del servidor CAS especificado y registra la extensión en todas los dispositivos multifunción de Xerox que aparecen en la lista de dispositivos.
/?	Permite ver una lista de los parámetros para esta extensión.

Ejemplo:

```
saxeroxeipregistration.exe -i 192.168.97.180 -r 192.168.97.137
```

Dirección IP de la impresora **Dirección IP del DCE**

Resultado: registra la actualización con el servidor DCE especificado e instala la extensión de Release My Documents en un solo dispositivo multifunción.

Acceso a la pantalla Release My Documents

Si ha instalado la extensión Release My Documents (consulte la Guía de instalación para obtener las instrucciones), los usuarios pueden acceder a la pantalla correspondiente para ver sus trabajos de impresión de una o varias colas seguras, y liberar o borrar los trabajos si lo desean.

1. Después de autenticarse, pulse **All Services** (Todos los servicios).
2. Pulse **Custom Services** (Servicios personalizados).
3. Pulse **Release My Documents** (Liberar mis documentos).
4. Todos los documentos que tiene el usuario en el servidor de impresión local se muestran en esta pantalla. En la tabla siguiente, se describe cada botón.

Botón	Función
Print (Imprimir)	Toque uno o varios documentos de la lista y pulse **Print** para imprimirlos y eliminarlos de la lista. Si se especifica más de una copia, haga clic en **OK** para confirmar la solicitud.
Print & Save (Imprimir y guardar)	Toque uno o varios documentos de la lista y pulse **Print & Save** para imprimirlos y guardarlos en la lista. Si se especifica más de una copia, haga clic en **OK** para confirmar la solicitud.
Delete (Eliminar)	Toque uno o varios documentos de la lista y pulse **Delete** para borrarlos de la lista sin imprimirlos.
Select All (Seleccionar todo)	Selecciona todos los trabajos de la lista.
Refresh (Actualizar)	Conecta con el servidor DCE para determinar si se debe añadir algún trabajo pendiente a la lista del usuario actual. Si se encuentra algún documento, se añade al final de la lista.
Details (Detalles)	Toque un documento de la lista y pulse **Details** para ver detalles, como, por ejemplo, el nombre del trabajo, la fecha y la hora de envío, el nombre de la impresora a la que se envió originalmente el trabajo y el PC cliente desde donde se originó.
Exit (Salir)	Vuelve a la pantalla Servicios personalizados.

Definición del número de copias para un trabajo de impresión

Después de autenticarse, los usuarios pueden utilizar el teclado numérico del dispositivo multifunción para especificar el número de copias que desean realizar. Si el número es superior a 1, cuando pulse los botones **Print** (Imprimir) o **Print & Save** (Imprimir y guardar), aparecerá un cuadro de diálogo de confirmación. Para imprimir el número de copias indicado, pulse **OK**; para cambiarlo, pulse **Cancel** (Cancelar) y vuelva a escribir la cantidad correspondiente con el teclado numérico del panel frontal del dispositivo multifunción. Pulse **Print** (Imprimir) o **Print & Save** (Imprimir y guardar) para volver a liberar el trabajo.

Si se realizaron 2 copias del documento original, al utilizar esta función y seleccionar 2, se generarán 4 copias del documento original.

Finalización de una sesión de usuario

Para volver a la pantalla Custom Services (Servicios personalizados) desde la pantalla Release My Documents, pulse **Exit** (Salir) primero. Para volver a la pantalla principal del panel frontal, pulse **Close** (Cerrar). Y para cerrar la sesión, pulse dos veces el botón **Clear All** (Borrar todo), situado junto al teclado del panel, y luego seleccione **Log out** (Cerrar sesión) en el cuadro de diálogo de confirmación.