



Lexmark™

Autenticación por tarjeta

Guía del administrador

Contenido

- Descripción general..... 4**
- Requisitos de configuración previos..... 5**
 - Acceso a Embedded Web Server..... 5
 - Añadición de una cuenta de usuario interno..... 5
 - Configuración de grupos para cuentas de usuarios internos..... 5
 - Creación de una plantilla de seguridad..... 6
 - Configuración de los controles de acceso..... 6
- Configuración de la aplicación..... 8**
 - Acceso a la página de configuración de la aplicación..... 8
 - Configuración de la autenticación de administrador..... 8
 - Configuración de la pantalla de inicio de sesión..... 9
 - Autenticación basada en impresora..... 9
 - autenticación mediante el servicio web..... 11
 - Autenticación mediante el servicio de identidad..... 12
 - Autenticación con PIN..... 13
 - Autenticación LDAP..... 14
 - Configuración de preferencias de aplicación..... 15
 - Mostrar dominios de las cuentas de usuario..... 16
 - Exportación o importación de archivos de configuración..... 16
- Administración de la aplicación..... 17**
 - Acceso a la página de estado de la aplicación..... 17
 - Administración de cuentas de usuario e impresoras del cliente..... 17
 - Reasignación de funciones de impresora..... 18
- Uso de la aplicación..... 20**
 - Registro de usuarios..... 20
 - Registro de un PIN..... 20
 - Inicio de sesión manual en la impresora..... 20
- Solución de problemas..... 21**

Preguntas más frecuentes.....	25
Avisos.....	27
Índice.....	28

Descripción general

Utilice la aplicación para proteger el acceso a la impresora con un lector de tarjetas. Cuando los usuarios se identifican, sus credenciales se autentican con una de las siguientes opciones:

- Una impresora principal. Si la impresora principal está desconectada, la de seguridad asume su función hasta que la principal vuelva a estar conectada.
Nota: A la hora de configurar las impresoras, asegúrese de que se encuentran en la misma red.
- Servidores Lightweight Directory Access Protocol (LDAP) Lexmark™ Document Distributor (LDD) o proveedores de servicios de identificación en función del tipo de autenticación definida por la organización.

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

Requisitos de configuración previos

Es posible que necesite derechos de administrador para configurar la aplicación.

Acceso a Embedded Web Server

- 1 Obtenga la dirección IP de la impresora. Realice una de las siguientes acciones:
 - Localice la dirección IP de la impresora en la pantalla de inicio de la impresora.
 - Vea la dirección IP en la sección TCP/IP del menú Red/Puertos.
- 2 Abra un explorador web e introduzca la dirección IP de la impresora.

Adición de una cuenta de usuario interno

Una cuenta de usuario interno es necesaria al utilizar la autenticación basada en impresora.

- 1 En el servidor Web incorporado, haga clic en **Valores** o **Configuración**.
- 2 En función del modelo de impresora, realice una de las siguientes acciones:
 - Haga clic en **Seguridad > Configuración de seguridad > Cuentas internas > Agregar cuenta interna**.
 - Haga clic en **Seguridad > Editar configuraciones de seguridad > Cuentas internas > Agregar cuenta interna**.
- 3 Introduzca la información de cuenta y, a continuación, haga clic en **Enviar**.
- 4 Si es necesario, en la sección Gestionar cuentas internas, escriba un nombre de bloque de seguridad y, a continuación, especifique las credenciales de usuario necesarias.
- 5 Haga clic en **Enviar**.

Configuración de grupos para cuentas de usuarios internos

- 1 En el servidor Web incorporado, haga clic en **Valores** o **Configuración**.
- 2 En función del modelo de impresora, realice una de las siguientes acciones:
 - Haga clic en **Seguridad > Configuración de seguridad > Cuentas internas > Configuración de grupos para su uso con cuentas internas**.
 - Haga clic en **Seguridad > Editar configuraciones de seguridad > Cuentas internas > Configuración de grupos para su uso con cuentas internas**.
- 3 Introduzca un nombre de grupo y, a continuación, haga clic en **Agregar**.
- 4 Añada cuentas internas al grupo.
- 5 Haga clic en **Enviar**.

Creación de una plantilla de seguridad

Una plantilla de seguridad se compone de bloques de seguridad, como Cuentas internas, Kerberos, LDAP, LDAP+GSSAPI o Active Directory. Estas plantillas se aplican al control de acceso a funciones y aplicaciones de impresora.

- 1 En Embedded Web Server, haga clic en **Valores** o **Configuración**.
- 2 En función del modelo de impresora, realice una de las siguientes acciones:
 - Haga clic en **Seguridad > Configuración de seguridad > Plantilla de seguridad > Agregar plantilla de seguridad**.
 - Haga clic en **Seguridad > Editar configuraciones de seguridad > Plantillas de seguridad > Agregar plantilla de seguridad**.
- 3 Escriba un nombre de plantilla de seguridad y, a continuación, seleccione una de las siguientes configuraciones de autenticación:
 - Para la autenticación basada en impresora dentro de una configuración independiente, seleccione un bloque de cuenta interna.
 - Para la autenticación basada en impresora mediante Lexmark Print Management (LPM) Serverless Print Release en una configuración de Active Directory, seleccione un bloque de LDAP+GSSAPI.
 - Para la autenticación LDAP, seleccione un bloque de LDAP.
- 4 Haga clic en **Guardar plantilla**.

Nota: Para modificar una plantilla de seguridad existente, seleccione la plantilla de seguridad y, a continuación, añada o modifique una autorización para la plantilla.

Configuración de los controles de acceso

Nota: Al utilizar la función **Inicio de sesión del administrador**, asegúrese de haber configurado la plantilla de seguridad para las cuentas internas. Para obtener más información, consulte [“Creación de una plantilla de seguridad” en la página 6](#).

- 1 En Embedded Web Server, haga clic en **Valores** o **Configuración**.
- 2 En función del modelo de impresora, realice una de las siguientes acciones:
 - Haga clic en **Seguridad > Configuración de seguridad > Controles de acceso**.
 - Haga clic en **Seguridad > Editar configuraciones de seguridad > Controles de acceso**.
- 3 Haga clic en **Aplicaciones del dispositivo** o **Soluciones de dispositivo** y, a continuación, haga lo siguiente:
 - Establezca Aplicación 1 o Solución 1 en una cuenta interna o plantilla de seguridad de Active Directory o LDAP+GSSAPI.
 - Configure Aplicación 2 o Solución 2 en la plantilla de seguridad de la aplicación.

Nota: La plantilla de seguridad de la aplicación es la plantilla con CardAuth como configuración de autenticación. Para obtener más información, consulte [“Creación de una plantilla de seguridad” en la página 6](#).
 - Establezca Aplicación 3 o Solución 3 en una plantilla de seguridad de LDAP.

Notas:

- Si instala LPM Print Release, configure el control de acceso de Print Release en la plantilla de seguridad de la aplicación.

- Las impresoras de Embedded Solutions Framework (eSF) versión 2.x requieren el uso de la aplicación eSF Security Manager para configurar el control de acceso. Si desea acceder a una lista de dichas impresoras, consulte el archivo *Léame*.

4 Haga clic en **Enviar**.

Configuración de la aplicación

Antes de empezar, realice las siguientes acciones:

- Desactive Pantalla inactiva y fondo y cualquier otra aplicación de autenticación existente.
- Instale lo siguiente:
 - Instalador de autenticación de tarjetas
 - Controlador de lector de tarjetas
 - Lector de tarjetas
 - Gestor de seguridad eSF

Nota: Las impresoras de eSF versión 2.x requieren el uso de la aplicación eSF Security Manager para configurar el control de acceso. Si desea acceder a una lista de dichas impresoras, consulte el archivo *Léame*.

Acceso a la página de configuración de la aplicación

- 1 En el servidor Web incorporado, haga clic en **Valores** o **Configuración**.
- 2 En función del modelo de impresora, realice una de las siguientes acciones:
 - Haga clic en **Aplicaciones** > **Administración de aplicaciones**.
 - Haga clic en **Soluciones de dispositivo** > **Soluciones (eSF)**.
 - Haga clic en **Embedded Solutions**.
- 3 Haga clic en **Autenticación de tarjetas** > **Configurar**.

Configuración de la autenticación de administrador

Nota: Al utilizar la función **Inicio de sesión del administrador**, asegúrese de haber configurado la plantilla de seguridad para Cuentas internas, PIN o Contraseña. Para obtener más información, consulte [“Creación de una plantilla de seguridad” en la página 6](#).

- 1 Desde Embedded Web Server, acceda a la página de configuración de la aplicación.
- 2 En la sección Autenticación de usuario, establezca **Control de acceso de inicio de sesión del administrador** en su método de inicio de sesión preferido.

Notas:

- Asegúrese de que el control de acceso seleccionado esté configurado con una plantilla de seguridad. Para obtener más información, consulte [“Creación de una plantilla de seguridad” en la página 6](#).
- Si selecciona **Desactivado**, se ocultará la opción **Inicio de sesión del administrador** en el panel de la impresora.

- 3 Haga clic en **Aplicar**.

Configuración de la pantalla de inicio de sesión

La pantalla de inicio de sesión se puede configurar para lo siguiente:

- Permite a los usuarios utilizar las funciones de copia y fax sin necesidad de iniciar sesión.
- Permite a los usuarios seleccionar el método de inicio de sesión que deseen utilizar.
- Agregar un fondo a la pantalla de inicio de sesión y personalizar el mensaje de inicio de sesión.
- Desactive la advertencia si no hay un lector de tarjetas conectado.

1 Desde Embedded Web Server, acceda a la página de configuración de la aplicación.

2 En la sección Pantalla de inicio de sesión, ajuste los valores.

Nota: Para obtener más información acerca de cada valor, pase el ratón sobre cada uno de ellos para consultar los mensajes de ayuda.

3 Haga clic en **Aplicar**.

Activación de las funciones de copia y fax sin iniciar sesión

Si las opciones "Permitir copia sin iniciar sesión" o "Permitir fax sin iniciar sesión" están activadas, haga lo siguiente:

1 En Embedded Web Server, haga clic en **Valores** o **Configuración**.

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

- Haga clic en **Seguridad** > **Configuración de seguridad** > **Controles de acceso** > **Acceso a función**.
- Haga clic en **Seguridad** > **Editar configuraciones de seguridad** > **Controles de acceso**.

3 Establezca las funciones de copia o fax en **Sin seguridad**.

4 Haga clic en **Enviar**.

Autenticación basada en impresora

Utilice la autenticación basada en impresora al validar usuarios a través de una impresora principal.

Configuración de la autenticación de usuario basada en impresora

Antes de empezar, asegúrese de que:

- Los controles de acceso Aplicación 1 o Solución 1 se establecen en una cuenta interna, LDAP+GSSAPI o una plantilla de seguridad de Active Directory.
- Los controles de acceso Aplicación 2 o Solución 2 se configuran en la plantilla de seguridad de la aplicación.

Nota: Para obtener más información, consulte [“Configuración de los controles de acceso” en la página 6](#).

1 Desde Embedded Web Server, acceda a la página de configuración para la aplicación.

2 Desde la sección Pantalla de inicio de sesión, establezca Método de inicio de sesión en **con tarjeta o manual**.

3 En la sección Autenticación de usuario, realice una de las siguientes acciones:

- Establezca Validación de tarjetas en **Basada en impresora**.
- Establezca Control de acceso al registro de tarjetas en **Aplicación 1** o en **Solución 1**.

- Establezca Control de acceso de inicio de sesión manual en **Aplicación 1** o en **Solución 1**.
- Establezca Control de acceso a sesión en **Aplicación 2** o en **Solución 2**.

Notas:

- Si Control de acceso a registro de tarjetas se ha establecido en **Ninguno**, no podrá registrar su tarjeta en la impresora.
- Establecer Control de acceso de inicio de sesión manual en **Ninguno** solo requiere una tarjeta para iniciar una sesión incluso si Método de inicio de sesión se ha establecido como **manual o con tarjeta**.
- Para obtener más información acerca de cada valor, pase el ratón sobre cada uno de ellos para consultar los mensajes de ayuda.

4 Haga clic en **Aplicar**.

Configuración de la función de la impresora

Nota: Una impresora cliente requiere una impresora principal y otra de seguridad.

- 1** Desde Embedded Web Server, acceda a la página de configuración para la aplicación.
- 2** En la sección Validación de tarjetas basada en la impresora, seleccione una función para la impresora.
 - **Principal:** la impresora almacena la lista de los usuarios registrados.
 - **De seguridad:** si la impresora principal está desconectada, la de seguridad asume su función hasta que la principal vuelva a estar conectada.
 - **Cliente:** la impresora no almacena información del usuario. Se requiere una impresora principal o de seguridad para validar las credenciales de usuario.

Notas:

- Si tiene una impresora, establézcala como la principal.
- Si tiene dos impresoras, establezca una como la principal y otra como la de seguridad.
- Si tiene tres impresoras o más, establezca una como la principal, otra como la de seguridad y las demás como impresoras cliente.

- 3** Introduzca los nombres de host o las direcciones IP de la impresora principal y de la de seguridad.

Notas:

- Para configurar una impresora de seguridad, se requiere el nombre de host o la dirección IP de la impresora principal.
- Para configurar impresoras cliente, se requieren nombres de host o direcciones IP de las impresoras principal y de seguridad.
- Antes de asignar una impresora cliente a una nueva impresora principal, elimínela de la antigua impresora principal.

4 Haga clic en **Aplicar**.

autenticación mediante el servicio web

Utilice la autenticación en servidor web al validar usuarios a través de un servidor LDD.

Configuración de la autenticación de usuario mediante el servicio web

Antes de empezar, compruebe que los controles de acceso Aplicación 2 o Solución 2 se hayan configurado en la plantilla de seguridad de la aplicación. Para obtener más información, consulte [“Configuración de los controles de acceso” en la página 6](#).

- 1 Desde Embedded Web Server, acceda a la página de configuración de la aplicación.
- 2 Desde la sección Pantalla de inicio de sesión, establezca Método de inicio de sesión en **Inicio de sesión manual o con tarjeta**.
- 3 En la sección Autenticación de usuario, realice una de las siguientes acciones:
 - Establezca Validación de tarjetas en **Servicio web**.
 - Establezca Control de acceso a registro de tarjetas y Control de acceso de inicio de sesión manual en su control de acceso preferido.
 - Establezca Control de acceso a sesión en **Aplicación 2** o en **Solución 2**.

Notas:

- Si Control de acceso a registro de tarjetas se ha establecido en **Ninguno**, no podrá registrar su tarjeta en la impresora.
 - Establecer Control de acceso de inicio de sesión manual en **Ninguno** solo requiere una tarjeta para iniciar una sesión incluso si Método de inicio de sesión se ha establecido como **Inicio de sesión manual o con tarjeta**.
 - Para obtener más información acerca de cada valor, pase el ratón sobre cada uno de ellos para consultar los mensajes de ayuda.
- 4 Seleccione **Verificar certificado** para validar todas las conexiones al servidor. Si Verificar certificado no está seleccionado, no se validará la CA.

Nota: La configuración de Verificar certificado solo se aplica a la validación del servicio de identidad y del servicio web.

- 5 En el menú Modo de verificación, seleccione **cadena** o **igual**.

Nota: El valor predeterminado es cadena.

- 6 Cargue el certificado SSL del servidor para conectarse de forma segura al servidor.

- 7 En el campo Comprobacióndehosts, escriba los nombres de host adicionales (que no sean la URL del servidor predeterminado) para verificar las entradas en el certificado. Utilice comas para separar varios nombres de host.

Nota: De forma predeterminada, esa lista blanca solo contiene la URL del servidor. Escriba los nombres de host adicionales en el campo Comprobacióndehosts para incluirlos en la lista blanca.

- 8 Haga clic en **Aplicar**.

Configuración de los valores del servicio web

- 1 Desde Embedded Web Server, acceda a la página de configuración para la aplicación.
- 2 En la sección Valores del servicio web, ajuste los valores.

Nota: Para obtener más información acerca de cada valor, pase el ratón sobre cada uno de ellos para consultar los mensajes de ayuda.

- 3 Haga clic en **Aplicar**.

Autenticación mediante el servicio de identidad

Utilice la autenticación mediante el servicio identidad al validar usuarios a través de un servidor de identidad servidor de servicio, como el servidor LPM Software as a Service (SaaS).

Configuración de la autenticación de usuario mediante el servicio de identidad

Antes de empezar, compruebe que los controles de acceso Aplicación 2 o Solución 2 se hayan configurado en la plantilla de seguridad de la aplicación. Para obtener más información, consulte [“Configuración de los controles de acceso” en la página 6](#).

- 1 Desde Embedded Web Server, acceda a la página de configuración de la aplicación.
- 2 Desde la sección Pantalla de inicio de sesión, establezca Método de inicio de sesión en **Inicio de sesión manual o con tarjeta**.
- 3 En la sección Autenticación de usuario, realice una de las siguientes acciones:
 - Establezca Validación de tarjetas en **Servicio de identidad**.
 - Establezca Control de acceso a registro de tarjetas en **Servicio de identidad**.
 - Establezca Control de acceso de inicio de sesión manual en **Servicio de identidad**.
 - Establezca Control de acceso a sesión en **Aplicación 2** o en **Solución 2**.

Notas:

- Si Control de acceso a registro de tarjetas se ha establecido en **Ninguno**, no podrá registrar su tarjeta en la impresora.
 - Establecer Control de acceso de inicio de sesión manual en **Ninguno** solo requiere una tarjeta para iniciar una sesión incluso si Método de inicio de sesión se ha establecido como **Inicio de sesión manual o con tarjeta**.
 - Para obtener más información acerca de cada valor, pase el ratón sobre cada uno de ellos para consultar los mensajes de ayuda.
- 4 Seleccione **Verificar certificado** para validar todas las conexiones al servidor. Si Verificar certificado no está seleccionado, no se validará la CA.

Nota: La configuración de Verificar certificado solo se aplica a la validación del servicio de identidad y del servicio web.

- 5 En el menú Modo de verificación, seleccione **cadena** o **igual**.

Nota: El valor predeterminado es cadena.

- 6 Cargue el certificado SSL del servidor para conectarse de forma segura al servidor.
- 7 En el campo Comprobación de hosts, escriba los nombres de host adicionales (que no sean la URL del servidor predeterminado) para verificar las entradas en el certificado. Utilice comas para separar varios nombres de host.
Nota: De forma predeterminada, esa lista blanca solo contiene la URL del servidor. Escriba los nombres de host adicionales en el campo Comprobación de hosts para incluirlos en la lista blanca.
- 8 Haga clic en **Aplicar**.

Configuración de los ajustes del servicio de identidad

- 1 Desde Embedded Web Server, acceda a la página de configuración para la aplicación.
- 2 Si es necesario, en la sección Ajustes del servicio de identidad, seleccione **Activar pantalla inactiva**.
Nota: Las impresoras eSF versión 2.x requieren el uso de la aplicación eSF Security Manager al desactivar **Activar pantalla inactiva**. Si desea acceder a una lista de dichas impresoras, consulte el archivo *Léame*.
- 3 Introduzca la dirección IP o el nombre de host del proveedor de servicios de identidad.
- 4 Si es necesario, introduzca la dirección IP o el nombre de host del proveedor de servicios de identidad.
- 5 Cargue el certificado SSL del servidor para conectarse de forma segura al servidor.
- 6 Si tiene un ID de cliente y un Secreto de cliente del proveedor de servicios de identidad, introduzca los datos en los campos correspondientes.
- 7 Configure la política de acceso a aplicaciones.
 - **Continuar:** se sigue utilizando la impresora incluso si la conexión con el servidor del servicio de identidad falla.
 - **Fallar:** se vuelve a la pantalla de inicio de sesión incluso si la conexión con el servidor del servicio de identidad falla.
- 8 Para permitir a los usuarios iniciar sesión en la impresora mediante una cuenta de servicio independiente, seleccione **Utilizar cuenta de servicio** y, a continuación, introduzca las credenciales de la cuenta de servicio.
- 9 Haga clic en **Aplicar**.

Autenticación con PIN

Configuración de autenticación de usuario con PIN

Antes de empezar, compruebe que los controles de acceso Aplicación 2 o Solución 2 se hayan configurado en la plantilla de seguridad de la aplicación. Para obtener más información, consulte [“Configuración de los controles de acceso” en la página 6](#).

- 1 Desde Embedded Web Server, acceda a la página de configuración para la aplicación.
- 2 Desde la sección Pantalla de inicio de sesión, establezca Método de inicio de sesión en una opción compatible con la autenticación con PIN.

- 3 En la sección Autenticación de usuario, realice una de las siguientes acciones:
 - Establezca Validación de tarjetas en su método de autenticación preferido.
 - Establezca Control de acceso a registro de tarjetas en su control de acceso preferido.
 - Establezca Control de acceso a PIN en **Aplicación 1** o en **Solución 1**.
 - Establezca Control de acceso de inicio de sesión manual en su control de acceso preferido.
 - Establezca Control de acceso a sesión en **Aplicación 2** o en **Solución 2**.

Notas:

- Si Control de acceso a PIN se ha establecido en **Ninguno**, no podrá registrar su PIN en la impresora.
- Para obtener más información acerca de cada valor, pase el ratón sobre cada uno de ellos para consultar los mensajes de ayuda.

- 4 Haga clic en **Aplicar**.

Configuración de los valores de PIN

- 1 Desde Embedded Web Server, acceda a la página de configuración para la aplicación.
- 2 En la sección Valores de PIN, dentro del menú Credenciales obligatorias, seleccione un método de inicio de sesión.
 - ID de usuario y PIN: requiere un nombre de usuario y un PIN para la autenticación.
 - Solo PIN: requiere un PIN para la autenticación.
- 3 Escriba la dirección del servidor web y, a continuación, seleccione la longitud mínima de PIN.
- 4 Escriba los mensajes de error de PIN no válido.
- 5 Haga clic en **Aplicar**.

Autenticación LDAP

Utilice la autenticación LDAP al validar usuarios a través de un servidor LDAP.

Configuración de autenticación de usuario con LDAP

Antes de empezar, asegúrese de que:

- Los controles de acceso Aplicación 2 o Solución 2 se configuran en la plantilla de seguridad de la aplicación.
- Los controles de acceso Aplicación 3 o Solución 3 se configuran en una plantilla de seguridad de LDAP.

Nota: Para obtener más información, consulte [“Configuración de los controles de acceso” en la página 6](#).

- 1 Desde Embedded Web Server, acceda a la página de configuración para la aplicación.
- 2 Desde la sección Pantalla de inicio de sesión, establezca Método de inicio de sesión en **con tarjeta o manual**.
- 3 En la sección Autenticación de usuario, realice una de las siguientes acciones:
 - Establezca Validación de tarjetas en **LDAP**.
 - Establezca Control de acceso al registro de tarjetas en **Aplicación 3** o en **Solución 3**.

- Establezca Control de acceso de inicio de sesión manual en **Aplicación 3** o en **Solución 3**.
- Establezca Control de acceso a sesión en **Aplicación 2** o en **Solución 2**.

Notas:

- Si Control de acceso a registro de tarjetas se ha establecido en **Ninguno**, no podrá registrar su tarjeta en la impresora.
- Establecer Control de acceso de inicio de sesión manual en **Ninguno** solo requiere una tarjeta para iniciar una sesión incluso si Método de inicio de sesión se ha establecido como **manual o con tarjeta**.
- Para obtener más información acerca de cada valor, pase el ratón sobre cada uno de ellos para consultar los mensajes de ayuda.

4 Haga clic en **Aplicar**.

Configuración de los ajustes de LDAP

- 1** Desde Embedded Web Server, acceda a la página de configuración para la aplicación.
- 2** En la sección Configuración LDAP, ajuste los valores.

Notas:

- Si la opción **Utilizar libreta de direcciones** está seleccionada, la aplicación utiliza la configuración LDAP que ya esté configurada en las cuentas de red de la impresora.
- Para obtener más información acerca de cada valor, pase el ratón sobre cada uno de ellos para consultar los mensajes de ayuda.

3 Haga clic en **Aplicar**.

Configuración de preferencias de aplicación

- 1** Desde Embedded Web Server, acceda a la página de configuración para la aplicación.
- 2** Realice al menos una de las acciones siguientes:
 - Para personalizar la pantalla de inicio de la impresora, ajuste la configuración de la pantalla de inicio.
 - Para mostrar mensajes de registro, en la sección Valores avanzados, seleccione **Mostrar mensaje de introducción de registro** y **Mostrar mensaje de finalización de registro**.
 - Para escuchar un *pitido* tras iniciar sesión correctamente, en la sección Valores avanzados, seleccione **Activar pitido al iniciar sesión correctamente** y, a continuación, ajuste la frecuencia de pitido.
 - Para utilizar un perfil concreto al iniciar sesión correctamente, en la sección Valores avanzados, en el campo Perfil de inicio de sesión, escriba un nombre de perfil.

Nota: Para obtener más información acerca de cada valor, pase el ratón sobre cada uno de ellos para consultar los mensajes de ayuda.

3 Haga clic en **Aplicar**.

Ver perfiles disponibles

- 1** En el servidor Web incorporado, haga clic en **Valores** o **Configuración**.
- 2** Haga clic en **Administrar métodos abreviados** > **Administrar métodos abreviados de perfiles**.

Mostrar dominios de las cuentas de usuario

La función Usar dominio seleccionado solo se aplica cuando el método de inicio de sesión para el registro de tarjetas y el inicio de sesión manual es Kerberos, Active Directory o LDAP+GSSAPI. Esta función también se aplica únicamente si se ha configurado la validación de tarjeta como servicio web o basada en la impresora.

Si esta función está activada para el registro de tarjeta, el ID de distintivo que se registra se encuentra en el formato nombredeusuario@dominio.

Si esta función está activada para el inicio de sesión manual, el nombre de usuario que aparece en el panel de control de la impresora se encuentra en el formato nombredeusuario@dominio.

Estos parámetros no se aplican al inicio de sesión con PIN ni al registro de PIN.

Para activar esta función, haga lo siguiente:

- 1 Desde Embedded Web Server, acceda a la página de configuración para la aplicación.
- 2 En la sección Valores avanzados, seleccione **Usar dominio seleccionado**.
- 3 Haga clic en **Aplicar**.

Exportación o importación de archivos de configuración

- 1 Desde Embedded Web Server, acceda a la página de configuración para la aplicación.
- 2 Exporte o importe el archivo de configuración.

Notas:

- Si se produce un error **Sin memoria** de JVM, repita el proceso de exportación hasta que se guarde el archivo de configuración.
- Si se supera el tiempo de espera y aparece una pantalla en blanco, actualice el navegador web y, a continuación, haga clic en **Aplicar**.

Administración de la aplicación

Nota: La página de estado de la aplicación solo está disponible al utilizar la autenticación basada en impresora.

Acceso a la página de estado de la aplicación

Utilice la página de estado para controlar la actividad de la impresora.

- 1 En Embedded Web Server, haga clic en **Aplicaciones > Autenticación de tarjetas**.
- 2 Tenga en cuenta la siguiente información:
 - **Estado:** Muestra el estado de actividad de la impresora.
 - **No configurada:** no se ha configurado ninguna impresora.
 - **Fuera de línea:** La impresora no lleva a cabo ninguna actividad ni comunicación.
 - **En línea:** La impresora está activa.
 - **Tiempo de funcionamiento:** indica el tiempo que ha estado funcionando la aplicación.
 - **(esta impresora):** La impresora actual.
 - **Última actividad:** La última actividad de la impresora principal.
 - **Número de usuarios:** El número total de usuarios registrados.
 - **Estado de registro:** Indica si la impresora se encuentra fuera de línea o en línea.
 - **Última sincronización con impresora principal:** Indica la última vez que la impresora de seguridad se actualizó con la principal.
 - **Último contacto con impresora principal:** indica la última vez que la impresora de seguridad se comunicó con la principal.
 - **Última sincronización como impresora principal:** Indica la última vez que la impresora de seguridad funcionó como principal.
 - **Última actividad como impresora principal:** Indica la última actividad de la impresora de seguridad funcionando como impresora principal.
 - **Duración como impresora principal:** indica el tiempo durante el que la impresora de seguridad ha funcionado como principal.
 - **Actualmente atendido por:** La impresora cliente ha estado recientemente en contacto con la principal o con la de seguridad.
 - **Última actividad con impresora de seguridad:** Indica la última vez que la impresora cliente estuvo en contacto con la de seguridad.

Administración de cuentas de usuario e impresoras del cliente

Nota: Esta función solo aparece cuando una impresora funciona como principal.

- 1 Desde Embedded Web Server, acceda a la página de estado de la aplicación.
- 2 Haga lo siguiente:

Eliminación de cuentas de usuario

- a En la sección Principal, haga clic en **Eliminar usuarios**.
- b Escriba uno o más ID de usuario y, a continuación, elimínelos.

Añadir impresoras cliente

- a En la sección Clientes, haga clic en **Añadir clientes**.
- b Escriba una o más direcciones IP de impresoras y, a continuación, agréguelas.

Borrado de impresoras cliente

Nota: No puede eliminar impresoras del cliente cuando la impresora principal está desconectada o cuando se desinstala la aplicación.

- a En la sección Clientes, seleccione una o más impresoras.
- b Haga clic en **Borrar clientes**.

Reasignación de funciones de impresora

- 1 Configure una nueva impresora principal.
 - a Desde Embedded Web Server de la nueva impresora principal, acceda a la página de configuración de la aplicación.
 - b En la sección Validación de tarjetas basada en impresora, establezca Función en **Principal**.
 - c Introduzca la dirección IP o el nombre de host de la impresora de seguridad.
 - d Haga clic en **Aplicar**.
- 2 Asigne la impresora de seguridad a la nueva impresora principal.
 - a Desde Embedded Web Server de la nueva impresora principal, acceda a la página de configuración de la aplicación.
 - b En la sección Validación de tarjetas basada en la impresora, introduzca el nombre de host o la dirección IP de la nueva impresora principal.
 - c Haga clic en **Aplicar**.
- 3 Elimine la impresora cliente de la impresora principal actual.
 - a Desde Embedded Web Server de la impresora principal actual, acceda a la página de estado de la aplicación.
 - b En la sección Clientes, elimine la impresora cliente.
- 4 Vuelva a asignar la impresora cliente a la nueva impresora principal. Realice una de las siguientes acciones:

Uso de la página de configuración de la aplicación

- a Desde Embedded Web Server de la nueva impresora principal, acceda a la página de configuración de la aplicación.
- b En la sección Validación de tarjetas basada en impresora, establezca Función en **Cliente**.

- c** Introduzca la dirección IP o el nombre de host de la nueva impresora principal.

Nota: Compruebe que la dirección IP o el nombre de host de la impresora de seguridad son correctos.

- d** Haga clic en **Aplicar**.

Uso de la página de estado de la impresora principal

- a** Desde Embedded Web Server de la nueva impresora principal, acceda a la página de estado de la aplicación.
- b** En la sección Clientes, haga clic en **Añadir clientes**.
- c** Escriba la dirección IP de la impresora cliente y añádala.

Uso de la aplicación

Registro de usuarios

- 1 Acerque su tarjeta al lector de tarjetas.
- 2 Introduzca sus credenciales desde el panel de control de la impresora.

Nota: Si utiliza Kerberos, Active Directory o LDAP+GSSAPI para el registro de tarjetas, seleccione un dominio.

- 3 Siga las instrucciones que aparecen en pantalla.

Registro de un PIN

Antes de empezar, compruebe que el método de inicio de sesión se ha configurado para ser compatible con la autenticación con PIN.

- 1 En el panel de control de la impresora, toque **Inicio de sesión con PIN**.
- 2 Siga las instrucciones que aparecen en pantalla.

Inicio de sesión manual en la impresora

- 1 En el panel de control de la impresora, toque una de las siguientes opciones:
 - **Inicio sesión PIN**
 - **Inicio sesión man.**
 - **Inicio de sesión del administrador**

Nota: Al seleccionar **Inicio de sesión del administrador**, no podrá recuperar el resto de la información de usuario del servidor LDAP.

- 2 Introduzca sus credenciales de inicio de sesión.

Nota: Si utiliza Kerberos, Active Directory[®] o LDAP+GSSAPI para el inicio de sesión manual, seleccione un dominio.

- 3 Siga las instrucciones que aparecen en pantalla.

Solución de problemas

Error de la aplicación

Realice alguna de estas acciones:

Compruebe el registro del sistema

- 1 En el servidor Web incorporado, haga clic en **Valores** o **Configuración**.
- 2 En función del modelo de impresora, realice una de las siguientes acciones:
 - Haga clic en **Aplicaciones** > **Administración de aplicaciones**.
 - Haga clic en **Soluciones de dispositivo** > **Soluciones (eSF)**.
 - Haga clic en **Embedded Solutions**.
- 3 Haga clic en **Sistema** > **Registro**.
- 4 Seleccione y envíe los filtros apropiados.
- 5 Analice el registro y resuelva el problema.

Póngase en contacto con el representante de Lexmark

La aplicación no se ejecuta con la versión actualizada de SaaS Print Release

Realice alguna de estas acciones:

Asegúrese de que la activación de la impresión está configurada correctamente

Si ha actualizado su aplicación Print Management SaaS a Print Release v2.0 o posterior, asegúrese de desactivar Background and Idle Screen. Asigne el control de acceso a la autenticación de tarjetas a Print Release y asegúrese de que Print Release esté configurado correctamente. Para obtener más información, consulte la *Guía del administrador de activación de la impresión*.

Póngase en contacto con el representante de Lexmark

Error de autenticación

Realice alguna de estas acciones:

Aumento del tiempo de espera de la impresora

Si está utilizando el servicio de identidad como método de validación de la tarjeta, puede que la impresora necesite más tiempo para comunicar con el proveedor de servicios de identidad.

- 1 En el servidor Web incorporado, haga clic en **Valores** o **Configuración**.
- 2 Haga clic en **Valores generales > Tiempos de espera**.
- 3 Aumente el tiempo de espera de inactividad de la pantalla y el modo de suspensión.
- 4 Haga clic en **Enviar**.

Asegúrese de que la impresora esté conectada a la red

Para obtener más información, consulte la *Guía del usuario* de la impresora.

Asegúrese de que el servidor de seguridad esté en línea y no está ocupado

Póngase en contacto con el administrador del sistema para obtener más información.

El usuario está bloqueado.

Puede que el usuario haya alcanzado el número permitido de intentos fallidos de conexión.

Aumente el tiempo de bloqueo y el número permitido de intentos de conexión fallidos

- 1 En función del modelo de impresora, realice una de las siguientes acciones en Embedded Web Server:
 - Haga clic en **Valores > Seguridad > Otros valores de seguridad > Restricciones de conexión**.
 - Haga clic en **Configuración > Seguridad**.
- 2 Aumente el tiempo de bloqueo y el número permitido de intentos de conexión fallidos o la demora de cierre de sesión.
- 3 Haga clic en **Enviar**.

No se puede registrar una impresora cliente

Realice alguna de estas acciones:

Asegúrese de que la impresora principal o la de seguridad estén en línea.

Para obtener más información, consulte [“Acceso a la página de estado de la aplicación” en la página 17](#).

Asegúrese de que la impresora principal y la de seguridad estén configuradas correctamente

Para obtener más información, consulte [“Configuración de la autenticación de usuario basada en impresora” en la página 9.](#)

Asegúrese de no superar el máximo de 23 impresoras cliente registradas

Para obtener más información, consulte [“Administración de cuentas de usuario e impresoras del cliente” en la página 17.](#)

Póngase en contacto con el representante de Lexmark

No se puede validar la tarjeta

Realice alguna de estas acciones:

Establecimiento del método de inicio de sesión como manual o con tarjeta

- 1 Desde Embedded Web Server, acceda a la página de configuración para la aplicación.
- 2 Desde la sección Pantalla de inicio de sesión, establezca Método de inicio de sesión en **con tarjeta o manual**.
- 3 Haga clic en **Aplicar**.

Póngase en contacto con el representante de Lexmark

No se puede encontrar información del dominio

Realice alguna de estas acciones:

Algunos métodos de inicio de sesión para el inicio de sesión manual o el registro de tarjetas, como cuentas locales o LDAP, no requieren seleccionar un dominio. Los métodos de inicio de sesión que requieren una selección de dominio son Kerberos, Active Directory y LDAP+GSSAPI.

Desactivar la selección de dominio

- 1 Desde Embedded Web Server, acceda a la página de configuración para la aplicación.
- 2 En la sección Valores avanzados, desactive **Utilizar dominio seleccionado**.
- 3 Haga clic en **Aplicar**.

Cambio del método de inicio de sesión

- 1 Desde Embedded Web Server, acceda a la página de configuración para la aplicación.
- 2 En la sección Autenticación de usuario, establezca Control de acceso a registro de tarjetas y Control de acceso de inicio de sesión manual en **Aplicación 1** o **Solución 1**.

3 Haga clic en **Aplicar**.

Póngase en contacto con el representante de Lexmark

No se puede conectar al servidor LDAP

Realice alguna de estas acciones:

Asegúrese de que los valores de LDAP están configurados correctamente

Para obtener más información, consulte [“Configuración de los ajustes de LDAP” en la página 15](#).

Póngase en contacto con el representante de Lexmark

Preguntas más frecuentes

¿Por qué no puedo añadir o borrar una impresora cliente cuando una impresora de seguridad funciona como principal?

Solo puede hacerlo cuando la impresora principal se encuentra en línea.

¿Puedo eliminar una impresora cliente y asignarla a su nueva impresora principal incluso si la impresora principal actual está desconectada?

Sí, haciendo lo siguiente:

- 1 Desde Embedded Web Server en la impresora cliente, instale la aplicación.
- 2 Establézcala como impresora cliente y configúrela de acuerdo con las nuevas impresoras principal y de seguridad. Para obtener más información, consulte [“Configuración de la función de la impresora” en la página 10.](#)

¿Qué ocurre si desinstalo la aplicación de la impresora por error?

- 1 Desde Embedded Web Server, instale la aplicación.
- 2 Establezca la función de la impresora. Para obtener más información, consulte [“Configuración de la función de la impresora” en la página 10.](#)

Nota: Asegúrese de configurar primero la impresora principal, después la de seguridad y, por último, las impresoras cliente.

- 3 Configure la impresora de acuerdo con su función.

Notas:

- Si reinstala la aplicación en una impresora principal, asígnela a su impresora de seguridad.
- Si reinstala la aplicación en una impresora de seguridad, asígnela a su impresora principal.
- Si reinstala la aplicación en una impresora cliente, asígnela a las impresoras principal y de seguridad.
- Para obtener más información, consulte [“Reasignación de funciones de impresora” en la página 18.](#)

¿Por qué no veo los botones Copiar o Fax en la pantalla de bloqueo aunque tenga activadas ambas funciones sin iniciar sesión?

Establezca el control de acceso a las funciones Copiar o Fax en **Sin seguridad**. Para obtener más información, consulte [“Configuración de la pantalla de inicio de sesión” en la página 9](#).

¿Qué ocurre si cuento con los mismos controles de acceso para Control de acceso de inicio de sesión manual y Control de acceso a sesión?

Para acceder a las funciones de la impresora desde la pantalla de inicio, se le solicitará que introduzca sus credenciales al iniciar sesión de forma manual.

¿Puedo utilizar diferentes controles de acceso para Control de acceso de inicio de sesión manual y Validación de tarjetas?

Sí, excepto cuando esté utilizando una autenticación del servicio de identidad, en cuyo caso, establezca Control de acceso de inicio de sesión manual y Validación de tarjetas en **Servicio de identidad**.

¿Por qué no funciona la función Inicio de sesión del administrador con las cuentas de red?

La función **Inicio de sesión del administrador** solo se aplica a las plantillas de seguridad Cuentas internas, PIN y Contraseña.

Avisos

Nota sobre la edición

Diciembre de 2020

El párrafo siguiente no se aplica a los países en los que tales disposiciones son contrarias a la legislación local: LEXMARK INTERNATIONAL, INC, PROPORCIONA ESTA PUBLICACIÓN «TAL CUAL» SIN GARANTÍA DE NINGÚN TIPO, NI EXPLÍCITA NI IMPLÍCITA, LO QUE INCLUYE, PERO SIN LIMITARSE A ELLO, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD O IDONEIDAD PARA UN PROPÓSITO EN PARTICULAR. Algunos estados no permiten la renuncia a garantías explícitas ni implícitas en algunas transacciones; por lo tanto, es posible que la presente declaración no se aplique en su caso.

Esta publicación puede incluir inexactitudes técnicas o errores tipográficos. Periódicamente se realizan modificaciones en la presente información; dichas modificaciones se incluyen en ediciones posteriores. Las mejoras o modificaciones en los productos o programas descritos pueden efectuarse en cualquier momento.

Las referencias hechas en esta publicación a productos, programas o servicios no implican que el fabricante tenga la intención de ponerlos a la venta en todos los países en los que opere. Cualquier referencia a un producto, programa o servicio no indica o implica que sólo se pueda utilizar dicho producto, programa o servicio. Se puede utilizar cualquier producto, programa o servicio de funcionalidad equivalente que no infrinja los derechos de la propiedad intelectual. La evaluación y comprobación del funcionamiento junto con otros productos, programas o servicios, excepto aquellos designados expresamente por el fabricante, son responsabilidad del usuario.

Para obtener soporte técnico de Lexmark, visite <http://support.lexmark.com>.

Para obtener información sobre la política de privacidad de Lexmark que rige el uso de este producto, visite www.lexmark.com/privacy.

Para obtener información sobre los consumibles y descargas, visite www.lexmark.com.

© 2014 Lexmark International, Inc.

Reservados todos los derechos.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

Marcas comerciales

Lexmark y el logotipo de Lexmark son marcas comerciales o marcas registradas de Lexmark International, Inc. en EE.UU. y/o en otros países.

Las otras marcas comerciales pertenecen a sus respectivos propietarios.

Índice

A

- acceso
 - página de estado 17
- acceso a Embedded Web Server 5
- acceso a la página de configuración 8
- acceso, controles
 - configuración 6
- activación de un pitido tras iniciar sesión 15
- adición
 - impresoras cliente 17
 - usuarios 20
- adición de una cuenta de usuario interno 5
- archivo de configuración
 - exportar o importar 16
- asignación de la impresora de seguridad 18
- autenticación de administrador
 - configuración 8
- autenticación de usuario basada en impresora
 - configuración 9
- autenticación de usuario con LDAP
 - configuración 14
- autenticación de usuario con PIN
 - configuración 13
- autenticación de usuario mediante el servicio de identidad
 - configuración 12
- autenticación de usuario mediante el servicio web
 - configuración 11

C

- configuración
 - impresoras 10
 - inicio de sesión, método 9
 - inicio de sesión, pantalla 9
- configuración de autenticación de usuario con LDAP 14
- configuración de autenticación de usuario con PIN 13

- configuración de dominios
 - métodos de inicio de sesión 16
- configuración de grupos para una cuenta de usuario interno 5
- configuración de la autenticación de administrador 8
- configuración de la autenticación de usuario basada en impresora 9
- configuración de la autenticación de usuario mediante el servicio de identidad 12
- configuración de la autenticación de usuario mediante el servicio web 11
- configuración de los ajustes de LDAP 15
- configuración de los ajustes del servicio de identidad 13
- configuración de los controles de acceso 6
- configuración de los valores de PIN 14
- configuración de los valores del servicio web 12
- configuración de preferencias de aplicación 15
- configuración de una nueva impresora principal 18
- Configuración LDAP
 - configuración 15
- creación de una plantilla de seguridad 6
- cuentas de usuario interno
 - adición 5
 - agrupación 5

D

- descripción general 4

E

- el usuario está bloqueado 22
- eliminación
 - impresoras cliente 17
 - usuario, cuentas 17
- Embedded Web Server
 - acceso 5
 - error de aplicación 21

- error de autenticación 22
- exportación de un archivo de configuración 16

F

- funciones, impresora
 - reasignación 18

I

- importación de un archivo de configuración 16
- impresora de seguridad
 - asignación 18
 - configuración 10
- impresora principal
 - configuración 10
- impresoras
 - configuración 10
- impresoras cliente
 - adición 17
 - configuración 10
 - eliminación 17
 - migración 18
- inicio de sesión
 - manual 20
 - PIN 20
- inicio de sesión manual 20
- inicio de sesión manual en la impresora 20
- inicio de sesión mediante PIN 20
- inicio de sesión, método
 - configuración 9
- inicio de sesión, pantalla
 - configuración 9

M

- mensajes de registro
 - configuración 15
- migración
 - impresoras cliente 18
- mostrar dominios de las cuentas de usuario 16

N

- no se puede conectar al servidor LDAP 24

no se puede encontrar información del dominio 23
no se puede registrar una impresora cliente 22
no se puede validar la tarjeta 23
nueva impresora principal configuración 18

P

página de configuración para la aplicación
acceso 8
página de estado
acceso 17
perfil de inicio de sesión
uso 15
PIN
registro 20
plantilla de seguridad
creación 6
preferencias de aplicación
configuración 15
preguntas más frecuentes 25

R

reasignación de funciones de impresora 18
registro de un PIN 20
registro de usuarios 20

S

solución de problemas
el usuario está bloqueado 22
error de aplicación 21
error de autenticación 22
no se puede conectar al servidor LDAP 24
no se puede encontrar información del dominio 23
no se puede registrar una impresora cliente 22
no se puede validar la tarjeta 23

U

uso de la función de copia sin iniciar sesión 9
uso de la función de fax sin iniciar sesión 9
uso de un perfil de inicio de sesión 15

usuario, cuentas
eliminación 17
usuarios
adición 20
registro 20

V

Valores de PIN
configuración 14
Valores del servicio de identidad
configuración 13
valores del servicio web
configuración 12