



Lexmark™

Autenticación por tarjeta

Versión 5.8

Guía del administrador

Diciembre de 2020

www.lexmark.com

Contenido

- Historial de cambios..... 4**
- Descripción general..... 5**
- Lista de comprobación de aptitud para la implementación..... 6**
- Configuración de la aplicación..... 8**
 - Acceso a Embedded Web Server..... 8
 - Configuración de la aplicación como método de inicio de sesión predeterminado..... 8
 - Configuración de la validación de tarjetas basadas en impresora..... 8
 - Configuración de la validación de tarjetas en el servicio web..... 9
 - Configuración de la validación de tarjetas LDAP..... 10
 - Configuración de la validación de tarjetas del servicio de identidad..... 11
 - Configuración de la autenticación con PIN..... 12
 - Asignación de un método de inicio de sesión para el registro de tarjetas..... 12
 - Asignación de un método de inicio de sesión para el inicio de sesión manual..... 13
 - Configuración de la autenticación de administrador..... 13
 - Mostrar dominios de las cuentas de usuario..... 14
 - Configuración de la pantalla de inicio de sesión..... 14
 - Protección del acceso a aplicaciones y funciones individuales..... 15
 - Configuración de la demora de cierre de sesión de distintivo..... 16
 - Importación o exportación de archivos de configuración..... 16
- Administración de la aplicación..... 17**
 - Acceso a la página de estado de la aplicación..... 17
 - Administración de impresoras cliente y de cuentas de usuario..... 18
 - 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**
 - Error de la aplicación..... 21

Error de autenticación.....21

El usuario está bloqueado..... 22

No se puede registrar una impresora cliente..... 22

No se puede conectar al servidor LDAP.....22

Algunos valores no aparecen en la página de configuración.....23

El usuario no tiene privilegios de acceso..... 23

No se puede encontrar información del dominio.....24

Preguntas más frecuentes..... 25

Avisos..... 27

Índice..... 28

Historial de cambios

Diciembre de 2020

- Se ha añadido información sobre una advertencia relacionada con la falta de un lector de tarjetas.

Junio de 2020

- Se ha añadido información sobre los nuevos valores para verificar certificados.
- Información eliminada sobre requisitos de licencia.

Julio de 2019

- Se han añadido instrucciones sobre cómo configurar la autenticación con PIN.

Diciembre de 2018

- Se han añadido instrucciones sobre cómo configurar la autenticación de administrador.

Agosto de 2017

- Se ha añadido información sobre lo siguiente:
 - Valores de bloqueo de pantalla
 - Perfil personalizado
- Se ha eliminado información sobre el uso de la aplicación Personalización de pantalla para gestionar la pantalla de inicio de sesión.

Agosto de 2016

- Se ha añadido información sobre lo siguiente:
 - Compatibilidad con autenticación con PIN
 - Botones de acceso rápido para inicio de sesión mediante PIN y manual

Julio de 2016

- Se ha añadido información sobre lo siguiente:
 - Inicio de sesión manual
 - Compatibilidad con varios dominios
 - Uso de las cuentas de servicio para autenticarse en el proveedor de servicios de identidad
 - Varios dominios Kerberos para el registro de tarjetas y el inicio de sesión manual
 - Color del texto de inicio de sesión personalizado
 - Permisos de grupo

Enero de 2016

- Versión inicial del documento para productos multifunción con pantalla táctil de tipo tableta.

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 vuelva a estar conectada.

Nota: A la hora de configurar las impresoras, asegúrese de que se encuentran en la misma red.

- Lightweight Directory Access Protocol (LDAP), servidores Document Distributor (LDD) de Lexmark™ o proveedores de servicios de identidad en función del tipo de autenticación definida por la organización.

También puede configurar la aplicación para permitir a los usuarios iniciar sesión utilizando una cuenta de servicio, un nombre de usuario, un nombre de usuario y contraseña o un PIN.

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

Lista de comprobación de aptitud para la implementación

Antes de empezar, asegúrese de que:

- Se ha configurado al menos una cuenta local o de red en la impresora. Póngase en contacto con el administrador del sistema para obtener más información.
- Se ha instalado un lector de tarjetas y su controlador en la impresora.
- Tiene la dirección del servidor web para configurar la autenticación con PIN.

Dispone de la siguiente información para configurar la validación de tarjetas basada en impresora:

- Dirección IP o el nombre de host de la nueva impresora principal

- Dirección IP o el nombre de host de la nueva impresora de seguridad

Dispone de la siguiente información para configurar la validación de tarjetas en el servicio web:

- URL del servidor

- Versión de la interfaz de registro y búsqueda

Dispone de la siguiente información para configurar la validación de tarjetas LDAP:

Nota: También puede utilizar una cuenta de red LDAP existente que se haya configurado en la impresora.

- Dirección del servidor

- Número de puerto del servidor

- Base de búsqueda

- Nombre de usuario de inicio de sesión

- Contraseña de inicio de sesión

- Atributos LDAP

- ID de usuario

- ID placa

- Información de usuario (opcional)

Dispone de la siguiente información para configurar la validación de tarjetas en el servicio de identidad:

- Dirección del proveedor de servicios de identidad

- Dirección del proveedor de servicios de distintivo

Configuración de 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.
 - En la pantalla de inicio de la impresora, toque **Valores > Red/Puertos > Descripción general de red**.
- 2 Abra un explorador web e introduzca la dirección IP de la impresora.

Configuración de la aplicación como método de inicio de sesión predeterminado

- 1 En Embedded Web Server, haga clic en **Valores > Seguridad > Métodos de inicio de sesión**.
- 2 Haga clic en **Cambiar** junto a Método de inicio de sesión en el panel de control predeterminado.
- 3 En el menú del panel de control, seleccione **Autenticación de tarjetas**.
- 4 Haga clic en **Guardar**.

Configuración de la validación de tarjetas basadas en impresora

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

- 1 Desde Embedded Web Server, desplácese a la página de configuración de la aplicación:
Aplicaciones > Autenticación por tarjeta > Configurar
- 2 En la sección Autenticación de usuario, establezca Validación de tarjetas en **Basada en la impresora**.
Nota: La configuración de Verificar certificado solo se aplica a la validación del servicio de identidad y del servicio web.
- 3 En la sección Configuración basada en impresora, haga lo siguiente:
 - a Seleccione la función de 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.

b Introduzca el nombre de host o la dirección 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 **Guardar**.

Configuración de la validación de tarjetas en el servicio web

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

1 Desde Embedded Web Server, desplácese a la página de configuración de la aplicación:

Aplicaciones > Autenticación por tarjeta > Configurar

2 En la sección Autenticación de usuario, establezca Validación de tarjetas en **Servicio web**.

3 Seleccione **Verificar certificado** para validar todas las conexiones al servidor. Si Verificar certificado no está seleccionado, no se validará la CA.

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

Nota: El valor predeterminado es cadena.

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

6 En el campo Comprobar 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 Comprobar hosts para incluirlos en la lista blanca.

7 En la sección Valores del servicio web, escriba la dirección URL del servidor LDD.

8 Si fuera necesario, ajuste el tiempo de espera de conexión del servidor.

9 Establezca la interfaz de registro. Seleccione una de las siguientes opciones:

- **Versión 1:** solo se muestran el ID de distintivo y el ID de usuario en el cuadro de diálogo Información del distintivo.
- **Versión 2:** se muestra lo siguiente en el cuadro de diálogo Información del distintivo:
 - ID de distintivo
 - ID de usuario
 - Dirección IP
 - Nombre de host

- 10 Establezca la interfaz de búsqueda. Para registrar cuándo y dónde se usó el distintivo por última vez, seleccione **Versión 2**.
- 11 Haga clic en **Guardar**.

Configuración de la validación de tarjetas LDAP

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

- 1 Desde Embedded Web Server, desplácese a la página de configuración de la aplicación:

Aplicaciones > Autenticación por tarjeta > Configurar

- 2 En la sección Autenticación de usuario, establezca Validación de tarjetas en **LDAP**.

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

- 3 En la sección Configuración de servidor LDAP, configure los valores.

Nota: 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. Si hay configuradas varias cuentas LDAP en la impresora, la aplicación seleccionará el nombre de configuración por orden alfabético. Los nombres de configuración que empiecen por letras en mayúsculas se seleccionan antes que los que empiezan por letras en minúsculas.

- **Dirección del servidor:** introduzca la dirección del servidor LDAP.
- **Puerto del servidor:** introduzca el número de puerto LDAP.
- **Utilizar SSL:** seleccione esta opción para activar una conexión segura.
- **Base de búsqueda:** introduzca el nodo en el servidor LDAP en el que se encuentren las cuentas de usuario. Puede introducir varias bases de búsqueda separadas por comas.
- **Nombre de usuario de inicio de sesión:** introduzca el nombre de usuario de la cuenta LDAP. En algunas configuraciones del servidor LDAP, las credenciales de usuario son obligatorias.
- **Contraseña de inicio de sesión:** introduzca la contraseña de la cuenta LDAP. En algunas configuraciones del servidor LDAP, las credenciales de usuario son obligatorias.

- 4 En la sección Atributos LDAP, configure los ajustes.

- **ID de usuario:** introduzca el atributo LDAP que la aplicación busca al autenticar las credenciales de usuario. Por ejemplo, **samaccountname**, **uid**, **cn** o un atributo definido por el usuario.
- **Id. de distintivo:** escriba el atributo LDAP para autenticar los usuarios con sus números de distintivo asignados. Por ejemplo, **employeeNumber**.
- **Información de usuario:** introduzca el resto de la información de usuario que la aplicación puede recuperar del servidor LDAP.
- **Atributo de miembro del grupo:** introduzca el atributo LDAP necesario para la búsqueda de grupos.
- **Lista de grupos:** introduzca el grupo LDAP al que pertenezcan las cuentas de usuario. Los grupos especificados se añaden a la lista de permisos de grupo de la aplicación, donde puede definir controles de acceso específicos para cada grupo. Puede escribir varios nombres de grupo separados por comas.

- 5 Haga clic en **Guardar**.

Configuración de la validación de tarjetas del servicio de identidad

Utilice la validación de tarjetas del servicio de identidad al validar usuarios mediante un proveedor de servicios de identidad.

1 Desde Embedded Web Server, desplácese a la página de configuración de la aplicación:

Aplicaciones > Autenticación por tarjeta > Configurar

2 En la sección Autenticación de usuario, establezca Validación de tarjetas en **Servicio de identidad**.

3 Seleccione **Verificar certificado** para validar todas las conexiones al servidor. Si Verificar certificado no está seleccionado, no se validará la CA.

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

Nota: El valor predeterminado es cadena.

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

6 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.

7 En la sección Configuración del servicio de identidad, introduzca el nombre de host o la dirección IP del proveedor de servicios de identidad.

8 Introduzca la dirección IP o el nombre de host del proveedor de servicios de distintivos.

9 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.

10 Si tiene un ID de cliente y un Secreto de cliente del proveedor de servicios de identidad, introduzca los datos en los campos correspondientes.

11 Ajuste el tiempo de espera de la red y la toma.

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

13 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.

14 Configure el Registro de tarjetas en **Servicio de identidad**.

15 Haga clic en **Guardar**.

Configuración de la autenticación con PIN

Antes de empezar, asegúrese de que sus credenciales están configuradas en los valores de la cuenta local o de red de la impresora.

- 1 Desde Embedded Web Server, desplácese a la página de configuración de la aplicación:

Aplicaciones > Autenticación por tarjeta > Configurar

- 2 En la sección Autenticación de usuario, dentro de la sección Inicio de sesión mediante PIN, seleccione **Activar inicio de sesión con PIN**.
- 3 Seleccione **Mostrar en salvapantallas** para mostrar el botón de Inicio de sesión mediante PIN en el salvapantallas.
- 4 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.

Nota: Si se selecciona el método Solo PIN, no podrá registrar un PIN nuevo ni actualizar uno existente.

- 5 Introduzca la dirección de servidor web en la que se guardan los PIN.
- 6 Si es necesario, escriba el texto de inicio de sesión mediante PIN y, a continuación, defina la longitud mínima del PIN.

Nota: Si el campo de texto de inicio de sesión mediante PIN se deja en blanco, se mostrará el texto de inicio de sesión mediante PIN predeterminado. El texto de inicio de sesión mediante PIN predeterminado es **Escriba sus credenciales para iniciar sesión**.

- 7 Si es necesario, escriba los mensajes de error de PIN no válido.

Nota: Si los campos de texto se dejan en blanco, se mostrarán los mensajes de error predeterminados. Los mensajes de error predeterminados son **Longitud de PIN no válida.** y **PIN no válido.**

- 8 Si es necesario, defina los tiempos de espera de la red y la toma.

Nota: El valor predeterminado para el tiempo de espera de la red y la toma es 15 segundos.

- 9 Haga clic en **Guardar**.

Asignación de un método de inicio de sesión para el registro de tarjetas

Antes de empezar, asegúrese de que sus credenciales están configuradas en los valores de la cuenta local o de red de la impresora.

- 1 Desde Embedded Web Server, desplácese a la página de configuración de la aplicación:

Aplicaciones > Autenticación por tarjeta > Configurar

- 2 En la sección Autenticación de usuario, en el menú Registro de tarjetas, seleccione un método de inicio de sesión.

Nota: Si desea utilizar Kerberos, Active Directory o LDAP+GSSAPI, seleccione un dominio. Si el método de inicio de sesión seleccionado cuenta con varios dominios, el dominio seleccionado se mostrará por defecto durante el registro de la tarjeta.

3 Haga clic en **Guardar**.

Asignación de un método de inicio de sesión para el inicio de sesión manual

Antes de empezar, asegúrese de que sus credenciales están configuradas en los ajustes de la cuenta local o de red de la impresora.

1 Desde Embedded Web Server, desplácese a la página de configuración de la aplicación:

Aplicaciones > Autenticación por tarjeta > Configurar

2 En la sección Autenticación de usuario, dentro de la sección Valores de inicio de sesión manual, establezca **Inicio de sesión manual** como método de inicio de sesión.

Notas:

- Si Inicio de sesión manual está configurado como Utilizar cuenta de servicio, entonces no se solicitará a los usuarios que introduzcan manualmente las credenciales. La aplicación usa la cuenta de servicio para iniciar sesión.
- Si desea utilizar Kerberos, Active Directory o LDAP+GSSAPI, seleccione un dominio. Si el método de inicio de sesión seleccionado tiene varios dominios, el dominio seleccionado es el dominio predeterminado que se muestra durante el inicio de sesión manual.

3 Seleccione **Mostrar en protector de pantalla** para mostrar el botón de Inicio de sesión manual en el protector de pantalla.

4 Haga clic en **Guardar**.

Configuración de la autenticación de administrador

1 Desde Embedded Web Server, desplácese a la página de configuración de la aplicación:

Aplicaciones > Autenticación por tarjeta > Configurar

2 En la sección Autenticación de usuario, dentro de la sección Valores de inicio de sesión del administrador, establezca **Inicio de sesión del administrador** como método de inicio de sesión.

Nota: Asegúrese de que ha configurado una cuenta de administrador local para la impresora, así como de que ha configurado los permisos para el Grupo de administración de dispositivos. De forma predeterminada, las funciones y los menús no están permitidos en este grupo.

3 Seleccione un grupo autorizado que pueda usar la función de inicio de sesión del administrador.

Nota: Esta configuración solo es aplicable a las cuentas de usuario y contraseña, y de nombre de usuario.

4 Seleccione **Mostrar en salvapantallas** para mostrar el botón de Inicio de sesión del administrador en el salvapantallas.

5 Haga clic en **Guardar**.

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, desplácese a la página de configuración de la aplicación:

Aplicaciones > Autenticación por tarjeta > Configurar

- 2 En la sección Valores avanzados, seleccione **Usar dominio seleccionado**.

- 3 Haga clic en **Guardar**.

Configuración de la pantalla de inicio de sesión

Nota: Asegúrese de que la configuración del salvapantallas de la aplicación Personalización de pantalla está desactivada. Para obtener más información, consulte la *Guía del administrador de Personalización de pantalla*.

- 1 Desde Embedded Web Server, desplácese a la página de configuración de la aplicación:

Aplicaciones > Autenticación por tarjeta > Configurar

- 2 En la sección Configuración de la pantalla de inicio de sesión, haga lo siguiente:

- Para personalizar el mensaje de inicio de sesión, seleccione **Utilizar texto de inicio de sesión personalizado**, a continuación, escriba el mensaje.
- Configure el color del texto personalizado de inicio de sesión en blanco o negro.
- Para cambiar el fondo de la pantalla de inicio de sesión, seleccione **Usar imagen personalizada para la pantalla de inicio de sesión** y, a continuación, cargue el archivo de imagen.
- Para personalizar el mensaje del inicio de sesión manual, escriba el mensaje en el campo de Texto de inicio de sesión manual.
- Para personalizar el mensaje del inicio de sesión del administrador, escriba el mensaje en el campo de Texto de inicio de sesión del administrador.
- Active las funciones de copia y fax sin necesidad de iniciar sesión.
- Desactive la advertencia si no hay un lector de tarjetas conectado.

- 3 En la sección Valores de bloqueo de pantalla, seleccione la ubicación del texto de inicio de sesión y, a continuación, escriba el nombre de perfil o el ID de la aplicación. El perfil se ejecutará automáticamente tras el inicio de sesión.

4 Desde la sección Perfil personalizado, introduzca el nombre de perfil, el ID de la aplicación o la función de impresora, y, a continuación, escriba el nombre personalizado del icono. Si fuera necesario, seleccione **Utilizar icono personalizado** y, a continuación, cargue el archivo de imagen.

5 Haga clic en **Guardar**.

Nota: La pantalla de inicio de sesión solo puede desactivarse en entornos que usan servicio de identidad.

Permitir el acceso público para las funciones de copia y fax

1 En Embedded Web Server, haga clic en **Valores > Seguridad > Métodos de inicio de sesión**.

2 En la sección Público, haga clic en **Administrar permisos**.

3 Despliegue **Acceso a funciones**, a continuación, seleccione **Función Copiar** y **Función Fax**.

4 Haga clic en **Guardar**.

Protección del acceso a aplicaciones y funciones individuales

Para solicitar a los usuarios que se autentiquen antes de acceder a una aplicación o una función de la impresora, haga lo siguiente:

Restricción del acceso público a las aplicaciones o funciones

1 En Embedded Web Server, haga clic en **Valores > Seguridad > Métodos de inicio de sesión**.

2 En la sección Público, haga clic en **Administrar permisos**.

3 Despliegue una o más categorías y, a continuación, elimine la aplicación o función que desea proteger.

4 Haga clic en **Guardar**.

Administrar permisos de grupo

Nota: Si la función Inicio de sesión del administrador está activada, configure los permisos del Grupo de administración de dispositivos.

1 En la sección Métodos adicionales de inicio de sesión, haga clic en **Administrar permisos** junto a Autenticación por tarjeta.

2 Seleccione un grupo cuyos permisos desee administrar.

Nota: La lista muestra los grupos que se añaden a la lista de grupos LDAP en la página de configuración de la aplicación.

3 Despliegue una o más categorías y, a continuación, seleccione la aplicación o función cuyo acceso desee permitir.

4 Haga clic en **Guardar**.

Notas:

- Durante el inicio de sesión, la aplicación aplica los permisos del grupo al que pertenece el usuario. Si el usuario pertenece a varios grupos, la aplicación fusionará todos los permisos. Por ejemplo, el grupo A

solo tiene permiso de copia, y el B solo tiene permiso de envío de faxes. Si el usuario pertenece a ambos grupos, la aplicación le permitirá tanto copiar como enviar faxes.

- Los permisos de grupo del método de inicio de sesión asignado para el registro de tarjetas y el inicio de sesión manual deben tener configurados los mismos permisos de grupo en la aplicación.

Configuración de la demora de cierre de sesión de distintivo

Puede establecer el tiempo que debe transcurrir hasta que la impresora registre un acercamiento de la tarjeta como una desconexión. Si acerca la tarjeta dentro del tiempo especificado, permanecerá conectado. Si acerca la tarjeta después de que termine el tiempo de espera, se cerrará la sesión.

Si ha iniciado sesión y otro usuario inicia la sesión utilizando una tarjeta, se cerrará su sesión inmediatamente y se iniciará la del otro usuario. Esto ocurre aunque el temporizador de demora de cierre de sesión de distintivo esté activo.

- 1 Desde Embedded Web Server, desplácese a la página de configuración de la aplicación:
Aplicaciones > Autenticación por tarjeta > Configurar
- 2 En la sección Configuración avanzada, establezca la demora de cierre de sesión de distintivo.
- 3 Haga clic en **Guardar**.

Importación o exportación de archivos de configuración

Si importa archivos de configuración, las configuraciones de aplicaciones existentes se sobrescribirán.

- 1 Desde Embedded Web Server, desplácese a la página de configuración de la aplicación:
Aplicaciones > Autenticación por tarjeta > Configurar
- 2 Haga clic en **Configuración de importación/exportación**.
- 3 Realice una de las siguientes acciones:
 - Busque el archivo de configuración y, a continuación, haga clic en **Importar**.
 - Haga clic en **Exportar**.

Administración de la aplicación

La validación de tarjetas basada en impresora le permite administrar impresoras cliente y cuentas de usuario en la página de estado de la aplicación.

Notas:

- La página de estado de la aplicación solo está disponible al utilizar la autenticación basada en impresora.
- Si no se les asignan funciones a las impresoras, aparecen como No configuradas en la página de estado de la aplicación. Asegúrese de configurar la función de la impresora. Para obtener más información, consulte [“Configuración de la validación de tarjetas basadas en impresora” en la página 8.](#)

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 > Iniciar 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 impresoras cliente y de cuentas de usuario

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

- 1 En Embedded Web Server, haga clic en **Aplicaciones > Iniciar aplicaciones > Autenticación de tarjetas**.
- 2 En la sección Clientes, realice una de las siguientes acciones:

Añadir impresoras cliente

- a Haga clic en **Añadir clientes**.
- b Escriba la dirección IP de la impresora cliente y haga clic en **Añadir clientes**.

Notas:

- Utilice comas para separar varias direcciones IP.
- Utilice un asterisco como último octeto para buscar varias direcciones IP. Por ejemplo, escriba **10.194.1.***.

Borrado de impresoras cliente

- a Seleccione una o más impresoras cliente de la lista Clientes.
- b Haga clic en **Borrar clientes**.

Nota: No puede borrar las impresoras cliente si la aplicación se encuentra fuera de línea o no está instalada.

Borrado de cuentas de usuario

- 1 En Embedded Web Server, haga clic en **Aplicaciones > Iniciar aplicaciones > Autenticación de tarjetas**.
- 2 En la sección Principal, haga clic en **Eliminar usuarios**.
- 3 Escriba un ID de usuario.
Nota: Utilice comas para separar varios ID de usuario.
- 4 Haga clic en **Eliminar**.

Reasignación de funciones de impresora

Configuración de una nueva impresora principal

- 1 Desde el Embedded Web Server de la nueva impresora principal, desplácese a la página de configuración de la aplicación:
Aplicaciones > Autenticación por tarjeta > Configurar
- 2 Haga clic en **Autenticación de usuario** y, a continuación, en la sección Configuración basada en impresora, seleccione la función **Principal**.
- 3 Introduzca la dirección IP o el nombre de host de la impresora de seguridad.
- 4 Haga clic en **Guardar**.

Asignación de la impresora de seguridad a la nueva impresora principal

- 1 Desde el Embedded Web Server de la impresora de seguridad, desplácese a la página de configuración de la aplicación:
Aplicaciones > Autenticación por tarjeta > Configurar
- 2 Haga clic en **Autenticación de usuario** y, a continuación, en la sección Configuración basada en impresora, seleccione la función **De seguridad**.
- 3 Introduzca la dirección IP o el nombre de host de la nueva impresora principal.
- 4 Haga clic en **Guardar**.

Reasignación de una impresora cliente

- 1 En el Embedded Web Server de la actual impresora principal, haga clic en **Aplicaciones > Iniciar aplicaciones > Autenticación de tarjetas**.
- 2 En la sección Clientes, elimine la impresora cliente.
- 3 Realice una de las siguientes acciones:

Añada la impresora cliente mediante la página de configuración de la aplicación

- a Desde el Embedded Web Server de la impresora cliente, desplácese a la página de configuración de la aplicación:
Aplicaciones > Autenticación por tarjeta > Configurar
- b Haga clic en **Autenticación de usuario** y, a continuación, en la sección Configuración basada en impresora, seleccione la función **Cliente**.
- c Introduzca los nombres de host o las direcciones IP de la nueva impresora principal y la nueva impresora de seguridad.
- d Haga clic en **Guardar**.

Añada la impresora cliente a mediante la página de estado de la principal

- a En el Embedded Web Server de la nueva impresora principal, haga clic en **Aplicaciones > Iniciar aplicaciones > Autenticación de tarjetas**.
- b En la sección Clientes, haga clic en **Añadir clientes**.
- c Escriba la dirección IP de la impresora cliente.
- d Haga clic en **Añadir clientes**.

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 Toque **Registrarse**.

Nota: Una vez realizado el registro, se iniciará sesión automáticamente. Si acerca la tarjeta dentro del periodo especificado en la demora de cierre de sesión, permanecerá conectado. Para cerrar sesión, pulse el botón de inicio o toque el nombre de usuario en la esquina superior derecha del panel de control de la impresora y, a continuación, confirme el cierre de sesión. Para obtener más información, consulte [“Configuración de la demora de cierre de sesión de distintivo” en la página 16](#).

Registro de un PIN

- 1 En el panel de control de la impresora, toque **Inicio de sesión con PIN**.
- 2 Toque  > **Registrar PIN**.

Nota: Para cambiar un PIN existente, toque **Cambiar PIN**.

- 3 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 de sesión mediante PIN**
 - **Inicio de sesión manual**
 - **Inicio de sesión del administrador**

Nota: Si selecciona **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 de diagnóstico

- 1 Abra un navegador web y, a continuación, introduzca **IP/se**, en donde **IP** es la dirección IP de la impresora.
- 2 Haga clic en **Embedded Solutions** y, a continuación, haga lo siguiente:
 - a Borre el archivo de registro.
 - b Configure el nivel de inicio de sesión en **Sí**.
 - c Genere el archivo de registro.
- 3 Analice el registro y resuelva el problema.

Nota: Después de resolver el problema, configure el nivel de inicio de sesión en **No**.

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 Embedded Web Server, haga clic en **Valores > Dispositivo**.
- 2 Haga lo siguiente:

Ajuste del tiempo de espera de inactividad de la pantalla

- a Haga clic en **Preferencias**.
- b Aumente el valor del tiempo de espera de inactividad de la pantalla.
- c Haga clic en **Guardar**.

Ajuste del tiempo de espera del modo de suspensión

- a Haga clic en **Gestión de energía**.
- b Aumente el valor del tiempo de espera del modo de suspensión.
- c Haga clic en **Guardar**.

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 está en línea y no está ocupado

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

El usuario está bloqueado.

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

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

Nota: Esta solución solo se puede aplicar en algunos modelos de impresora.

- 1 En Embedded Web Server, haga clic en **Valores > Seguridad > Restricciones de conexión**.
- 2 Actualice el tiempo de bloqueo y el número permitido de intentos de conexión fallidos.
- 3 Haga clic en **Guardar**.

Nota: Espere a que pase la duración de bloqueo antes de que surtan efectos los nuevos valores.

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 validación de tarjetas basadas en impresora” en la página 8](#).

Póngase en contacto con el proveedor de la solución

Si aun así no puede solucionar el problema, póngase en contacto con el proveedor de la solución.

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 la validación de tarjetas LDAP” en la página 10](#).

Póngase en contacto con el proveedor de la solución

Si aun así no puede solucionar el problema, póngase en contacto con el proveedor de la solución.

Algunos valores no aparecen en la página de configuración

Realice al menos una de las siguientes acciones:

Asegúrese de que utiliza el navegador Web recomendado

Para obtener más información, consulte el archivo *Léame*.

Cuando utilice Internet Explorer, asegúrese de que no se muestran los sitios de la intranet en la vista de compatibilidad

Para conocer más detalles, consulte la información de ayuda del navegador.

Póngase en contacto con el representante de Lexmark

El usuario no tiene privilegios de acceso

Realice alguna de estas acciones:

Active los permisos del método de inicio de sesión asignado al registro de tarjeta y al inicio de sesión manual

- 1** En Embedded Web Server, haga clic en **Valores > Seguridad > Métodos de inicio de sesión**.
- 2** Haga clic en **Administrar grupos/permisos** junto al método de inicio de sesión asignado al registro de tarjeta y el inicio de sesión manual.
- 3** Active los permisos idénticos a los permisos de autenticación de tarjetas.
- 4** Haga clic en **Guardar**.

Póngase en contacto con el representante de Lexmark

No se puede encontrar información del dominio

La opción Utilizar dominio seleccionado está activada en la aplicación, pero el método de inicio de sesión asignado para el inicio de sesión manual o de registro de tarjetas no requiere la selección de un dominio. Por ejemplo, cuentas locales o LDAP. Los métodos de inicio de sesión que requieren una selección de dominio son Kerberos, Active Directory y LDAP+GSSAPI.

Realice alguna de estas acciones:

Desactivar la selección de dominio

- 1 Desde Embedded Web Server, desplácese a la página de configuración de la aplicación:
Aplicaciones > Autenticación por tarjeta > Configurar
- 2 En la sección Valores avanzados, desactive **Utilizar dominio seleccionado**.
- 3 Haga clic en **Guardar**.

Cambio del método de inicio de sesión

- 1 Desde Embedded Web Server, desplácese a la página de configuración de la aplicación:
Aplicaciones > Autenticación por tarjeta > Configurar
- 2 En la sección Autenticación de usuario, cambie el método de inicio de sesión para el registro de tarjetas y el inicio de sesión manual a Kerberos, Active Directory o LDAP+GSSAPI.
- 3 Haga clic en **Guardar**.

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 aunque la principal esté fuera de línea y reasignarla a la nueva impresora principal?

Sí. Haga lo siguiente:

- 1 Vuelva a instalar la aplicación desde la impresora cliente.
- 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 validación de tarjetas basadas en impresora” en la página 8.](#)

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

Los botones Copiar o Fax no aparecen si se ha establecido el control de acceso a las funciones Copiar y Fax. Para obtener más información, consulte [“Configuración de la pantalla de inicio de sesión” en la página 14.](#)

¿Cómo puedo restringir el acceso público a la página de configuración para todas las aplicaciones?

- 1 En Embedded Web Server, haga clic en **Valores > Seguridad > Métodos de inicio de sesión.**
- 2 En la sección Público, haga clic en **Administrar permisos.**
- 3 Despliegue **Administración de dispositivos** y, a continuación, desactive **Configuración.**
- 4 Haga clic en **Guardar.**
- 5 En Embedded Web Server, haga clic en **Valores > Seguridad > Métodos de inicio de sesión.**
- 6 Haga clic en **Administrar permisos** o **Administrar grupos/permisos** junto al método de inicio de sesión que desea configurar.
- 7 Haga clic en el grupo para el que desea permitir acceso a la página de configuración para todas las aplicaciones.

8 Despliegue **Administración de dispositivos** y, a continuación, asegúrese de que la opción **Configuración** está seleccionada.

9 Haga clic en Guardar.

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.

© 2016 Lexmark International, Inc.

Reservados todos los derechos.

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 8
acceso, controles 15
adición
 impresoras cliente 18
 usuarios 20
agregar cuentas locales 12
algunos valores no aparecen en la página de configuración 23
aplicaciones
 seguridad 15
archivo de configuración
 importación o exportación 16
asignación de un método de inicio de sesión 12
asignación de un método de inicio de sesión para el inicio de sesión manual 13
autenticación
 configuración 8
Autenticación con PIN
 configuración 12
autenticación de administrador
 configuración 13

C

cambio de PIN 20
configuración
 Autenticación con PIN 12
 demora de cierre de sesión de distintivo 16
 inicio de sesión, pantalla 14
 nueva impresora de seguridad 18
 nueva impresora principal 18
 servicio web, validación de tarjetas 9
 tarjetas LDAP, validación 10
 validación de la tarjeta, basada en impresora 8
 Validación de tarjetas del servicio de identidad 11
configuración de dominios
 métodos de inicio de sesión 14

configuración de la autenticación de administrador 13
cuentas locales
 adición 12

D

demora de cierre de sesión de distintivo
 configuración 16
descripción general 5

E

el usuario está bloqueado 22
el usuario no tiene privilegios de acceso 23
eliminación
 impresoras cliente 18
 usuario, cuentas 18
Embedded Web Server
 acceso 8
error de aplicación 21
error de autenticación 21
exportación de un archivo de configuración 16

F

función de copia
 uso sin iniciar sesión 14
función de fax
 uso sin iniciar sesión 14
funciones
 seguridad 15
funciones, impresora
 reasignación 18

H

historial de cambios 4

I

importación de un archivo de configuración 16
impresoras cliente
 adición 18
 eliminación 18
 migración 18
inicio de sesión
 manual 20

PIN 20

inicio de sesión manual 20
 asignación de un método de inicio de sesión 13
inicio de sesión manual en la impresora 20
inicio de sesión mediante PIN 20
inicio de sesión, pantalla
 configuración 14

L

lista de comprobación
 aptitud para la implementación 6
lista de comprobación de aptitud para la implementación 6

M

migración
 impresoras cliente 18
 usuario, cuentas 18
mostrar dominios de las cuentas de usuario 14

N

no se puede conectar al servidor LDAP 22
no se puede encontrar información del dominio 24
no se puede registrar una impresora cliente 22

P

página de estado
 acceso 17
PIN
 registro 20
predeterminado, método de inicio de sesión 8
preguntas frecuentes 25
preguntas más frecuentes 25

R

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

S

- seguridad
 - aplicaciones 15
 - funciones de la impresora 15
- servicio web, validación de
- tarjetas
 - configuración 9
- solución de problemas
 - algunos valores no aparecen en la página de configuración 23
 - el usuario está bloqueado 22
 - el usuario no tiene privilegios de acceso 23
 - error de aplicación 21
 - error de autenticación 21
 - no se puede conectar al servidor LDAP 22
 - no se puede encontrar información del dominio 24
 - no se puede registrar una impresora cliente 22

T

- tarjetas LDAP, validación
 - configuración 10
- tarjetas, autenticación
 - predeterminado, método de inicio de sesión 8

U

- uso de la función de copia sin iniciar sesión 14
- uso de la función de fax sin iniciar sesión 14
- usuario, cuentas
 - eliminación 18
 - migración 18
- usuarios
 - adición 20
 - registro 20

V

- validación de la tarjeta, basada en impresora
 - configuración 8
- Validación de tarjetas del servicio de identidad
 - configuración 11