Autenticación de tarjeta inteligente

Guía del administrador

Agosto de 2017

www.lexmark.com

Contenido

Historial de cambios

Agosto de 2017

- Se han añadido instrucciones sobre el cambio de método de inicio de sesión.
- Se han añadido instrucciones sobre cómo deshabilitar la aplicación de cuotas de dispositivos.
- Se han añadido los idiomas portugués de Brasil, finés, francés, alemán, italiano, chino simplificado y español.

Julio de 2016

- Se han añadido instrucciones sobre cómo configurar la aplicación de envío de correo electrónico a dirección propia.

Enero de 2016

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

Descripción general

Autenticación de tarjetas inteligentes es una recopilación de aplicaciones empleadas para proteger el acceso a las impresoras y sus funciones. Las aplicaciones permiten iniciar sesión en una impresora de forma manual o con una tarjeta inteligente y, a continuación, envían correos electrónicos de forma segura y activan los trabajos de impresión. También puede configurar otros valores de seguridad en una aplicación, como la el cifrado o la firma de correos electrónicos.

El paquete Autenticación de tarjetas inteligentes incluye las siguientes aplicaciones:

- **Cliente de autenticación de tarjetas inteligentes**: permite acceder de forma segura a impresoras al solicitar a los usuarios que inicien sesión utilizando una tarjeta inteligente o un nombre de usuario y contraseña. Puede proteger el acceso a la pantalla de inicio de la impresora o a aplicaciones y funciones concretas. La aplicación también proporciona opciones de autenticación Kerberos y un ticket Kerberos que puede utilizarse para proteger otras aplicaciones.
- **Controlador de tarjetas inteligentes**: permite a la impresora comunicarse con una tarjeta inteligente compatible.
- **Personalización de pantalla**: permite cargar imágenes a la impresora. Puede usar las imágenes para crear presentaciones personalizadas o para establecer el fondo de escritorio y el salvapantallas de la impresora. Proteja esta aplicación mediante el Cliente de autenticación de tarjetas inteligentes para solicitar a los usuarios que se autentiquen antes de acceder a la pantalla de inicio de la impresora.
- **Correo electrónico seguro**: permite cifrar y firmar de forma digital los correos electrónicos enviados desde la impresora. Esta opción anula la función estándar de correo electrónico de la impresora.
- **Trabajos de impresión en espera protegidos**: permite a los usuarios autenticados ver o activar sus trabajos de impresión en espera.

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

Lista de comprobación de aptitud para la implementación

Asegúrese de que:

- ☐ Cuenta con los siguientes elementos instalados en la impresora:
  - Al menos 512 MB de RAM
  - Un lector de tarjetas inteligentes y su controlador
- ☐ Ha desactivado la aplicación de cuotas de dispositivos:
  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.
  3. Haga clic en **Aplicaciones** > **Cuotas de dispositivos** > **Detener**.

Cuenta con los siguientes elementos para configurar el Cliente de autenticación de tarjetas inteligentes:

- ☐ Certificado de autoridad certificadora (archivo .cer)
- ☐ Cuentas de Lightweight Directory Access Protocol (LDAP) y Active Directory®

  _____
- ☐ Dominio Kerberos, dominio y controlador de dominio

  _____
- ☐ Archivo de Kerberos (para varios dominios)

Configuración de los valores de la impresora

Es posible que necesite derechos de administrador para configurar los valores de la impresora.

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.

Ajuste del tiempo de espera de la pantalla

Para evitar el acceso no autorizado, puede limitar la cantidad de tiempo que un usuario permanece conectado a la impresora sin actividad.

1. En el servidor Embedded Web Server, haga clic en **Valores** > **Dispositivo** > **Preferencias**.
2. En el campo Tiempo de espera de pantalla, especifique el tiempo que debe pasar antes de que la pantalla entre en estado de inactividad y se cierre la sesión del usuario. Se recomienda configurar el valor en 30 segundos.
3. Haga clic en **Guardar**.

Instalación manual de certificados

Nota: Para descargar el certificado de CA automáticamente, consulte “Instalación automática de certificados” en la página 8.

Antes de configurar los valores de Kerberos o del controlador de dominio, instale el certificado de CA que se utiliza para la validación del controlador de dominio. Si desea utilizar la validación de cadenas para el certificado del controlador de dominio, instale la cadena de certificados completa. Cada certificado debe estar en un archivo PEM (.cer) independiente.

1. En Embedded Web Server, haga clic en **Valores** > **Seguridad** > **Administración de certificados**.
2. En la sección Gestionar certificados de CA, haga clic en **Cargar CA** y, a continuación, vaya al archivo PEM (.cer).

   Certificado de muestra:

   ```
   -----BEGIN CERTIFICATE-----
   MIIE1jCCA76gAwIBAgIQY6sV0KL3tIhBtlr4gHG85zANBgkqhkiG9w0BAQUFADBs
   …
   l3DTbPe0mnIbTq0iWqKEaVne1vvaDt52iSpEQyevwgUcHD16rFy+sOnCaQ==
   -----END CERTIFICATE-----
   ```

3. Haga clic en **Guardar**.

Instalación automática de certificados

1 En Embedded Web Server, haga clic en **Valores** > **Seguridad** > **Administración de certificados** > **Configurar actualización automática de certificados**.

2 Si se le solicita unirse a un dominio de Active Directory, haga clic en **Unirse al dominio** y, a continuación, escriba la información del dominio.

Nota: Asegúrese de que el dominio de Active Directory coincide con el dominio o nombre de dominio Kerberos que se utiliza en los valores de la tarjeta inteligente. Para obtener más información, consulte "Configuración de los valores de la tarjeta inteligente" en la página 14.

3 Seleccione **Activar Actualización automática**.

Nota: Si desea instalar el certificado de CA sin esperar a la hora de ejecución programada, seleccione **Obtener inmediatamente**.

4 Haga clic en **Guardar**.

Configuración de valores TCP/IP

1 Desde Embedded Web Server, haga clic en **Valores** > **Red/Puertos** > **TCP/IP**.

2 Haga lo siguiente:

- Si utiliza una dirección IP estática, escriba la dirección del servidor DNS. Si hay disponible un servidor DNS de seguridad, introduzca la dirección del servidor DNS de seguridad.
- Si la impresora está ubicada en un dominio diferente, escriba los otros dominios en el campo Orden de búsqueda de dominio. Utilice comas para separar varios dominios.

Nota: Utilice el nombre de dominio asignado a las estaciones de trabajo del usuario.

3 Haga clic en **Guardar**.

Definición de fecha y hora

Cuando utilice la autenticación Kerberos, asegúrese de que la diferencia de tiempo entre la impresora y el controlador de dominio no supera los cinco minutos. Puede actualizar manualmente los ajustes de fecha y hora o utilizar el protocolo de tiempo de red (NTP) para sincronizar automáticamente la hora con el controlador de dominio.

1 En Embedded Web Server, haga clic en **Valores** > **Dispositivo** > **Preferencias** > **Fecha y hora**.

Configuración manual

Nota: La configuración manual de la fecha y la hora desactiva NTP.

a En la sección Configurar, en el campo Ajustar manualmente fecha y hora", introduzca la fecha y la hora adecuadas.

b Seleccione el formato de la fecha, el formato de la hora y la zona horaria.

Nota: Si selecciona **(UTC+usuario) personalizado**, especifique los valores de desplazamiento de UTC (GMT) y el horario de verano o invierno (DST).

Configuración de NTP

a Desde la sección de protocolo de tiempo de red, seleccione **Activar NTP** y, a continuación, escriba la dirección IP o el nombre de host del servidor NTP.

b Si el servidor NTP requiere autenticación, en el menú Activar autenticación, seleccione la **clave MD5**.

c En función de su modelo de impresora, introduzca el ID de clave y la contraseña, o bien busque el archivo que contiene las credenciales de autenticación de NTP.

2 Haga clic en **Guardar**.

Configuración de los valores de la cuenta de red LDAP

Se necesita una cuenta de red LDAP para enviar correos electrónicos cifrados. Los certificados de cifrado para destinatarios se añaden y configuran desde el servidor LDAP. Póngase en contacto con el administrador del sistema para obtener más información.

Nota: Se necesita una cuenta de red Kerberos para crear una cuenta de red LDAP + GSSAPI.

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

2 En la sección Cuentas de red, haga clic en **Añadir método de inicio de sesión** > **LDAP**.

3 Seleccione **LDAP** o **LDAP + GSSAPI**.

4 En la sección Información general, configure lo siguiente:

- **Configurar nombre**: un nombre único para la cuenta de red LDAP.
- **Dirección del servidor**

  Nota: Asegúrese de que la dirección es la misma que la del controlador de dominio Cliente de autenticación de tarjetas inteligentes o que la dirección KDC en el archivo de configuración Kerberos.
- **Puerto del servidor**: si utiliza SSL, utilice el puerto **636**. De lo contrario, utilice el puerto **389**.

5 En la sección Credenciales de dispositivo, desactive la opción **Enlace LDAP anónimo** y, a continuación, escriba las credenciales de autenticación que se utilizan para conectar con el servidor LDAP.

6 Si el servidor LDAP requiere SSL, en la sección Opciones avanzadas, establezca Utilizar SSL/TLS en **SSL/TLS**.

7 En la sección Valores de libreta de direcciones, seleccione **Utilizar credenciales de usuario**.

8 Haga clic en **Guardar y comprobar**.

Protección del acceso a la impresora

Protección del acceso a la pantalla de inicio

Los usuarios deben autenticarse antes de acceder a la pantalla de inicio de la impresora.

Nota: Antes de comenzar, asegúrese de que la aplicación Personalización de pantalla está activada en la impresora. Para obtener más información, consulte la *Guía del administrador de Personalización de la pantalla*.

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. Expanda **Aplicaciones** y, a continuación, desactive **Presentación de diapositivas**, **Cambiar fondo de pantalla** y **Salvapantallas**; a continuación, haga clic en **Guardar**.
4. En la sección Métodos adicionales de inicio de sesión, haga clic en **Administrar permisos** junto a Tarjeta inteligente.
5. Seleccione un grupo cuyos permisos desee administrar.

   Nota: El grupo Todos los usuarios se crea de forma predeterminada. Cuando especifica grupos de Active Directory existentes en el campo de la lista de autorización de grupos, aparecen más nombres de grupos. Para obtener más información, consulte "Configuración de valores avanzados" en la página 15.
6. Despliegue **Aplicaciones**y, a continuación, seleccione **Pase de diapositivas**, **Cambiar fondo de pantalla**y **Salvapantallas**.
7. Haga clic en **Guardar**.

Protección del acceso a aplicaciones y funciones individuales

Es necesario que los usuarios se autentiquen antes de acceder a una aplicación o a una función integrada de la impresora.

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. Restrinja el acceso público a las aplicaciones o funciones que desee proteger. Haga lo siguiente:
   - Para Correo electrónico seguro, amplíe **Acceso a función**, desactive **Función de correo electrónico** y, a continuación, haga clic en **Guardar**.
   - Para Trabajos de impresión en espera protegidos, amplíe **Aplicaciones**, desactive **Trabajos de impresión en espera protegidos** y, a continuación, haga clic en **Guardar**.
   - Para otras aplicaciones o funciones, amplíe una o más categorías, desactive la aplicación o función y, a continuación, haga clic en **Guardar**.
4. En la sección Métodos adicionales de inicio de sesión, haga clic en **Administrar permisos** junto a Tarjeta inteligente.
5. Seleccione un grupo cuyos permisos desee administrar.

   Nota: El grupo Todos los usuarios se crea de forma predeterminada. Cuando especifica grupos de Active Directory existentes en el campo de la lista de autorización de grupos, aparecen más nombres de grupos. Para obtener más información, consulte "Configuración de valores avanzados" en la página 15.
6. Seleccione las aplicaciones o funciones cuyo acceso desee permitir a los usuarios autenticados. Haga lo siguiente:
   - Para Correo electrónico seguro, amplíe **Acceso a función** y, a continuación, seleccione **Función de correo electrónico**.
   - Para Trabajos de impresión en espera protegidos, amplíe **Aplicaciones** y, a continuación, seleccione **Trabajos de impresión en espera protegidos**.

- Para otras aplicaciones o funciones, amplíe una o varias categorías y, a continuación, seleccione la aplicación o función.

7 Haga clic en **Guardar**.

Mostrar las aplicaciones o funciones seguras en la pantalla de inicio

De forma predeterminada, las aplicaciones o funciones seguras están ocultas en la pantalla de inicio de la impresora.

1 En el servidor Embedded Web Server, haga clic en **Valores** > **Seguridad** > **Otros**.

2 En el menú Características protegidas, seleccione **Mostrar**.

3 Haga clic en **Guardar**.

Configuración de los valores del correo electrónico de la impresora

La aplicación anula la función de correo electrónico de la impresora.

Configuración de los valores de SMTP

1 En Embedded Web Server, haga clic en **Valores** > **Correo electrónico** > **Configurar correo electrónico**.

2 Configure lo siguiente:

- **Gateway SMTP primario**: la dirección IP o el nombre de host del servidor que se utiliza para enviar correos electrónicos.

  Nota: Para la autenticación Kerberos, utilice el nombre de host.
- **Puerto del gateway SMTP primario**
- **Gateway SMTP secundario**: la dirección IP o el nombre de host del servidor SMTP secundario o de copia de seguridad.
- **Puerto del gateway SMTP secundario**
- **Tiempo de espera SMTP**
- **Utilizar SSL/TLS**
- **Dirección de respuesta**
- **Autenticación del servidor SMTP**

  Notas:

  - Si se selecciona **Kerberos 5**, escriba el dominio Kerberos.
  - Si se selecciona **NTLM**, escriba el dominio NTLM.
  - Si el servidor SMTP requiere autenticación, pero no es compatible con Kerberos, escriba la dirección IP o el nombre de host en el campo Dirección de respuesta.

- **Correo electrónico iniciado por dispositivo**: se necesitan las credenciales del dispositivo para los correos electrónicos iniciados por dispositivo.

  Nota: Si se selecciona **Usar credenciales de dispositivo SMTP**, escriba las credenciales de autenticación.
- **Correo electrónico iniciado por usuario**: se necesitan las credenciales del usuario para los correos electrónicos iniciados por usuario.

  Nota: Si utiliza la autenticación Kerberos, seleccione **Usar ID y contraseña del usuario de la sesión**.

3 Haga clic en **Guardar**.

Configuración de los valores predeterminados de correo electrónico y digitalización

1 En Embedded Web Server, haga clic en **Valores** > **Correo electrónico** > **Valores predeterminados de correo electrónico**.

2 Configure los valores.

3 Si es necesario, ajuste los valores de imágenes avanzadas y los de los controles administrativos.

4 Haga clic en **Guardar**.

Configuración de envío de correo electrónico a dirección propia

Enviar correo electrónico a dirección propia permite a los usuarios enviar una copia del correo electrónico a su propia dirección de correo electrónico. Para obtener más información, consulte la *Guía del administrador de Enviar correo electrónico a dirección propia*.

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

Para la versión integrada de la aplicación

1 En Embedded Web Server, haga clic en **Valores** > **Correo electrónico** > **Valores predeterminados de correo electrónico** > **Controles de administrador**.

2 Seleccione **Limitar destinatarios de correos electrónicos**.

3 Haga clic en **Guardar**.

Para la aplicación Embedded Solutions Framework (eSF)

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

Aplicaciones > **Enviar correo electrónico a dirección propia** > **Configurar**

2 Seleccione **Activar**.

3 Haga clic en **Aplicar**.

Configuración de las aplicaciones

Configuración del Cliente de autenticación de tarjetas inteligentes

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

Configuración de los valores de la pantalla de inicio de sesión

Utilice los valores de la pantalla de inicio de sesión para establecer cómo desea que los usuarios inicien sesión en la impresora.

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

   Aplicaciones > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**

2. En la sección Pantalla de inicio de sesión, seleccione el tipo de inicio de sesión.
3. En el menú Modo de validación de usuario, seleccione el método para validar los certificados de usuario.
   - **Active Directory**: el certificado de usuario de la tarjeta inteligente se valida mediante la autenticación Kerberos. Este valor puede necesitar búsquedas de LDAP.
   - **Active Directory con acceso de invitado**: los usuarios que tienen tarjetas inteligentes, pero no están en Active Directory, pueden acceder a algunas de las funciones de la impresora. Se necesita un servidor de Protocolo de estado de certificados en línea (OCSP) configurado correctamente. Si la autenticación de Active Directory falla, la aplicación envía una consulta al servidor OCSP.
   - **Solo pin**: los usuarios solo pueden acceder a las aplicaciones o funciones que no requieren la autenticación Kerberos.
4. En el menú Validar tarjeta inteligente, seleccione el método para autenticar usuarios después de tocar una tarjeta inteligente.
5. Si es necesario, permita a los usuarios cambiar el método de inicio de sesión.
6. Haga clic en **Aplicar**.

Configuración de los valores del inicio de sesión manual

Para el inicio de sesión manual, la impresora utiliza el dominio predeterminado especificado en el archivo de configuración Kerberos. Si utiliza un dominio diferente, especifique el nombre de dominio en los valores de inicio de sesión manual.

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

   Aplicaciones > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**

2. En la sección Configuración de inicio de sesión manual, en el campo Dominios de inicio de sesión manual, escriba uno o más dominios.
3. Haga clic en **Aplicar**.

Configuración de los valores de la tarjeta inteligente

Nota: Asegúrese de que la conexión de red entre la impresora y el servidor de autenticación está configurada correctamente. Póngase en contacto con el administrador del sistema para obtener más información.

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

   Aplicaciones > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**

2. En la sección Configuración de tarjetas inteligentes, en el menú Información de Kerberos, seleccione una de las opciones siguientes:
   - **Utilizar el archivo de configuración Kerberos del dispositivo**: debe instalarse un archivo de configuración Kerberos de forma manual en la impresora. Haga lo siguiente:
     a. En Embedded Web Server, haga clic en **Valores** > **Seguridad** > **Métodos de inicio de sesión**.
     b. En la sección Cuentas de red, haga clic en **Añadir método de inicio de sesión** > **Kerberos**.
     c. En la sección Importar archivo Kerberos, busque el archivo krb5.conf adecuado.
     d. Si su red no utiliza la consulta de DNS inversa, en la sección Otros valores, seleccione **Desactivar búsquedas inversas de IP**.
     e. Haga clic en **Guardar y comprobar**.
   - **Utilizar configuración Kerberos simple**: se crea automáticamente un archivo Kerberos en la impresora. Especifique lo siguiente:
     - **Dominio**: el dominio debe escribirse en mayúsculas.
     - **Controlador de dominio**: utilice comas para separar varios valores. Los controladores de dominio se validarán en el orden en el que aparezcan.
     - **Nombre de dominio**: el nombre de dominio que debe asignarse al dominio Kerberos especificado en el campo Dominio. Utilice comas para separar varios dominios.

       Nota: El dominio distingue entre mayúsculas y minúsculas.
     - **Tiempo de espera**: introduzca un valor entre 3 y 30 segundos.

3. En el menú Validación del controlador de dominio, seleccione el método para validar el certificado de controlador de dominio.

   Nota: Antes de configurar este valor, asegúrese de que los certificados adecuados están instalados en la impresora. Para obtener más información, consulte “Instalación manual de certificados” en la página 7.
   - **Utilizar validación del certificado de dispositivo**: se utiliza el certificado de CA que está instalado en la impresora.
   - **Utilizar validación de cadenas de dispositivo**: se utiliza la cadena de certificados completa que está instalada en la impresora.
   - **Utilizar validación OCSP**: se utiliza el servidor OCSP. Toda la cadena del certificado debe estar instalada en la impresora. En la sección Protocolo de estado de certificados en línea (OCSP), configure lo siguiente:
     - **URL del respondedor**: la dirección IP o el nombre de host del respondedor o repetidor OCSP, y el número de puerto que se utiliza. Utilice comas para separar varios valores.
       Por ejemplo, **`http://x:y`**, donde ***x*** es la dirección IP o el nombre de host, e ***y*** es el número de puerto.
     - **Certificado del respondedor**: se utiliza el certificado X.509.

- **Tiempo de espera del respondedor**: introduzca un valor entre 5 y 30 segundos.
- **Permitir estado desconocido**: los usuarios pueden iniciar sesión incluso si el estado de uno o más certificados es desconocido.

4 Haga clic en **Aplicar**.

Configuración de valores avanzados

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

Aplicaciones > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**

2 En la sección Valores avanzados, seleccione un ID de usuario de sesión.

Nota: Algunas aplicaciones, como Trabajos de impresión en espera protegidos y Correo electrónico seguro, requieren un valor para el ID de usuario de sesión.

3 En el menú Dirección de correo electrónico, seleccione de dónde desea que la impresora recupere la dirección de correo electrónico del usuario.

4 Si es necesario, seleccione **Esperar a la información del usuario** para recuperar toda la información del usuario antes de que el usuario tenga permiso para acceder a la pantalla de inicio o una aplicación segura.

Si los valores siguientes están establecidos en la búsqueda de LDAP, seleccione esta opción.

- ID de usuario de sesión
- Dirección de correo electrónico

Si los valores siguientes no están vacíos, seleccione esta opción.

- Otros atributos de usuario
- Lista de autorizaciones de grupos

Nota: Si utiliza el inicio de sesión manual para Correo electrónico seguro, seleccione esta opción para almacenar la dirección de correo electrónico del usuario de la sesión de inicio. Para permitir que los usuarios de inicio de sesión manual puedan enviarse correos electrónicos a sí mismos, active la opción "Enviarme una copia" en los valores de correo electrónico de la impresora.

5 Si es necesario, seleccione **Utilizar SSL para información del usuario** para recuperar la información del usuario desde el controlador de dominio mediante una conexión SSL.

6 Si es necesario, en el campo Otros atributos de usuario, escriba otros atributos LDAP que deban añadirse a la sesión. Utilice comas para separar varios valores.

7 En Lista de autorizaciones de grupos, escriba los grupos de Active Directory que pueden acceder a aplicaciones o funciones. Utilice comas para separar varios valores.

Nota: Los grupos deben estar en el servidor LDAP.

8 Si DNS no está activado en su red, cargue un archivo hosts.

Escriba las asignaciones en el archivo de texto en el formato ***xy***, donde ***x*** es la dirección IP e ***y*** es el nombre de host. Puede asignar varios nombres de host a una dirección IP. Por ejemplo, **`255.255.255.255 NombreHost1 NombreHost2 NombreHost3`**.

No puede asignar varias direcciones IP a un nombre de host. Para asignar direcciones IP a grupos de nombres de host, introduzca cada dirección IP y sus nombres de host asociados en una línea independiente del archivo de texto.

Por ejemplo:

```
123.123.123.123 NombreHost1 NombreHost2
456.456.456.456 NombreHost3
```

9 Haga clic en **Aplicar**.

Configuración de Correo electrónico protegido

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

Configuración de los valores de Correo electrónico seguro

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

Aplicaciones > **Correo electrónico seguro** > **Configurar**

2 Configure los valores.

Notas:

- Para firmar un correo electrónico digitalmente, debe disponer de un certificado de firma digital válido y haber iniciado sesión con una tarjeta inteligente. Los certificados de firma solo están disponibles desde la tarjeta inteligente. Póngase en contacto con el administrador del sistema para obtener más información.
- Para recibir un correo electrónico cifrado, el destinatario debe estar en la libreta de direcciones del servidor LDAP y debe contar con un certificado de cifrado válido. Para obtener más información, consulte “Configuración de los valores de la cuenta de red LDAP” en la página 9.
- Para aplicar un marcado de seguridad a un correo electrónico, active el valor y, a continuación, escriba el texto que desea utilizar.
- 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 trabajos de impresión en espera protegidos

Restringir a los usuarios no autenticados para que no vean los trabajos en espera

La aplicación Trabajos en espera integrada permite ver todos los trabajos en espera en la impresora. Tras configurar Trabajos de impresión en espera protegidos, desmarque el icono Trabajos en espera de la pantalla de inicio de la impresora.

1 En Embedded Web Server, haga clic en **Configuración** > **Dispositivo** > **Iconos visibles en la pantalla de inicio**.

2 Desmarque **Trabajos en espera**.

3 Haga clic en **Guardar**.

Configuración de los ajustes de trabajos de impresión en espera protegidos

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

   Aplicaciones > **Trabajos de impresión en espera protegidos** > **Configurar**

2. En la sección Opciones de activación, establezca la configuración.
   - **Métodos de activación**: Permite especificar la manera en que los usuarios imprimen sus trabajos en espera.
   - **Mostrar trabajos de impresión ordenados por**: Permite especificar la forma en que se muestran los trabajos de impresión en la pantalla.
3. Haga clic en **Aplicar**.

Convertir los trabajos de impresión en trabajos de impresión en espera protegidos

1. En Embedded Web Server, haga clic en **Configuración** > **Seguridad** > **Configuración de impresión confidencial**.
2. Seleccione **Mantener todos los trabajos en reserva**.
3. Haga clic en **Guardar**.

Importación o exportación de archivos de configuración

Nota: 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. Realice uno de los procedimientos siguientes:
   - Haga clic en **Aplicaciones** > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**
   - Haga clic en **Aplicaciones** > **Correo electrónico seguro** > **Configurar**
   - Haga clic en **Aplicaciones** > **Trabajos de impresión en espera protegidos** > **Configurar**
2. Haga clic en **Importar** o **Exportar**.

Uso de las aplicaciones

Correo electrónico seguro

Envío de correo electrónico firmado y cifrado digitalmente

Notas:

- Al utilizar el inicio de sesión manual, configure los valores de autenticación de Cliente de autenticación de tarjetas inteligentes para recuperar toda la información de los usuarios. Para obtener más información, consulte la *Guía del administrador del Cliente de Autenticación de tarjetas inteligentes*.
- Para enviar un correo electrónico, asegúrese de que dispone de una dirección de correo electrónico válida asignada a su cuenta.

1. Inicie sesión en la impresora.
2. En la pantalla de inicio de la impresora, toque el icono de la aplicación.
3. Cargue un documento en la bandeja del alimentador automático de documentos (ADF) o sobre el cristal del escáner.
4. Escriba la dirección de correo electrónico del destinatario. Utilice comas para separar varias direcciones de correo electrónico.
5. Si es necesario, configure otros valores de correo electrónico y digitalización.
6. Toque **Enviar**.
7. Firme o cifre digitalmente el correo electrónico.

   Nota: Para firmar un correo electrónico digitalmente, debe disponer de un certificado de firma digital válido y haber iniciado sesión con una tarjeta inteligente. Los certificados de firma solo están disponibles desde la tarjeta inteligente. Póngase en contacto con el administrador del sistema para obtener más información.
8. Si es necesario, seleccione una opción de seguridad.
9. Toque **Enviar**.
10. Si se produce un error de cifrado, realice una de las siguientes acciones:
    - Para enviar un correo electrónico cifrado solo a los destinatarios con certificados de cifrado, seleccione **Enviar cifrado**.
    - Para enviar un correo electrónico sin cifrar a todos los destinatarios, seleccione **Enviar sin cifrar**.
11. Toque **Enviar**.

Trabajos de impresión en espera protegidos

Impresión de trabajos en espera

Notas:

- Asegúrese de convertir los trabajos de impresión estándar en trabajos de impresión en espera protegidos. Para obtener más información, consulte "Convertir los trabajos de impresión en trabajos de impresión en espera protegidos" en la página 17.
- Al utilizar la función de imprimir y poner en espera, asegúrese de que el controlador de impresión es compatible con ella. Para conocer más detalles, consulte *Ayuda del controlador de impresión*. Puede descargar el controlador universal de impresión Lexmark para Windows y el controlador de impresión para Macintosh en **www.lexmark.com**.

1. Con un documento abierto, haga clic en **Archivo** > **Imprimir**.
2. Seleccione una impresora.

   Nota: Si fuera necesario, ajuste la configuración de impresión.
3. Si fuera necesario, utilice la función de imprimir y poner en espera.
   a. Seleccione la función de imprimir y poner en espera.
      - Si es usuario de Windows, haga clic en **Propiedades**, **Preferencias**, **Opciones** o **Configuración** y, a continuación, haga clic en **Imprimir y poner en espera**.
      - Si es usuario de Macintosh, seleccione **Imprimir y poner en espera** en el menú de opciones.

   b. Seleccione el tipo de trabajo de impresión.
      - **Reservar**: Envía trabajos de impresión y los almacena en la memoria de la impresora para imprimirlos más tarde.
      - **Comprobar**: Imprime la primera copia de un trabajo complejo de varias copias para realizar una comprobación. Las copias restantes se retienen hasta que se imprimen o se cancelan.
      - **Repetir**: Imprime el trabajo inmediatamente y almacenar una copia en la memoria de la impresora para poder imprimir más copias más adelante.

      Nota: La aplicación de Trabajos de impresión en espera protegidos no es compatible con los trabajos de impresión confidenciales.

   c. Escriba el nombre de usuario desde el directorio LDAP asociado al trabajo de impresión.
4. Haga clic en **Aceptar** o **Imprimir**.
5. En la pantalla de inicio de la impresora, inicie sesión en su cuenta y, a continuación, toque el icono de la aplicación.

   Notas:

   - Asegúrese de que se utiliza la misma cuenta al iniciar sesión en la impresora y al enviar los trabajos de impresión.
   - Dependiendo de cómo esté configurada la aplicación, todos los trabajos de la cola de impresión se pueden imprimir automáticamente cuando toque el icono de la aplicación. Para obtener más información, consulte "Configuración de los ajustes de trabajos de impresión en espera protegidos" en la página 17.
6. Si se le pide, introduzca sus credenciales de autenticación.

7 Seleccione los trabajos que desea imprimir y, a continuación, especifique el número de copias que desea.

8 Pulse **Imprimir**.

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

Problemas de acceso

No se puede detectar el lector de tarjetas o la tarjeta inteligente

Realice alguna de estas acciones:

Asegúrese de que el lector de tarjetas está conectado correctamente a la impresora

Asegúrese de que el lector de tarjetas y la tarjeta inteligente son compatibles

Asegúrese de que el lector de tarjetas es compatible

Si desea acceder a una lista de lectores de tarjetas compatibles, consulte el archivo *Léame*.

Asegúrese de que el controlador adecuado del lector de tarjetas está instalado en la impresora

Póngase en contacto con el representante de Lexmark

El usuario está bloqueado.

Realice alguna de estas acciones:

Aumente el número permitido de intentos fallidos de conexión y la duración de bloqueo

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. Aumente el número permitido de intentos fallidos de conexión y de la duración de bloqueo.
3. Haga clic en **Guardar**.

   Nota: Los valores nuevos se aplican cuando haya transcurrido la duración de bloqueo.

Restablezca o sustituya la tarjeta inteligente

No se puede validar el PIN

Realice alguna de estas acciones:

Asegúrese de que el PIN que ha introducido es correcto

Póngase en contacto con el administrador del sistema.

No se puede iniciar sesión manualmente

Realice alguna de estas acciones:

Asegúrese de que el dominio especificado en la configuración Kerberos es correcto

Especifique los dominios en los valores de inicio de sesión manual

Para obtener más información, consulte “Configuración de los valores del inicio de sesión manual” en la página 13.

Póngase en contacto con el administrador del sistema.

La pantalla de inicio de la impresora no se bloquea

Realice alguna de estas acciones:

Asegúrese de que la opción Personalización de pantalla está activada

Para obtener más información, consulte la *Guía del administrador de Personalización de la pantalla*.

Acceso seguro a la pantalla de inicio

Para obtener más información, consulte “Protección del acceso a la pantalla de inicio” en la página 9.

Problemas de autenticación

Error de autenticación Kerberos

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 analizar el registro, configure el nivel de inicio de sesión en **No**.

Asegúrese de que el archivo de configuración está instalado en la impresora

- Si utiliza la configuración Kerberos simple para crear el archivo de configuración Kerberos, haga lo siguiente:
  1. Desde Embedded Web Server, desplácese a la página de configuración de la aplicación: **Aplicaciones** > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**
  2. En la sección Configuración Kerberos simple, asegúrese de que el dominio, el controlador de dominio, el nombre de dominio y los valores de tiempo de espera son correctos.
- Si utiliza el archivo de configuración Kerberos del dispositivo, haga lo siguiente:
  1. En Embedded Web Server, haga clic en **Valores** > **Seguridad** > **Métodos de inicio de sesión**.
  2. En la sección Cuentas de red, haga clic en **Kerberos** > **Ver archivo**.
  3. Si el archivo de configuración Kerberos no está instalado, en la sección Importar archivo Kerberos, busque el archivo krb5.conf adecuado.
  4. Haga clic en **Guardar y comprobar**.

Asegúrese de que el contenido y el formato del archivo de configuración son correctos

- Si utiliza la configuración Kerberos simple, modifique los valores de configuración Kerberos simple.
- Si utiliza el archivo de configuración Kerberos del dispositivo, modifique el archivo y vuelva a instalarlo.

Asegúrese de que el dominio Kerberos está escrito en mayúsculas

- Si utiliza la configuración Kerberos simple, haga lo siguiente:
  1. Desde Embedded Web Server, desplácese a la página de configuración de la aplicación: **Aplicaciones** > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**
  2. En la sección Configuración Kerberos simple, asegúrese de que el dominio es correcto y que se ha escrito en mayúsculas.
  3. Haga clic en **Aplicar**.

- Si utiliza el archivo de configuración Kerberos del dispositivo, haga lo siguiente:
  1. En Embedded Web Server, haga clic en **Valores** > **Seguridad** > **Métodos de inicio de sesión**.
  2. En la sección Cuentas de red, haga clic en **Kerberos** > **Ver archivo**.
  3. Asegúrese de que los dominios que hay en el archivo de configuración están escritos en mayúsculas.

Especifique el dominio del sistema operativo Microsoft® Windows®

- Si utiliza la configuración Kerberos simple, haga lo siguiente:
  1. Desde Embedded Web Server, desplácese a la página de configuración de la aplicación: **Aplicaciones** > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**
  2. En la sección Configuración Kerberos simple, en el campo Dominio, añada el dominio Windows en el campo Dominio.

     Por ejemplo, si el valor del campo Dominio es **`DomainName,.DomainName`** y el dominio Windows es **`x.y.z`**, cambie el valor del campo Dominio a **`DomainName,.DomainName,x.y.z`**.

     Nota: El dominio distingue entre mayúsculas y minúsculas.
  3. Haga clic en **Aplicar**.
- Si utiliza el archivo de configuración Kerberos del dispositivo, añada una entrada en la sección **`domain_realm`** del archivo. Escriba el nombre de dominio de Windows en mayúsculas y, a continuación, vuelva a instalar el archivo en la impresora.

Póngase en contacto con el representante de Lexmark

No se puede generar o leer la información del certificado de la tarjeta inteligente

Realice alguna de estas acciones:

Asegúrese de que la información del certificado en la tarjeta inteligente es correcta

Póngase en contacto con el representante de Lexmark

No se puede validar el controlador de dominio

Realice alguna de estas acciones:

Asegúrese de que el dominio, el controlador de dominio y el nombre de dominio en el archivo de configuración Kerberos son correctos

- Si utiliza la configuración Kerberos simple, haga lo siguiente:
  1. Desde Embedded Web Server, desplácese a la página de configuración de la aplicación: **Aplicaciones** > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**
  2. En la sección Configuración Kerberos simple, asegúrese de que el dominio, el controlador de dominio y el nombre de dominio son correctos.

- Si utiliza el archivo de configuración Kerberos del dispositivo, haga lo siguiente:
  1. En Embedded Web Server, haga clic en **Valores** > **Seguridad** > **Métodos de inicio de sesión**.
  2. En la sección Cuentas de red, haga clic en **Kerberos** > **Ver archivo**.
  3. Asegúrese de que el dominio, el controlador de dominio y el nombre de dominio son correctos.

Aumente el tiempo de espera del controlador de dominio

- Si utiliza la configuración Kerberos simple, haga lo siguiente:
  1. Desde Embedded Web Server, desplácese a la página de configuración de la aplicación:
     Aplicaciones > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**
  2. En la sección Configuración Kerberos simple, en el campo Tiempo de espera, introduzca un valor de 3 a 30 segundos.
  3. Haga clic en **Aplicar**.
- Si utiliza el archivo de configuración Kerberos del dispositivo, introduzca un valor de 3 a 30 segundos. Cuando haya terminado, vuelva a instalar el archivo en la impresora. Para obtener más información sobre la configuración de los valores de la tarjeta inteligente, consulte “Configuración de los valores de la tarjeta inteligente” en la página 14.

Asegúrese de que el controlador de dominio está disponible

Utilice comas para separar varios valores. Los controladores de dominio se validarán en el orden en el que aparezcan.

Asegúrese de que el puerto 88 no está bloqueado entre la impresora y el controlador de dominio

No se puede validar el certificado del controlador de dominio

Realice alguna de estas acciones:

Asegúrese de que los certificados que están instalados en la impresora son correctos

Para obtener más información, consulte “Instalación manual de certificados” en la página 7.

Asegúrese de que el método de validación del controlador de dominio está configurado correctamente

1. Desde Embedded Web Server, desplácese a la página de configuración de la aplicación:
   Aplicaciones > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**
2. En la sección Configuración de tarjetas inteligentes, en el menú Validación del controlador de dominio, seleccione el método de validación correcto.
3. Haga clic en **Aplicar**.

No se puede encontrar el dominio en el archivo de configuración Kerberos

Añadir o cambiar el dominio

- Si utiliza la configuración Kerberos simple, haga lo siguiente:
  1. Desde Embedded Web Server, desplácese a la página de configuración de la aplicación: **Aplicaciones** > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**
  2. En la sección Configuración Kerberos simple, en el campo Dominio, añada o cambie el dominio. El dominio debe escribirse en mayúsculas.

     Nota: La configuración Kerberos simple no admite varias entradas de dominios Kerberos. Si se necesitan varios dominios, instale un archivo de configuración Kerberos que contenga los dominios necesarios.
  3. Haga clic en **Aplicar**.
- Si utiliza el archivo de configuración Kerberos del dispositivo, añada o cambie el dominio en el archivo. El dominio debe escribirse en mayúsculas. Cuando haya terminado, vuelva a instalar el archivo en la impresora.

Controlador de dominio y relojes de dispositivo no sincronizados

Asegúrese de que la diferencia de tiempo entre la impresora y el controlador de dominio no supera cinco minutos

Para obtener más información, consulte “Definición de fecha y hora” en la página 8.

No se puede validar la cadena de certificados del controlador de dominio

Realice alguna de estas acciones:

Asegúrese de que todos los certificados necesarios para la validación de la cadena están instalados en la impresora y que la información es correcta

Para obtener más información, consulte “Instalación manual de certificados” en la página 7.

Asegúrese de que la cadena de certificados va desde el controlador de dominio hasta el certificado raíz (autoridad certificadora)

Asegúrese de que los certificados no han caducado

1. En Embedded Web Server, haga clic en **Valores** > **Seguridad** > **Administración de certificados**.
2. Asegúrese de que las fechas de Válido desde y Válido hasta no han caducado.

Permite a los usuarios iniciar sesión incluso cuando el estado de uno o varios de los certificados sea desconocido

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

   Aplicaciones > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**
2. En la sección Protocolo de estado de certificados en línea (OCSP), seleccione **Permitir estado desconocido**.
3. Haga clic en **Aplicar**.

Póngase en contacto con el representante de Lexmark

No se puede conectar al respondedor OCSP

Realice alguna de estas acciones:

Asegúrese de que la URL del respondedor OCSP es correcta

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

   Aplicaciones > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**
2. En la sección Protocolo de estado de certificados en línea (OCSP), asegúrese de que la URL del respondedor es correcta.
3. Haga clic en **Aplicar**.

Aumente el valor de tiempo de espera del respondedor

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

   Aplicaciones > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**
2. En la sección Protocolo de estado de certificados en línea (OCSP), en el campo Tiempo de espera del respondedor, introduzca un valor de 5 a 30.
3. Haga clic en **Aplicar**.

No se puede validar el certificado del controlador de dominio con el respondedor OCSP

Realice alguna de estas acciones:

Asegúrese de que la URL del respondedor OCSP y el certificado del respondedor están configurados correctamente

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

   Aplicaciones > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**
2. En la sección Protocolo de estado de certificados en línea (OCSP), en el campo URL del respondedor, especifique lo siguiente:
   - Dirección IP o nombre de host del respondedor o repetidor OCSP
   - Número de puerto utilizado

Por ejemplo, **http://*x*:*y***, donde ***x*** es la dirección IP e ***y*** es el número de puerto.

3 En el campo Certificado del respondedor, busque el certificado adecuado.

4 Haga clic en **Aplicar**.

Asegúrese de que el controlador de dominio devuelve el certificado correcto

Asegúrese de que el respondedor OCSP valida el certificado de controlador de dominio correcto

No se puede acceder a las aplicaciones y funciones individuales de la impresora

Realice alguna de estas acciones:

Permita el acceso seguro a las aplicaciones o funciones

Para obtener más información, consulte "Protección del acceso a aplicaciones y funciones individuales" en la página 10.

Si el usuario pertenece a un grupo de Active Directory, asegúrese de que el grupo tiene autorización para acceder a las aplicaciones y funciones

Problemas de Correo electrónico protegido

No se puede enviar correo electrónico mediante la aplicación

Asegúrese de que la aplicación Cuotas de dispositivos está desactivada

En Embedded Web Server, haga clic en **Aplicaciones** > **Cuotas de dispositivos** > **Detener**.

No se puede recuperar la dirección de correo electrónico del usuario

Realice alguna de estas acciones:

Asegúrese de que la función de correo electrónico de la impresora esté protegida

Para obtener más información, consulte "Protección del acceso a la impresora" en la página 9.

Asegúrese de que la dirección de correo electrónico del usuario se ha recuperado correctamente

1 Desde Embedded Web Server, desplácese a la página de configuración de Cliente de autenticación de tarjetas inteligentes:

Aplicaciones > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**

2 En la sección Valores avanzados, en el menú Dirección de correo electrónico, seleccione de dónde desea que la impresora recupere la dirección de correo electrónico del usuario.

3 Seleccione **Esperar a la información del usuario**.

4 Haga clic en **Aplicar**.

Póngase en contacto con el representante de Lexmark

No se puede recuperar el certificado de firma del usuario

Realice alguna de estas acciones:

Asegúrese de que un certificado de firma está disponible para el usuario

Instale el certificado de firma adecuado en la tarjeta inteligente del usuario.

Asegúrese de que los certificados se han recuperado correctamente

1 Desde Embedded Web Server, desplácese a la página de configuración de Cliente de autenticación de tarjetas inteligentes:

Aplicaciones > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**

2 En la sección Valores avanzados, seleccione **Esperar a la información del usuario**.

3 Haga clic en **Aplicar**.

Póngase en contacto con el representante de Lexmark

El certificado de firma no está disponible para el usuario

Pruebe una o varias de las acciones siguientes:

Envíe el correo electrónico sin una firma digital

Asegúrese de que un certificado de firma está disponible para el usuario

Instale el certificado de firma adecuado en la tarjeta inteligente del usuario.

Póngase en contacto con el administrador del sistema.

No se pueden recuperar certificados desde el servidor LDAP

Realice alguna de estas acciones:

Asegúrese de que todos los cables de red están conectados de forma segura y que los valores de red de la impresora están configurados correctamente

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

Asegúrese de que los valores del servidor y el cortafuegos están configurados para permitir la comunicación entre la impresora y el servidor LDAP en el puerto 389 o el puerto 636

Si usa SSL, utilice el puerto **636**. De lo contrario, utilice el puerto **389**.

Asegúrese de que la dirección del servidor LDAP contiene el nombre de host, no la dirección IP

Para obtener más información, consulte “Configuración de los valores de la cuenta de red LDAP” en la página 9.

Si el servidor LDAP requiere SSL, asegúrese de que los valores de SSL son correctos

Para obtener más información, consulte “Configuración de los valores de la cuenta de red LDAP” en la página 9.

Restrinja la base de búsqueda de LDAP al alcance mínimo posible que incluya a todos los usuarios necesarios

Asegúrese de que todos los atributos de LDAP son correctos

Póngase en contacto con el administrador del sistema.

No se puede cifrar el correo electrónico para uno o varios destinatarios

Realice alguna de estas acciones:

Envíe un correo electrónico sin cifrar a destinatarios sin un certificado de cifrado y un correo electrónico cifrado a destinatarios con un certificado de cifrado

Seleccione **Enviar a todos**. Para obtener más información, consulte “Envío de correo electrónico firmado y cifrado digitalmente” en la página 18.

Envíe un correo electrónico cifrado solo a los destinatarios con certificados de cifrado

Seleccione **Enviar cifrado**. Para obtener más información, consulte “Envío de correo electrónico firmado y cifrado digitalmente” en la página 18.

Envíe un correo electrónico sin cifrar a todos los destinatarios

Seleccione **Enviar sin cifrar**. Para obtener más información, consulte “Envío de correo electrónico firmado y cifrado digitalmente” en la página 18.

Póngase en contacto con el representante de Lexmark

No se puede conectar al servidor de correo electrónico

Realice alguna de estas acciones:

Asegúrese de que la impresora esté conectada a un dominio

Para obtener más información, consulte “Configuración de valores TCP/IP” en la página 8.

Asegúrese de que el valor de Autenticación del servidor SMTP es correcto

1. En Embedded Web Server, haga clic en **Valores** > **Correo electrónico** > **Configurar correo electrónico**.
2. En el menú Autenticación del servidor SMTP, realice una de las siguientes acciones:
   - Si el servidor SMTP requiere credenciales de usuario, seleccione **Kerberos 5**.
   - Si Kerberos no es compatible, seleccione **No se necesita autenticación**.
   - Si el servidor SMTP requiere autenticación, pero no es compatible con Kerberos, escriba la dirección IP o el nombre de host en el campo Dirección de respuesta.
3. Haga clic en **Guardar**.

Nota: Para obtener más información, consulte "Configuración de los valores de SMTP" en la página 11.

Si el servidor SMTP utiliza Kerberos, asegúrese de que los nombres de host de los gateway SMTP primario y secundario son correctos

1. En Embedded Web Server, haga clic en **Valores** > **Correo electrónico** > **Configurar correo electrónico**.
2. En los campos Gateway SMTP primario y Gateway SMTP secundario, escriba el nombre de host del gateway en lugar de la dirección IP.
3. Haga clic en **Guardar**.

Asegúrese de que los valores del servidor y el cortafuegos están configurados para permitir la comunicación entre la impresora y el servidor SMTP en el puerto 25

Asegúrese de que todos los cables de red están conectados de forma segura y que los valores de red de la impresora están configurados correctamente

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

Póngase en contacto con el administrador del sistema.

No se puede enviar una copia a uno mismo

Realice alguna de estas acciones:

Asegúrese de que introduce toda la información de usuario en la sesión de inicio

Asegúrese de que la impresora está configurada para recuperar toda la información del usuario

1. Desde Embedded Web Server, desplácese a la página de configuración de Cliente de autenticación de tarjetas inteligentes:

   Aplicaciones > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**
2. En la sección Valores avanzados, seleccione **Esperar a la información del usuario**.
3. Haga clic en **Aplicar**.

Asegúrese de que Enviar correo electrónico a dirección propia está configurado correctamente

Para obtener más información, consulte “Configuración de envío de correo electrónico a dirección propia” en la página 12.

Póngase en contacto con el representante de Lexmark

Problemas de Trabajos de impresión en espera protegidos

no se puede determinar el ID de usuario

Este error indica que el método de inicio de sesión en la cuenta local, la cuenta de red o el módulo de autenticación no está estableciendo el ID de usuario para la sesión. Realice alguna de estas acciones:

Asegúrese de que la aplicación está protegida

Para obtener más información, consulte “Configuración de los ajustes de trabajos de impresión en espera protegidos” en la página 17.

Asegúrese de que el ID de usuario de la sesión se ha especificado correctamente

Realice una de las siguientes acciones en Embedded Web Server:

Método de inicio de sesión con una cuenta local

1. Haga clic en **Configuración** > **Seguridad** > **Métodos de inicio de sesión**.
2. En la sección de cuentas locales, haga clic en el tipo de cuenta local y, a continuación, asegúrese de que la cuenta tiene un nombre de usuario.
3. Haga clic en **Guardar**.

Método de inicio de sesión con una cuenta de red

1. Haga clic en **Configuración** > **Seguridad** > **Métodos de inicio de sesión**.
2. En la sección de cuentas de la red, haga clic en la cuenta de la red y, a continuación, asegúrese de que la cuenta tiene el ID de usuario correcto. Póngase en contacto con el administrador del sistema para obtener más información.
3. Haga clic en **Guardar**.

Mediante un módulo de autenticación

1. Haga clic en **Aplicaciones**.
2. Seleccione el módulo de autenticación y, a continuación, haga clic en **Configurar**.
3. Especifique el valor adecuado para el ID de usuario de la sesión.
4. Haga clic en **Guardar** o **Aplicar**.

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 hay trabajos de impresión disponibles para el usuario

Realice alguna de estas acciones:

Asegúrese de que se enviaron trabajos a la impresora correcta y que no han caducado

El usuario puede haber enviado los trabajos a una impresora distinta o los trabajos pueden haberse eliminado automáticamente porque no se imprimieron a tiempo.

Asegúrese de que el ID de usuario de la sesión se ha especificado correctamente

Realice una de las siguientes acciones en Embedded Web Server:

Método de inicio de sesión con una cuenta local

1. Haga clic en **Configuración** > **Seguridad** > **Métodos de inicio de sesión**.
2. En la sección de cuentas locales, haga clic en el tipo de cuenta local y, a continuación, asegúrese de que la cuenta tiene un nombre de usuario.
3. Haga clic en **Guardar**.

Método de inicio de sesión con una cuenta de red

1. Haga clic en **Configuración** > **Seguridad** > **Métodos de inicio de sesión**.
2. En la sección de cuentas de la red, haga clic en la cuenta de la red y, a continuación, asegúrese de que la cuenta obtiene el ID de usuario correcto. Póngase en contacto con el administrador del sistema para obtener más información.
3. Haga clic en **Guardar**.

Mediante un módulo de autenticación

1. Haga clic en **Aplicaciones**.
2. Seleccione el módulo de autenticación y, a continuación, haga clic en **Configurar**.
3. Especifique el valor adecuado para el ID de usuario de la sesión.
4. Haga clic en **Guardar** o **Aplicar**.

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.

Problemas de LDAP

error de búsquedas LDAP

Realice alguna de estas acciones:

Asegúrese de que los valores del servidor y el cortafuegos están configurados para permitir la comunicación entre la impresora y el servidor LDAP en el puerto 389 y el puerto 636

Si no se utiliza en su red la consulta de DNS inversa, desactívela en los valores de Kerberos

1. En el servidor Embedded Web Server, haga clic en **Configuración** > **Seguridad**.
2. En la sección Cuentas de red, haga clic en **Kerberos**.
3. En la sección Otros valores, seleccione **Desactivar búsquedas inversas de IP**.
4. Haga clic en **Guardar y comprobar**.

Si el servidor LDAP requiere SSL, active SSL para las búsquedas de LDAP

1. Desde Embedded Web Server, desplácese a la página de configuración de la aplicación: **Aplicaciones** > **Cliente de autenticación de tarjetas inteligentes** > **Configurar**
2. En la sección Valores avanzados, seleccione **Utilizar SSL para información del usuario**.
3. Haga clic en **Aplicar**.

Restrinja la base de búsqueda de LDAP al alcance mínimo posible que incluya a todos los usuarios necesarios

Asegúrese de que todos los atributos de LDAP son correctos

Error de licencia

Póngase en contacto con el representante de Lexmark

Avisos

Nota sobre la edición

Agosto de 2017

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

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

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

Para obtener asistencia técnica de Lexmark, visite **http://support.lexmark.com**.

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

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.

Microsoft, Windows y Active Directory son marcas comerciales registradas o marcas comerciales del grupo de compañías Microsoft en los Estados Unidos y en otros países.

Las otras marcas comerciales pertenecen a sus respectivos propietarios.

Índice

T

U

V