Cliente de autenticación de tarjetas inteligentes

Versión 2,1

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 los idiomas portugués de Brasil, finés, francés, alemán, italiano, chino simplificado y español.

Enero de 2016

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

Descripción general

Utilice la aplicación para 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.

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

Lista de comprobación de aptitud para la implementación

Asegúrese de que:

- ☐ Hay al menos 512 MB de RAM instalada en la impresora.
- ☐ Se ha instalado un lector de tarjetas inteligentes y su controlador en la impresora.

Dispone de lo siguiente para configurar la aplicación:

- ☐ 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 7.

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 11.

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**.

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 12.

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

Los usuarios deben autenticarse antes de acceder a una aplicación o una función 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 Expanda una o más categorías, borre las aplicaciones o funciones que desea proteger 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 12.

6 Expanda una o más categorías y, a continuación, seleccione las aplicaciones o funciones a las que desea que los usuarios autenticados puedan acceder.

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 la aplicación

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 6.
   - **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**.

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:

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

2 Haga clic en **Importar** o **Exportar**.

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 10.

Póngase en contacto con el administrador del sistema.

Se ha cerrado la sesión del usuario inmediatamente después de iniciarse la sesión

Aumente el valor de tiempo de espera de la pantalla

Para obtener más información, consulte "Ajuste del tiempo de espera de la pantalla" en la página 6.

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 8.

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 11.

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 6.

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 7.

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 6.

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 8.

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 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.

Licencia GNU Lesser General Public License

Vea la licencia GNU Lesser General Public License en Internet en **http://www.gnu.org/licenses/lgpl.html**.

Additional copyrights

This product includes software developed by:

Índice