Autenticação por SmartCard

Guia do administrador

Agosto de 2017

www.lexmark.com

Conteúdo

Histórico de alterações

Agosto de 2017

- Instruções adicionadas sobre como alterar o método de login.
- Instruções adicionadas sobre desativar o aplicativo de Gestão de Quotas.
- Suporte adicionado para português brasileiro, finlandês, francês, alemão, italiano, chinês simplificado e espanhol.

Julho de 2016

- Instruções adicionadas sobre o aplicativo de como configurar e-mail para si mesmo.

Janeiro de 2016

- Documento inicial lançado para produtos multifuncionais com tela sensível ao toque do tipo tablet.

Visão geral

Autenticação por SmartCard é uma coleção de aplicativos usados para o acesso seguro a impressoras e suas funções. Os aplicativos permitem que você faça login em uma impressora manualmente ou use um smart card e, em seguida, envie e-mails e libere trabalhos de impressão de maneira segura. Você também poderá definir outras configurações de segurança em um aplicativo, como assinatura e criptografia de e-mail.

O pacote de Autenticação por SmartCard inclui os aplicativos a seguir:

- **Cliente de Autenticação por Smart Card** — Permite proteger o acesso às impressoras solicitando que os usuários façam login usando um smart card ou um nome de usuário e senha. Você pode proteger o acesso à tela de início da impressora ou os aplicativos e as funções individuais. O aplicativo também fornece opções de autenticação Kerberos e um ingresso Kerberos que pode ser usado para proteger outros aplicativos.
- **Driver do smart card**—Permite que a impressora se comunique com um smart card suportado.
- **Personalização da exibição**—Permite que você carregue imagens na impressora. É possível usar as imagens para criar apresentações de slides personalizadas ou para definir o papel de parede e o protetor de tela da impressora. Proteja este aplicativo usando o cliente de Autenticação por SmartCard para solicitar que os usuários autentiquem antes de poderem acessar a tela de início da impressora.
- **Proteger e-mail**—Permite que você assine digitalmente e criptografe e-mails enviados da impressora. O aplicativo substitui a função padrão de e-mail da impressora.
- **Proteção de trabalhos de impressão suspensos**— Permite que os usuários autenticados visualizem e liberem seus trabalhos de impressão suspensos.

Este documento oferece informações sobre como configurar, utilizar e solucionar problemas dos aplicativos.

Lista de verificação da prontidão de implementação

Verifique se:

- ☐ Você instalou os seguintes aplicativos da impressora:
  - No mínimo, 512MB de RAM
  - Um leitor de smart card e seu driver
- ☐ Você desativou o aplicativo de Gestão de Quotas:
  1. Obtenha o endereço IP da impressora. Execute um dos seguintes procedimentos:
     - Localize o endereço IP na tela inicial da impressora.
     - Na tela inicial da impressora, toque em **Configurações** > **Rede/Portas** > **Visão geral da rede**.
  2. Abra o navegador da Web e digite o endereço IP da impressora.
  3. Clique em **Aplicativos** > **Cotas do dispositivo** > **Parar**.

Você tem o seguinte para configurar o Cliente de Autenticação por SmartCard:

- ☐ Autoridade de certificações (.cer file)
- ☐ Contas do Lightweight Directory Access Protocol (LDAP) e do Active Directory®

  _____
- ☐ Domínio e controlador do domínio do Kerberos

  _____
- ☐ Arquivo do Kerberos (para vários domínios)

Configuração das definições da impressora

Talvez sejam necessários direitos administrativos para configurar as definições da impressora.

Acesso ao Embedded Web Server

1. Obtenha o endereço IP da impressora. Execute um dos seguintes procedimentos:
   - Localize o endereço IP na tela inicial da impressora.
   - Na tela inicial da impressora, toque em **Configurações** > **Rede/Portas** > **Visão geral da rede**.
2. Abra o navegador da Web e digite o endereço IP da impressora.

Configuração do tempo limite da tela

Para evitar acesso não autorizado, é possível limitar o tempo que o usuário permanece conectado à impressora sem atividade.

1. No Embedded Web Server, clique em **Definições** > **Dispositivo** > **Preferências**.
2. No campo Tempo Limite da Tela, especifique o tempo até que a tela fique ociosa e o usuário seja desconectado. Recomendamos configurar o valor para 30 segundos.
3. Clique em **Salvar**.

Instalação manual de certificados

Nota: Para fazer o download automático do certificado CA, consulte " Instalação automática de certificados" na página 8.

Antes de configurar as definições do Kerberos ou do controlador de domínio, instale o certificado CA usado para validação do controlador de domínio. Se desejar usar a validação de cadeia para o certificado do controlador de domínio, instale toda a cadeia de certificados. Cada certificado deve estar em um arquivo PEM (.cer) separado.

1. No Embedded Web Server, clique em **Configurações** > **Segurança** > **Gerenciamento de Certificados**.
2. Na seção Gerenciar Certificados CA, clique em **Carregar CA** e, em seguida, navegue para o arquivo PEM (.cer).

   Certificado de exemplo:

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

3. Clique em **Salvar**.

Instalação automática de certificados

1 No Embedded Web Server, clique em **Configurações** > **Segurança** > **Gerenciamento de Certificados** > **Configurar Atualização Automática de Certificado**.

2 Se for solicitado que você se associe a um domínio do Active Directory, clique em **Associar a um Domínio** e insira as informações do domínio.

Nota: Verifique se o domínio do Active Directory corresponde ao realm ou ao domínio do Kerberos utilizado nas configurações do SmartCard. Para obter mais informações, consulte " Configuração das definições de SmartCard" na página 14.

3 Selecione **Ativar Atualização Automática**.

Nota: Se desejar instalar o certificado CA sem aguardar o tempo de execução programado, selecione **Obter Imediatamente**.

4 Clique em **Salvar**.

Definindo configurações de TCP/IP

1 No Embedded Web Server, clique em **Configurações** > **Rede/Portas** > **TCP/IP**.

2 Tente um dos seguintes métodos:

- Caso esteja usando um endereço IP estático, insira o endereço de servidor DNS. Se um servidor DNS de backup estiver disponível, digite o endereço do servidor DNS de backup.
- Se a impressora estiver localizada em um domínio diferente, insira os outros domínios no campo Ordem de Pesquisa de Domínio. Use vírgulas para separar vários domínios.

Nota: Use o nome de domínio atribuído a estações de trabalho de usuário.

3 Clique em **Salvar**.

Configuração de data e hora

Ao usar a autenticação do Kerberos, certifique-se de que a diferença de tempo entre a impressora e o controlador de domínio não ultrapasse cinco minutos. É possível atualizar manualmente as configurações de data e hora ou usar o Protocolo de Tempo da Rede (NTP) para sincronizar o horário com o controlador de domínio automaticamente.

1 No Embedded Web Server, clique em **Configurações** > **Dispositivo** > **Preferências** > **Data e Hora**.

Configurando manualmente

Nota: Configurar a data e a hora manualmente desativa o NTP.

a Na seção Configurar, no campo "Definir Data e Hora Manualmente", insira a data e a hora adequadas.

b Selecione o formato de data, o formato da hora e o fuso horário.

Nota: Se você selecionar **(UTC+usuário) Personalizar**, especifique os valores de deslocamento para UTC (GMT) e DST.

Configurando o NTP

a Na seção Protocolo de Tempo da Rede, selecione **Ativar NTP** e digite o endereço IP ou nome do host do servidor NTP.

b Se o servidor NTP exigir autenticação, então, no menu Ativar Autenticação, selecione **Chave MD5**.

c Dependendo do modelo da impressora, insira o ID de chave e a senha, ou navegue até o arquivo que contém as credenciais de autenticação NTP.

2 Clique em **Salvar**.

Configuração de definições de conta de rede LDAP

Uma conta de rede LDAP é necessária para enviar e-mails criptografados. Certificados de criptografia para destinatários são adicionados e configurados a partir do servidor LDAP. Para obter mais informações, entre em contato com o administrador do sistema.

Nota: É necessária uma conta de rede do Kerberos para criar uma conta de rede LDAP + GSSAPI.

1 No Embedded Web Server, clique em **Configurações** > **Segurança** > **Métodos de login**.

2 Na seção Contas de Rede, clique em **Adicionar Método de Login** > **LDAP**.

3 Selecione **LDAP** ou **LDAP + GSSAPI**.

4 Na seção Informações Gerais, configure o seguinte:

- **Configurar Nome**—Um nome exclusivo para a conta de rede LDAP.
- **Endereço do servidor**

  Nota: Verifique se o endereço é o mesmo que o endereço do controlador de domínio do Cliente de Autenticação por SmartCard ou endereço de KDC no arquivo de configuração do Kerberos.
- **Porta do Servidor**—Se você estiver usando SSL, utilize a porta **636**. Caso contrário, utilize a porta **389**.

5 Na seção Credenciais do Dispositivo, desmarque **Associação LDAP Anônima** e insira as credenciais de autenticação utilizadas para conexão com o servidor LDAP.

6 Se o servidor LDAP pedir SSL, na seção Opções Avançadas, defina Usar SSL/TLS para **SSL/TLS**.

7 Na seção Configuração do Catálogo de Endereços, selecione **Usar credenciais de usuário**.

8 Clique em **Salvar e Verificar**.

Protegendo o acesso à impressora

Protegendo o acesso à tela inicial

Os usuários devem ser autenticados antes de poderem acessar a tela inicial da impressora.

Nota: Antes de começar, certifique-se de que o aplicativo Personalização da Exibição esteja ativado na impressora. Para obter mais informações, consulte o *Guia do administrador de Personalização da exibição*.

1 No Embedded Web Server, clique em **Configurações** > **Segurança** > **Métodos de login**.

2 Na seção Pública, clique em **Gerenciar permissões**.

3 Expanda **Aplicativos**, desmarque as opções **Apresentação de Slides**, **Alterar Papel de Parede** e **Proteção de Tela**; depois, clique em **Salvar**.

4 Na seção Métodos de Login Adicionais, clique em **Gerenciar Permissões** ao lado de SmartCard.

5 Selecione um grupo cujas permissões você queira gerenciar.

Nota: O grupo Todos os Usuários é criado por padrão. Mais nomes de grupo serão exibidos ao especificar grupos do Active Directory existentes no campo Lista de Autorização de Grupo. Para obter mais informações, consulte " Configuração de definições avançadas" na página 15.

6 Expanda **Aplicativos** e, em seguida, selecione as opções **Apresentação de slides**, **Alterar papel de parede** e **Proteção de tela**.

7 Clique em **Salvar**.

Proteger o acesso a funções e aplicativos individuais

Os usuários são solicitados a fazer a autenticação antes de acessar um aplicativo ou uma função incorporada da impressora.

1 No Embedded Web Server, clique em **Configurações** > **Segurança** > **Métodos de login**.

2 Na seção Pública, clique em **Gerenciar permissões**.

3 Restrinja o acesso público aos aplicativos ou funções que deseja proteger. Tente um dos seguintes métodos:

- Para Proteger e-mail, expanda **Acesso a funções**, desmarque **Função de e-mail** e, em seguida, clique em **Salvar**.
- Para Proteger trabalhos de impressão retidos, expanda **Aplicativos**, desmarque **Proteger trabalhos de impressão retidos** e, em seguida, clique em **Salvar**.
- Para outros aplicativos ou funções, expanda uma ou mais categorias, limpe o aplicativo ou a função e, em seguida, clique em **Salvar**.

4 Na seção Métodos de login adicionais, clique em **Gerenciar permissões** ao lado de Smart Card.

5 Selecione um grupo cujas permissões você queira gerenciar.

Nota: O grupo Todos os Usuários é criado por padrão. Mais nomes de grupos aparecem quando você especifica os grupos do Active Directory existentes no campo Lista de autorização de grupo. Para obter mais informações, consulte " Configuração de definições avançadas" na página 15.

6 Selecione os aplicativos ou as funções cujo acesso você queira conceder somente a usuários autenticados. Tente um dos seguintes métodos:

- Para Proteger e-mail, expanda **Acesso a funções** e, em seguida, selecione **Função de e-mail**.
- Para Proteger trabalhos de impressão retidos, expanda **Aplicativos** e, em seguida, clique em **Proteger trabalhos de impressão retidos, expanda**.
- Para outros aplicativos e funções, expanda uma ou mais categorias e, em seguida, selecione o aplicativo ou a função.

7 Clique em **Salvar**.

Mostrando aplicativos ou funções protegidos na tela inicial

Por padrão, os aplicativos ou funções protegidos estão ocultos da tela inicial da impressora.

1. No Embedded Web Server, clique em **Definições** > **Segurança** > **Variadas**.
2. No menu de Recursos Protegidos, selecione **Mostrar**.
3. Clique em **Salvar**.

Definição das configurações de e-mail da impressora

O aplicativo substitui a função de e-mail da impressora.

Configurando definições SMTP

1. No Embedded Web Server, clique em **Configurações** > **E-mail** > **Configuração de E-mail**.
2. Configure o seguinte:
   - **Gateway SMTP Primário**—O endereço IP ou o nome de host do servidor utilizado para enviar e-mails.

     Nota: Para autenticação de Kerberos, use o nome do host.
   - **Porta do gateway SMTP primário**
   - **Gateway SMTP Secundário**—O endereço IP ou o nome de host do servidor SMTP secundário ou de backup.
   - **Porta do gateway SMTP secundário**
   - **Tempo limite SMTP**
   - **Usar SSL/TLS**
   - **Endereço de resposta**
   - **Autenticação de servidor SMTP**

     Notas:

     - Se **Kerberos 5** estiver selecionado, insira o realm do Kerberos.
     - Se **NTLM** estiver selecionado, insira o domínio NTLM.
     - Se o servidor SMTP exigir autenticação, mas não suportar Kerberos, então, no campo Endereço de Resposta, digite o endereço IP ou o nome do host da impressora.
   - **E-mail Iniciado por Dispositivo**—As credenciais do dispositivo são necessárias para e-mails iniciados por dispositivo.

     Nota: Se **Usar Credenciais do Dispositivo SMTP** estiver selecionado, insira as credenciais de autenticação.
   - **E-mail Iniciado por Usuário**—As credenciais do usuário são necessárias para e-mails iniciados por usuário.

     Nota: Caso esteja usando autenticação do Kerberos, selecione **Utilizar Senha e ID do Usuário de Sessão**.
3. Clique em **Salvar**.

Configuração de definições padrão de e-mail e digitalização

1. No Embedded Web Server, clique em **Configurações** > **E-mail** > **Padrões do E-mail**.
2. Configure as definições.
3. Se necessário, ajuste Advanced Imaging e as configurações de controles administrativos.
4. Clique em **Salvar**.

Configuração de Email para si mesmo

Email para si mesmo permite que os usuários enviem uma cópia do e-mail para seus endereços de e-mail. Para obter mais informações, consulte o *Guia do Administrador do Email para si mesmo*.

Dependendo do modelo da sua impressora, faça o seguinte:

Para a versão integrada do aplicativo

1. No Embedded Web Server, clique em **Configurações** > **E-mail** > **Padrões do E-mail** > **Controles de Administrador**.
2. Selecione **Limitar Destinatários de E-mail**.
3. Clique em **Salvar**.

Para o aplicativo Framework de Soluções Embarcadas (eSF)

1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo:

   Aplicativos > **Email para si mesmo** > **Configurar**
2. Selecione **Ativar**.
3. Clique em **Aplicar**.

Como configurar os aplicativos

Como configurar o Cliente de autenticação do Smart Card

Talvez sejam necessários direitos administrativos para configurar o aplicativo.

Configurando definições da tela de login

Use as configurações da tela de login para definir como deseja que os usuários façam login na impressora.

1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo:

   Aplicativos > **Cliente de Autenticação por SmartCard** > **Configurar**

2. Na seção Tela de Login, selecione o tipo de login.
3. No menu Modo de Validação de Usuário, selecione o método para validar certificados do usuário.
   - **Active Directory**—O certificado de usuário no SmartCard é validado utilizando a autenticação do Kerberos. Essa configuração pode exigir pesquisas de LDAP.
   - **Active Directory com acesso de convidado**—Os usuários que possuem SmartCards mas não estão no Active Directory podem acessar algumas das funções da impressora. Um servidor de Protocolo de Status de Certificados On-line (OCSP) devidamente configurado é necessário. Caso a autenticação de Active Directory falhe, o aplicativo consultará o servidor OCSP.
   - **Somente Pin**—Os usuários podem acessar somente aplicativos ou funções que não exigem autenticação do Kerberos.
4. No menu Validar SmartCard, selecione o método para autenticar os usuários após utilizar um SmartCard.
5. Se necessário, permita que os usuários alterem o método de login.
6. Clique em **Aplicar**.

Configurando definições de login manual

Para login manual, a impressora usa o domínio padrão especificado no arquivo de configuração do Kerberos. Se você usar um domínio diferente, especifique o nome do domínio nas configurações de login manual.

1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo:

   Aplicativos > **Cliente de Autenticação por SmartCard** > **Configurar**

2. Na seção Configuração de Login Manual, no campo Domínios de Login Manual, insira um ou mais domínios.
3. Clique em **Aplicar**.

Configuração das definições de SmartCard

Nota: Verifique se a conexão de rede entre a impressora e o servidor de autenticação está corretamente configurada. Para obter mais informações, entre em contato com o administrador do sistema.

1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo:

   Aplicativos > **Cliente de Autenticação por SmartCard** > **Configurar**

2. Na seção Configuração do SmartCard, no menu Informações do Kerberos, selecione uma das opções seguintes:
   - **Usar arquivo de configuração do Kerberos do dispositivo**—Um arquivo de configuração do Kerberos deve ser instalado na impressora manualmente. Faça o seguinte:
     a. No Embedded Web Server, clique em **Configurações** > **Segurança** > **Métodos de login**.
     b. Na seção Contas de rede, clique em **Adicionar método de login** > **Kerberos**.
     c. Na seção Importar Arquivo do Kerberos, navegue até o arquivo krb5.conf adequado.
     d. Caso sua rede não utilize a opção de pesquisa inversa de DNS, na seção Configurações Variadas, selecione **Desativar Pesquisas de IP Inversas**.
     e. Clique em **Salvar e Verificar**.
   - **Usar configuração do Kerberos simples**—Um arquivo do Kerberos é criado na impressora automaticamente. Especifique o seguinte:
     - **Realm**—O realm deve ser digitado em letras maiúsculas.
     - **Controlador do Domínio**—Use vírgulas para separar vários valores. Os controladores de domínio são validados na ordem listada.
     - **Domínio**—Especifique o domínio que deve ser mapeado para o realm do Kerberos especificado no campo Realm. Use vírgulas para separar vários domínios.

       Nota: O domínio diferencia maiúsculas e minúsculas.
     - **Tempo limite**—Insira um valor de 3 a 30 segundos.

3. No menu Validação do Controlador de Domínio, selecione o método para validação do certificado do controlador de domínio.

   Nota: Antes de configurar essa definição, verifique se os certificados apropriados estão instalados na impressora. Para obter mais informações, consulte " Instalação manual de certificados" na página 7.
   - **Usar validação de certificado do dispositivo**—O certificado CA instalado na impressora é usado.
   - **Usar validação de cadeia do dispositivo**—Toda a cadeia de certificados instalados na impressora é usada.
   - **Usar validação de OCSP**—O servidor OCSP é usado. A cadeia inteira do certificado deve estar instalada na impressora. Na seção Protocolo de Status de Certificados On-line (OCSP), configure o seguinte:
     - **URL de Resposta**—O endereço IP ou nome do host do mecanismo de resposta/repetição OCSP e o número da porta usada. Use vírgulas para separar vários valores.
       Por exemplo, **`http://x:y`**, onde ***x*** é o endereço IP ou nome do host e ***y*** é o número da porta.
     - **Certificado de Resposta**—O certificado X.509 é usado.
     - **Tempo Limite de Resposta**—Digite um valor de 5 a 30 segundos.
     - **Permitir Status Desconhecido**—Os usuários podem fazer login mesmo quando o status de um ou mais certificados é desconhecido.

4. Clique em **Aplicar**.

Configuração de definições avançadas

1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo:

   Aplicativos > **Cliente de Autenticação por SmartCard** > **Configurar**

2. Na seção Configurações Avançadas, selecione um ID do usuário de sessão.

   Nota: Alguns aplicativos, como Trabalhos Seguros Retidos e E-mail Seguro, exigem um valor para o ID do usuário da sessão.

3. No menu Endereço de E-mail "De", selecione onde a impressora recupera o endereço de e-mail do usuário.

4. Se necessário, selecione **Aguardar informações do usuário** para obter todas as informações do usuário antes que este possa acessar a tela inicial ou um aplicativo seguro.

   Caso as configurações seguintes estejam definidas para Pesquisa de LDAP, selecione essa opção.

   - ID do Usuário de Sessão
   - Endereço de E-mail "De"

   Caso as configurações seguintes não estejam vazias, selecione essa opção.

   - Outros os Atributos do Usuário
   - Lista de Autorização de Grupo

   Nota: Caso esteja usando login manual para E-mail Seguro, marque esta opção para armazenar o endereço de e-mail do usuário na sessão de login. Para permitir que usuários de login manual enviem e-mails para si mesmos, ative "Enviar-me uma cópia" nas configurações de e-mail da impressora.

5. Se necessário, selecione **Usar SSL para Informações do Usuário** para recuperar as informações de usuário do controlador do domínio utilizando uma conexão SSL.

6. Se necessário, no campo Outros Atributos do Usuário, insira outros atributos de LDAP que precisem ser adicionados à sessão. Use vírgulas para separar vários valores.

7. Na Lista de Autorização de Grupo, insira os grupos do Active Directory que podem acessar aplicativos ou funções. Use vírgulas para separar vários valores.

   Nota: Os grupos devem estar no servidor LDAP.

8. Se DNS não estiver ativado em sua rede, carregue um arquivo de hosts.

   Digite os mapeamentos no arquivo de texto no formato ***xy***, onde ***x*** é o endereço IP e ***y*** é o nome do host. Você pode atribuir vários nomes de host a um endereço IP. Por exemplo, **`255.255.255.255 Nomedohost1 Nomedohost2 Nomedohost3`**.

   Não é possível atribuir vários endereços IP a um nome de host. Para atribuir endereços IP a grupos de nomes de host, digite cada endereço IP e os nomes de host associados em uma linha separada do arquivo de texto.

   Por exemplo:

   ```
   123.123.123.123 Nomedohost1 Nomedohost2
   456.456.456.456 Nomedohost3
   ```

9. Clique em **Aplicar**.

Configuração de Proteger e-mail

Talvez sejam necessários direitos administrativos para configurar o aplicativo.

Configuração das definições de E-mail Seguro

1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo:

   Aplicativos > **E-mail Seguro** > **Configurar**

2. Configure as definições.

   Notas:

   - Para assinar um e-mail digitalmente, você deve ter um certificado de assinatura digital válido e ter feito login usando um SmartCard. Certificados de assinatura estão disponíveis somente no SmartCard. Para obter mais informações, entre em contato com o administrador do sistema.
   - Para receber e-mails criptografados, o destinatário deve estar no catálogo de endereços do servidor LDAP e deve ter um certificado de criptografia válido. Para obter mais informações, consulte " Configuração de definições de conta de rede LDAP" na página 9.
   - Para aplicar a marca de segurança a um e-mail, ative a configuração e, em seguida, digite o texto que deseja usar.
   - Para obter mais informações em cada configuração, consulte a ajuda do mouse.

3. Clique em **Aplicar**.

Configuração da proteção de trabalhos de impressão suspensos

Restringindo os usuários não autenticados de visualizar trabalhos suspensos

O aplicativo integrado de trabalhos suspensos pode ser utilizado para exibir todos os trabalhos suspensos na impressora. Depois de configurar a Proteção de trabalhos de impressão suspensos, remova o ícone Trabalhos suspensos da tela inicial da impressora.

1. No Servidor da Web incorporado, clique em **Configurações** > **Dispositivo** > **Ícones visíveis da tela inicial**.
2. Excluir **Trabalhos suspensos**.
3. Clique em **Salvar**.

Configurar as definições de Proteção de trabalhos de impressão suspensos

1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo:

   Aplicativos > **Proteção de trabalhos de impressão suspensos** > **Configurar**

2. Na seção Opções de liberação, configure as definições.
   - **Método de liberação** - Especifique como os usuários imprimem seus trabalhos suspensos.
   - **Exibir trabalhos de impressão classificados por** - Especifique como os trabalhos de impressão são listados no visor.
3. Clique em **Aplicar**.

Converter trabalhos de impressão para proteger trabalhos de impressão suspensos

1. No Servidos da Web incorporado, clique em **Configurações** > **Segurança** > **Configurações de impressão confidencial**.
2. Selecionar **Exigir que todos os trabalhos sejam suspensos**.
3. Clique em **Salvar**.

Importação e exportação de um arquivo de configuração

Nota: Importar arquivos de configuração substitui as configurações existentes do aplicativo.

1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo. Execute um dos seguintes procedimentos:
   - Clique em **Aplicativos** > **Cliente de Autenticação por SmartCard** > **Configurar**
   - Clique em **Aplicativos** > **Proteger** > **Configurar**
   - Clique em **Aplicativos** > **Proteção de trabalhos de impressão suspensos** > **Configurar**
2. Clique em **Importar** ou **Exportar**.

Usando os aplicativos

Proteger e-mail

Envio de e-mail criptografado e assinado digitalmente

Notas:

- Ao usar login manual, configure as definições de autenticação de Cliente de Autenticação por SmartCard para recuperar todas as informações do usuário. Para obter mais informações, consulte o *Guia do Administrador do Cliente de autenticação do Cartão Smart*.
- Para enviar um e-mail, verifique se você tem um endereço de e-mail válido atribuído à sua conta.

1. Faça login na impressora.
2. Na tela inicial da impressora, toque no ícone do aplicativo.
3. Carregue um documento na bandeja do ADF ou no vidro do scanner.
4. Digite o endereço de e-mail do destinatário. Use vírgulas para separar diversos endereços de e-mail.
5. Se necessário, configure outras definições de e-mail e digitalização.
6. Toque em **Enviar**.
7. Assine digitalmente ou criptografe o e-mail.

   Nota: Para assinar um e-mail digitalmente, você deve ter um certificado de assinatura digital válido e ter feito login usando um SmartCard. Certificados de assinatura estão disponíveis somente no SmartCard. Para obter mais informações, entre em contato com o administrador do sistema.
8. Se necessário, selecione uma opção de segurança.
9. Toque em **Enviar**.
10. Se ocorrer um erro de criptografia, tente fazer o seguinte:
    - Para enviar um e-mail criptografado somente para destinatários com certificados de criptografia, selecione **Enviar Criptografado**.
    - Para enviar um e-mail não criptografado para todos os destinatários, selecione **Enviar Não Criptografado**.
11. Toque em **Enviar**.

Proteger trabalhos de impressão suspensos

Imprimindo trabalhos suspensos

Notas:

- Certifique-se de converter trabalhos de impressão padrão para proteger trabalhos de impressão suspensos. Para obter mais informações, consulte " Converter trabalhos de impressão para proteger trabalhos de impressão suspensos" na página 17.
- Ao usar o recurso imprimir e reter, certifique-se de que o driver de impressão suporta esse recurso. Para obter mais informações, consulte a *Ajuda do driver de impressão*. Você poderá fazer o download do driver de impressão da Lexmark Universal para Windows e o driver de impressão para Macintosh em **www.lexmark.com**.

1. Com um documento aberto, clique em **Arquivo** > **Imprimir**.
2. Selecione uma impressora.

   Nota: Se necessário, configure as definições de impressão.
3. Se necessário, use o recurso imprimir e reter.
   a. Selecione o recurso de imprimir e reter.
      - Para usuários do Windows, clique em **Propriedades**, **Preferências**, **Opções**, ou **Configurações**, e, em seguida, clique em **Imprimir e reter.**
      - Para usuários do Macintosh, selecione **Imprimir e reter** no menu de opções.

   b. Selecione o tipo de trabalho de impressão.
      - **Reservar** - Envia trabalhos de impressão e os armazena na memória da impressora para impressão posterior.
      - **Verificar** - Imprime a primeira cópia de um trabalho de impressão com várias cópias para verificação. As cópias restantes permanecem suspensas até serem impressas ou canceladas.
      - **Repetir** - Imprime o trabalho imediatamente e armazena uma cópia na memória da impressora para o caso de mais cópias precisarem ser impressas posteriormente.

      Nota: O aplicativo Proteção de trabalhos de impressão suspensos não suporta trabalhos de impressão confidenciais.

   c. Digite o nome de usuário no diretório LDAP associado ao trabalho de impressão.
4. Clique em **OK** ou **Imprimir**.
5. Na tela inicial da impressora, faça o login em sua conta, e, em seguida, toque no ícone do aplicativo.

   Notas:

   - Certifique-se de que a mesma conta é usada quando efetuar o login para a impressora e ao enviar os trabalhos de impressão.
   - Dependendo da configuração do aplicativo, todos os trabalhos na fila de liberação de impressão poderão ser impressos automaticamente quando você tocar no ícone do aplicativo. Para obter mais informações, consulte " Configurar as definições de Proteção de trabalhos de impressão suspensos" na página 17.
6. Se solicitado, insira as credenciais de autenticação.

7 Selecione o trabalho ou trabalhos que deseja imprimir e especifique o número de cópias a serem impressas.

8 Toque em **Imprimir**.

Solução de problemas

Erro de aplicativo

Experimente uma ou mais das seguintes opções:

Verifique o log de diagnóstico

1. Abra o navegador da Web e digite ***IP*/se**, no endereço ***IP*** da impressora.
2. Clique em **Soluções embarcadas** e faça o seguinte:
   a. Apague o arquivo de registro.
   b. Defina o nível de registro para **Sim**.
   c. Gere o arquivo de registro.
3. Analise o registro e solucione o problema.

   Nota: Após solucionar o problema, defina o nível de registro para **Não**.

Entre em contato com o seu representante da Lexmark

Problemas de login

Não é possível detectar o leitor de cartões ou o SmartCard

Experimente uma ou mais das seguintes opções:

Certifique-se de que o leitor de cartões esteja conectado corretamente à impressora

Certifique-se de que o leitor de cartões e o SmartCard sejam compatíveis

Verifique se o leitor de cartões é compatível

Para obter uma lista de leitores de cartão compatíveis, consulte o arquivo *Leiame*.

Verifique se o driver do leitor de cartões está instalado na impressora

Entre em contato com o seu representante da Lexmark

Usuário bloqueado

Experimente uma ou mais das seguintes opções:

Aumente o número permitido de falhas de login e o tempo de bloqueio

Nota: Essa solução aplica-se apenas em alguns modelos de impressora.

1. No Embedded Web Server, clique em **Configurações** > **Segurança** > **Restrições de login**.
2. Aumente o número permitido de falhas de login e o tempo de bloqueio.
3. Clique em **Salvar**.

   Nota: As novas configurações entram em vigor depois do término do tempo de bloqueio.

Reinicie ou substitua o SmartCard

Não é possível validar PIN

Experimente uma ou mais das seguintes opções:

Verifique se o PIN inserido está correto

Contate o administrador do sistema

Não é possível fazer login manualmente

Experimente uma ou mais das seguintes opções:

Verifique se o domínio especificado na configuração do Kerberos está correto

Especifique os domínios nas configurações de login manual

Para obter mais informações, consulte " Configurando definições de login manual" na página 13.

Contate o administrador do sistema

A tela inicial da impressora não bloqueia

Experimente uma ou mais das seguintes opções:

Verifique se a Personalização da Exibição está ativada

Para obter mais informações, consulte o *Guia do administrador de Personalização da exibição*.

Acesso seguro à tela inicial

Para obter mais informações, consulte " Protegendo o acesso à tela inicial" na página 9.

Problemas de autenticação

Falha na autenticação do Kerberos

Experimente uma ou mais das seguintes opções:

Verifique o log de diagnóstico

1. Abra o navegador da Web e digite ***IP*/se**, no endereço ***IP*** da impressora.
2. Clique em **Soluções embarcadas** e faça o seguinte:
   a. Apague o arquivo de registro.
   b. Defina o nível de registro para **Sim**.
   c. Gere o arquivo de registro.
3. Analise o registro e solucione o problema.

   Nota: Após analisar o registro, defina o nível de registro para **Não**.

Verifique se o arquivo de configuração está instalado na impressora

- Caso esteja usando a configuração do Kerberos simples para criar o arquivo de configuração do Kerberos, faça o seguinte:
  1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo: **Aplicativos** > **Cliente de Autenticação por SmartCard** > **Configurar**
  2. Na seção Configuração do Kerberos Simples, verifique se os valores de realm, controlador do domínio, domínio e tempo limite estão corretos.
- Caso esteja usando o arquivo de configuração do Kerberos do dispositivo, faça o seguinte:
  1. No Embedded Web Server, clique em **Configurações** > **Segurança** > **Métodos de login**.
  2. Na seção Contas de Rede, clique em **Kerberos** > **Exibir Arquivo**.
  3. Caso o arquivo de configuração do Kerberos não esteja instalado, navegue até o arquivo krb5.conf correto na seção Importar Arquivo do Kerberos.
  4. Clique em **Salvar e Verificar**.

Verifique se o conteúdo e o formato do arquivo de configuração estão corretos

- Se estiver usando a configuração do Kerberos simples, modifique as definições de configuração do Kerberos simples.
- Caso esteja usando o arquivo de configuração do Kerberos do dispositivo, modifique e reinstale o arquivo.

Verifique se o realm do Kerberos está em letras maiúsculas

- Caso esteja usando a configuração do Kerberos simples, faça o seguinte:
  1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo: **Aplicativos** > **Cliente de Autenticação por SmartCard** > **Configurar**
  2. Na seção Configuração do Kerberos Simples, verifique se o realm está correto e se foi digitado em letras maiúsculas.
  3. Clique em **Aplicar**.

- Caso esteja usando o arquivo de configuração do Kerberos do dispositivo, faça o seguinte:
  1. No Embedded Web Server, clique em **Configurações** > **Segurança** > **Métodos de login**.
  2. Na seção Contas de Rede, clique em **Kerberos** > **Exibir Arquivo**.
  3. Verifique se os realms no arquivo de configuração estão em letras maiúsculas.

Especifique o domínio do sistema operacional Microsoft® Windows®

- Caso esteja usando a configuração do Kerberos simples, faça o seguinte:
  1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo:
     Aplicativos > **Cliente de Autenticação por SmartCard** > **Configurar**
  2. Na seção Configuração do Kerberos Simples, no campo Domínio, adicione o domínio do Windows no campo de domínio.
     Por exemplo, caso o valor do campo domínio seja **`NomeDeDomínio,.NomeDeDomínio`** e o domínio do Windows seja **`x.y.z`**, altere o valor do campo Domínio para **`NomeDeDomínio,.NomeDeDomínio,x.y.z`**.

     Nota: O domínio diferencia maiúsculas e minúsculas.
  3. Clique em **Aplicar**.
- Caso esteja usando o arquivo de configuração do Kerberos do dispositivo, adicione uma entrada à seção **`domain_realm`** do arquivo. Insira o realm do domínio do Windows domínio em maiúsculas e, em seguida, reinstale o arquivo na impressora.

Entre em contato com o seu representante da Lexmark

Não é possível gerar ou ler informações de certificado no SmartCard

Experimente uma ou mais das seguintes opções:

Verifique se as informações do certificado no SmartCard estão corretas

Entre em contato com o seu representante da Lexmark

Não é possível validar o controlador de domínio

Experimente uma ou mais das seguintes opções:

Verifique se o realm, o controlador de domínio e o domínio no arquivo de configuração do Kerberos estão corretos

- Caso esteja usando a configuração do Kerberos simples, faça o seguinte:
  1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo:
     Aplicativos > **Cliente de Autenticação por SmartCard** > **Configurar**
  2. Na seção Configuração do Kerberos Simples, verifique se os valores de realm, controlador do domínio e domínio estão corretos.
- Caso esteja usando o arquivo de configuração do Kerberos do dispositivo, faça o seguinte:
  1. No Embedded Web Server, clique em **Configurações** > **Segurança** > **Métodos de login**.
  2. Na seção Contas de Rede, clique em **Kerberos** > **Exibir arquivo**.

3 Verifique se o realm, o controlador de domínio e o domínio estão corretos.

Aumente o valor do tempo limite do controlador de domínio

- Caso esteja usando a configuração do Kerberos simples, faça o seguinte:
  1 No Servidor da Web incorporado, navegue até a página de configuração do aplicativo:
  Aplicativos > **Cliente de Autenticação por SmartCard** > **Configurar**
  2 Na seção Configuração do Kerberos Simples, no campo Tempo Limite, insira um valor de 3 a 30 segundos.
  3 Clique em **Aplicar**.
- Caso esteja usando o arquivo de configuração do Kerberos do dispositivo, insira um valor de 3 a 30 segundos. Quando terminar, reinstale o arquivo na impressora. Para obter mais informações sobre configuração das definições de SmartCard, consulte " Configuração das definições de SmartCard" na página 14.

Verifique se o controlador de domínio está disponível

Use vírgulas para separar vários valores. Os controladores de domínio são validados na ordem listada.

Certifique-se de que a porta 88 não esteja bloqueada entre a impressora e o controlador de domínio

Não é possível validar o certificado do controlador de domínio

Experimente uma ou mais das seguintes opções:

Certifique-se de que os certificados instalados na impressora estejam corretos

Para obter mais informações, consulte " Instalação manual de certificados" na página 7.

Certifique-se de que o método de validação do controlador de domínio estejam configurado corretamente

1 No Servidor da Web incorporado, navegue até a página de configuração do aplicativo:
Aplicativos > **Cliente de Autenticação por SmartCard** > **Configurar**
2 Na seção Configuração do SmartCard, no menu Validação do Controlador de Domínio, selecione o método de validação apropriado.
3 Clique em **Aplicar**.

Não é possível encontrar o realm no arquivo de configuração do Kerberos

Adicionar ou alterar o realm

- Caso esteja usando a configuração do Kerberos simples, faça o seguinte:
  1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo:
     Aplicativos > **Cliente de Autenticação por SmartCard** > **Configurar**
  2. Na seção Configuração do Kerberos Simples, no campo Realm, adicione ou altere o realm. O domínio deve ser digitado em letras maiúsculas.

     Nota: A configuração do Kerberos simples não aceita várias entradas de realm do Kerberos. Se vários domínios forem necessários, instale um arquivo de configuração Kerberos que contenha os domínios necessários.
  3. Clique em **Aplicar**.
- Caso esteja usando o arquivo de configuração do Kerberos do dispositivo, adicione ou altere o realm do arquivo. O domínio deve ser digitado em letras maiúsculas. Quando terminar, reinstale o arquivo na impressora.

Relógios do controlador de domínio e do dispositivo não sincronizados

Certifique-se de que a diferença de tempo entre a impressora e o controlador de domínio não ultrapasse cinco minutos

Para obter mais informações, consulte " Configuração de data e hora" na página 8.

Não é possível validar a cadeia de certificados do controlador de domínio

Experimente uma ou mais das seguintes opções:

Verifique se todos os certificados necessários para validação de cadeia estão instalados na impressora e se as informações estão corretas

Para obter mais informações, consulte " Instalação manual de certificados" na página 7.

Certifique-se de que a cadeia de certificados seja do controlador do domínio para a CA raiz

Certifique-se de que nenhum certificado esteja expirado

1. No Embedded Web Server, clique em **Configurações** > **Segurança** > **Gerenciamento de Certificados**.
2. Certifique-se de que as datas Válido Desde e Válido Até não tenham expirado.

Permitir que os usuários façam login mesmo quando o status de um ou mais certificados é desconhecido

1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo:
   Aplicativos > **Cliente de Autenticação por SmartCard** > **Configurar**
2. Na seção Protocolo de Status de Certificados On-line (OCSP), selecione **Permitir Status Desconhecido**.
3. Clique em **Aplicar**.

Entre em contato com o seu representante da Lexmark

Não é possível conectar à resposta OCSP

Experimente uma ou mais das seguintes opções:

Certifique-se de que o URL de resposta OCSP esteja correto

1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo:

   Aplicativos > **Cliente de Autenticação por SmartCard** > **Configurar**
2. Na seção Protocolo de Status de Certificados On-line (OCSP), verifique se o URL de resposta está correto.
3. Clique em **Aplicar**.

Aumente o valor de tempo limite de resposta

1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo:

   Aplicativos > **Cliente de Autenticação por SmartCard** > **Configurar**
2. Na seção Protocolo de Status de Certificados On-line (OCSP), no campo Tempo Limite de Resposta, insira um valor de 5 a 30.
3. Clique em **Aplicar**.

Não é possível validar o certificado do controlador de domínio contra a resposta de OCSP

Experimente uma ou mais das seguintes opções:

Certifique-se de que o URL de resposta de OCSP e o certificado de resposta estejam configurados corretamente

1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo:

   Aplicativos > **Cliente de Autenticação por SmartCard** > **Configurar**
2. Na seção Protocolo de Status de Certificados On-line (OCSP), no campo URL de Resposta, especifique o seguinte:
   - Endereço IP ou nome do host da resposta/repetição OCSP
   - Número da porta usada

   Por exemplo, **`http://x:y`**, onde ***x*** é o endereço IP e ***y*** é o número da porta.
3. No campo Certificado de Resposta, navegue até o certificado adequado.
4. Clique em **Aplicar**.

Certifique-se de que o controlador de domínio retorne o certificado correto

Certifique-se de que a resposta de OCSP valide o certificado de controlador de domínio correto

Não é possível acessar aplicativos e funções individuais na impressora

Experimente uma ou mais das seguintes opções:

Permitir o acesso seguro a aplicativos ou funções

Para obter mais informações, consulte " Proteger o acesso a funções e aplicativos individuais" na página 10.

Se o usuário pertencer a um grupo do Active Directory, certifique-se de que esse grupo esteja autorizado a acessar os aplicativos e as funções

Problemas de proteger e-mail

Não é possível enviar e-mail usando o aplicativo

Verifique se o aplicativo Gestão de Quotas está desativado

No Embedded Web Server, clique em **Aplicativos** > **Gestão de Quotas** > **Parar**.

Não é possível recuperar o endereço de e-mail do usuário

Experimente uma ou mais das seguintes opções:

Verifique se a função de e-mail da impressora está protegida

Para obter mais informações, consulte " Protegendo o acesso à impressora" na página 9.

Verifique se o endereço de e-mail do usuário foi recuperado corretamente

1. No Embedded Web Server, navegue até a página de configuração para o Cliente de Autenticação por SmartCard:

   Aplicativos > **Cliente de Autenticação por SmartCard** > **Configurar**
2. Na seção Configurações Avançadas, no menu Endereço de E-mail "De", selecione onde a impressora recupera o endereço de e-mail do usuário.
3. Selecione **Aguardar informações do usuário**.
4. Clique em **Aplicar**.

Entre em contato com o seu representante da Lexmark

Não é possível recuperar o certificado de assinatura do usuário

Experimente uma ou mais das seguintes opções:

Certifique-se de que um certificado de assinatura esteja disponível para o usuário

Instale o certificado de assinatura adequado no SmartCard do usuário.

Certifique-se de que os certificados tenham sido recuperados corretamente

1. No Embedded Web Server, navegue até a página de configuração para o Cliente de Autenticação por SmartCard:

   Aplicativos > **Cliente de Autenticação por SmartCard** > **Configurar**
2. Na seção Configurações Avançadas, selecione **Aguardar informações do usuário**.
3. Clique em **Aplicar**.

Entre em contato com o seu representante da Lexmark

Certificado de assinatura indisponível para o usuário

Tente um dos seguintes procedimentos:

Enviar o e-mail sem a assinatura digital

Certifique-se de que um certificado de assinatura esteja disponível para o usuário

Instale o certificado de assinatura adequado no SmartCard do usuário.

Contate o administrador do sistema

Não é possível recuperar certificados do servidor LDAP

Experimente uma ou mais das seguintes opções:

Verifique se os cabos de rede estão conectados firmemente e se as configurações de rede da impressora estão corretas

Para obter mais informações, consulte o *Guia do Usuário* da impressora.

Verifique se as definições do servidor e do firewall estão configuradas para permitir a comunicação entre a impressora e o servidor LDAP na porta 389 ou na porta 636

Se você estiver usando SSL, utilize a porta **636**. Caso contrário, utilize a porta **389**.

Certifique-se de que o endereço do servidor LDAP contenha o nome do host, não o endereço IP

Para obter mais informações, consulte " Configuração de definições de conta de rede LDAP" na página 9.

Se o servidor LDAP exigir SSL, certifique-se de que as configurações de SSL estejam corretas

Para obter mais informações, consulte " Configuração de definições de conta de rede LDAP" na página 9.

Restrinja a base de pesquisa de LDAP para o menor escopo possível que inclua todos os usuários necessários

Verifique se todos os atributos de LDAP estão corretos

Contate o administrador do sistema

Não é possível criptografar e-mails para um ou mais destinatários

Experimente uma ou mais das seguintes opções:

Enviar um e-mail não criptografado para destinatários sem um certificado de criptografia e um e-mail criptografado para destinatários com um certificado de criptografia

Selecione **Enviar para Todos**. Para obter mais informações, consulte " Envio de e-mail criptografado e assinado digitalmente" na página 18.

Enviar um e-mail criptografado somente para destinatários com certificados de criptografia

Selecione **Enviar Criptografado**. Para obter mais informações, consulte " Envio de e-mail criptografado e assinado digitalmente" na página 18.

Enviar e-mail não criptografado para todos os destinatários

Selecione **Enviar Não Criptografado**. Para obter mais informações, consulte " Envio de e-mail criptografado e assinado digitalmente" na página 18.

Entre em contato com o seu representante da Lexmark

Não é possível conectar ao servidor de e-mail

Experimente uma ou mais das seguintes opções:

Verifique se a impressora está conectada a um domínio

Para obter mais informações, consulte " Definindo configurações de TCP/IP" na página 8.

Verifique se as configurações de Autenticação do Servidor SMTP estão corretas

1. No Embedded Web Server, clique em **Configurações** > **E-mail** > **Configuração de E-mail**.
2. No menu Autenticação do Servidor SMTP, execute uma das seguintes ações:
   - Se o servidor SMTP solicitar credenciais do usuário, selecione **Kerberos 5**.
   - Se Kerberos não for compatível, selecione **Nenhuma autenticação necessária**.
   - Se o servidor SMTP exigir autenticação, mas não suportar Kerberos, então, no campo Endereço de Resposta, digite o endereço IP ou o nome do host da impressora.
3. Clique em **Salvar**.

Nota: Para obter mais informações, consulte " Configurando definições SMTP" na página 11.

Se o servidor SMTP usar Kerberos, certifique-se de que os nomes do host dos gateways SMTP primário e secundário estejam corretos

1. No Embedded Web Server, clique em **Configurações** > **E-mail** > **Configuração de E-mail**.
2. Nos campos Gateway SMTP Primário e Gateway SMTP Secundário, digite o nome do host do gateway em vez do endereço IP.
3. Clique em **Salvar**.

Verifique se as definições do servidor e do firewall estão configuradas para permitir a comunicação entre a impressora e o servidor SMTP na porta 25

Verifique se os cabos de rede estão conectados firmemente e se as configurações de rede da impressora estão corretas

Para obter mais informações, consulte o *Guia do Usuário* da impressora.

Contate o administrador do sistema

Não é possível enviar uma cópia para si mesmo

Experimente uma ou mais das seguintes opções:

Verifique se todas as informações do usuário foram inseridas na sessão de login

Verifique se a impressora está configurada para recuperar todas as informações do usuário

1. No Embedded Web Server, navegue até a página de configuração para o Cliente de Autenticação por SmartCard:

   Aplicativos > **Cliente de Autenticação por SmartCard** > **Configurar**
2. Na seção Configurações Avançadas, selecione **Aguardar informações do usuário**.
3. Clique em **Aplicar**.

Certifique-se de que Email para si mesmo esteja configurado de forma correta

Para obter mais informações, consulte " Configuração de Email para si mesmo" na página 12.

Entre em contato com o seu representante da Lexmark

Problemas de Proteger trabalhos de impressão suspensos

Não é possível determinar o ID de usuário

Este erro indica que a conta local, a conta de rede ou o método de login do módulo de autenticação não está definindo o ID do usuário para a sessão. Experimente uma ou mais das seguintes opções:

Verifique se o aplicativo está protegido

Para obter mais informações, consulte " Configurar as definições de Proteção de trabalhos de impressão suspensos" na página 17.

Verifique se o ID do usuário da sessão está definido corretamente

No Servidor da Web incorporado, execute um dos procedimentos a seguir:

Usando um método de login de conta local

1. Clique em **Configurações** > **Segurança** > **Métodos de login**.
2. Na seção Contas locais, clique no tipo de conta local e certifique-se de que a conta tem um nome de usuário.
3. Clique em **Salvar**.

Usando um método de login da conta de rede

1. Clique em **Configurações** > **Segurança** > **Métodos de login**.
2. Na seção Contas de rede, clique na conta de rede e certifique-se de que a conta tem o ID do usuário correto. Para obter mais informações, entre em contato com o administrador do sistema.
3. Clique em **Salvar**.

Usando um módulo de autenticação

1. Clique em **Aplicativos**.
2. Selecione o módulo de autenticação e, em seguida, clique em **Configurar**.
3. Especifique as configurações apropriadas para o ID do usuário da sessão.
4. Clique em **Salvar** ou **Aplicar**.

Entre em contato com o seu provedor de soluções

Se você não conseguir resolver o problema, entre em contato com o seu provedor de soluções.

Nenhum trabalho de impressão está disponível para o usuário

Experimente uma ou mais das seguintes opções:

Verifique se os trabalhos foram enviados para a impressora correta e não expiraram

O usuário pode ter enviado os trabalhos para uma impressora diferente, ou os trabalhos podem ter sido excluídos automaticamente porque não foram impressos a tempo.

Verifique se o ID do usuário da sessão está definido corretamente

No Servidor da Web incorporado, execute um dos procedimentos a seguir:

Usando um método de login de conta local

1. Clique em **Configurações** > **Segurança** > **Métodos de login**.
2. Na seção Contas locais, clique no tipo de conta local e certifique-se de que a conta tem um nome de usuário.
3. Clique em **Salvar**.

Usando um método de login da conta de rede

1. Clique em **Configurações** > **Segurança** > **Métodos de login**.
2. Na seção Contas de rede, clique na conta de rede e certifique-se de que a conta tem o ID do usuário correto. Para obter mais informações, entre em contato com o administrador do sistema.
3. Clique em **Salvar**.

Usando um módulo de autenticação

1. Clique em **Aplicativos**.
2. Selecione o módulo de autenticação e, em seguida, clique em **Configurar**.
3. Especifique as configurações apropriadas para o ID do usuário da sessão.
4. Clique em **Salvar** ou **Aplicar**.

Entre em contato com o seu provedor de soluções

Se você não conseguir resolver o problema, entre em contato com o seu provedor de soluções.

Problemas de LDAP

falha de pesquisas de LDAP

Experimente uma ou mais das seguintes opções:

Verifique se as definições do servidor e do firewall estão configuradas para permitir a comunicação entre a impressora e o servidor LDAP na porta 389 e na porta 636

Se a pesquisa inversa de DNS não for utilizada em sua rede, desative-a nas configurações do Kerberos

1. No Embedded Web Server, clique em **Definições** > **Segurança**.
2. Na seção Contas de Rede, clique em **Kerberos**.
3. Na seção Configurações Variadas, selecione **Desativar Pesquisas de IP Inversas**.
4. Clique em **Salvar e Verificar**.

Se o servidor LDAP exigir SSL, ative o SSL para pesquisas de LDAP

1. No Servidor da Web incorporado, navegue até a página de configuração do aplicativo: **Aplicativos** > **Cliente de Autenticação por SmartCard** > **Configurar**
2. Na seção Configurações Avançadas, selecione **Usar SSL para Informações do Usuário**.
3. Clique em **Aplicar**.

Restrinja a base de pesquisa de LDAP para o menor escopo possível que inclua todos os usuários necessários

Verifique se todos os atributos de LDAP estão corretos

Erro de licença

Entre em contato com o seu representante da Lexmark

Avisos

Aviso de edição

Agosto de 2017

O parágrafo a seguir não se aplica a países onde as cláusulas descritas não são compatíveis com a lei local: A LEXMARK INTERNATIONAL, INC. FORNECE ESTA PUBLICAÇÃO “NO ESTADO EM QUE SE ENCONTRA”, SEM QUALQUER TIPO DE GARANTIA, EXPRESSA OU TÁCITA, INCLUINDO, ENTRE OUTRAS, GARANTIAS IMPLÍCITAS DE COMERCIABILIDADE OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns estados não permitem a contestação de garantias expressas ou implícitas em certas transações. Conseqüentemente, é possível que esta declaração não se aplique ao seu caso.

É possível que esta publicação contenha imprecisões técnicas ou erros tipográficos. Serão feitas alterações periódicas às informações aqui contidas; essas alterações serão incorporadas em edições futuras. Alguns aperfeiçoamentos ou alterações nos produtos ou programas descritos poderão ser feitos a qualquer momento.

As referências feitas nesta publicação a produtos, programas ou serviços não implicam que o fabricante pretenda torná-los disponíveis em todos os países nos quais opera. Qualquer referência a um produto, programa ou serviço não tem a intenção de afirmar ou sugerir que apenas aquele produto, programa ou serviço possa ser usado. Qualquer produto, programa ou serviço funcionalmente equivalente que não infrinja qualquer direito de propriedade intelectual existente poderá ser usado no seu lugar. A avaliação e verificação da operação em conjunto com outros produtos, programas ou serviços, exceto aqueles expressamente designados pelo fabricante, são de responsabilidade do usuário.

Para obter suporte técnico da Lexmark, acesse **http://support.lexmark.com**.

Para obter informações sobre suprimentos e downloads, acesse **www.lexmark.com**.

Marcas comerciais

Lexmark e o logotipo da Lexmark são marcas comerciais da Lexmark International, Inc. registradas nos Estados Unidos e/ou em outros países.

Microsoft, Windows e Active Directory são marcas comerciais registradas ou marcas comerciais do grupo de empresas Microsoft nos Estados Unidos e em outros países.

Todas as outras marcas comerciais pertencem a seus respectivos proprietários.

Índice

T

U

V