



# Autenticação por crachá

Versão 5.8

---

## Guia do administrador

# Conteúdo

- Histórico de alterações..... 4**
- Visão geral..... 5**
- Lista de verificação da prontidão para implantação..... 6**
- Configuração do aplicativo..... 8**
  - Acesso ao Embedded Web Server..... 8
  - Configurar o aplicativo como método de login padrão..... 8
  - Configurar validação do cartão baseada na impressora..... 8
  - Configuração da validação do cartão pelo serviço da Web..... 9
  - Como configurar a validação de cartão por LDAP..... 10
  - Configurando a validação do cartão de serviço de identificação..... 11
  - Configurar autenticação por PIN..... 12
  - Atribuir um método de login para registro de cartão..... 12
  - Atribuir um método de login para login manual..... 13
  - Configurar a autenticação do administrador..... 13
  - Exibindo domínios para contas de usuário..... 13
  - Configurar tela de login..... 14
  - Proteger o acesso a funções e aplicativos individuais..... 15
  - Configurar tempo de espera para desconexão das credenciais..... 15
  - Importação e exportação de um arquivo de configuração..... 16
- Gerenciar o aplicativo..... 17**
  - Acessar a página de status do aplicativo..... 17
  - Gerenciar impressoras de cliente e contas de usuário..... 18
  - Reatribuir funções da impressora..... 18
- Uso do aplicativo..... 20**
  - Registrar usuários..... 20
  - Como registrar um PIN..... 20
  - Efetuar login na impressora manualmente..... 20
- Solução de problemas..... 21**
  - Erro de aplicativo..... 21

---

Erro de autenticação.....	21
Usuário bloqueado.....	22
Não é possível registrar uma impressora cliente.....	22
Não é possível conectar ao servidor LDAP.....	22
Algumas configurações não aparecem na página de configurações.....	23
O usuário não possui privilégios de acesso.....	23
Não é possível encontrar informações do domínio.....	23
<b>Perguntas frequentes.....</b>	<b>25</b>
<b>Avisos.....</b>	<b>27</b>
<b>Índice.....</b>	<b>28</b>

# Histórico de alterações

## Dezembro de 2020

- Informações adicionadas sobre um aviso relacionado a um leitor de cartão ausente.

## Junho de 2020

- Informações adicionadas sobre novas configurações para a verificação de certificados.
- Solicitação de informações removidas da licença.

## Julho de 2019

- Instruções adicionais sobre como configurar a autenticação somente por PIN.

## Dezembro de 2018

- Instruções adicionais sobre como configurar a autenticação do administrador.

## Agosto de 2017

- Informações adicionadas sobre:
  - Definições da tela de bloqueio
  - Perfil personalizado
- Removidas as informações sobre a utilização do aplicativo Display Customization para o gerenciamento da tela de login.

## Agosto de 2016

- Informações adicionadas sobre:
  - Suporte de autenticação com PIN
  - Botões de acesso rápido para login manual e login com PIN

## Julho de 2016

- Informações adicionadas sobre:
  - Login manual
  - Compatibilidade de vários domínios
  - Utilizando contas do serviço para fazer autenticação no Provedor de serviço de identificação
  - Vários domínios do Kerberos para registro de cartão e login manual
  - Cor personalizada do texto de login
  - Permissões do grupo

## Janeiro de 2016

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

## Visão geral

Use o aplicativo para proteger o acesso a uma impressora usando uma leitora de cartões. Quando os usuários se conectarem, suas credenciais serão autenticadas usando um dos seguintes procedimentos:

- Impressora principal. Se a impressora principal estiver off-line, a impressora de backup funcionará como impressora principal até que a impressora principal volte a ficar on-line.

**Nota:** Ao definir as impressoras, verifique se elas estão na mesma rede.

- Servidores do Lightweight Directory Access Protocol (LDAP), Lexmark™ Document Distributor (LDD) ou de provedores de serviços de identidade, dependendo da autenticação definida pela organização.

Você também pode configurar o aplicativo para permitir que os usuários façam login usando uma conta de serviço, um nome de usuário, um nome de usuário e senha ou um PIN.

Este documento oferece instruções sobre como configurar, utilizar e solucionar problemas do aplicativo.

## Lista de verificação da prontidão para implantação

Antes de começar, verifique se:

- Pelo menos uma conta local ou em rede está configurada na impressora. Para obter mais informações, entre em contato com o administrador do sistema.
- Um leitor de cartões e seu driver estão instalados na impressora.
- Você possui o endereço do servidor da web para configurar autenticação com PIN.

Você tem as seguintes informações para configurar a validação de cartão baseada na impressora:

- Nome do host ou endereço IP da impressora principal

---

- Nome do host ou endereço IP da impressora de backup

---

Você tem as seguintes informações para configurar a validação de cartão pelo serviço da web:

- URL do servidor

---

- Versão da interface para pesquisa e registro

Você tem as seguintes informações para configurar a validação de cartão por LDAP:

**Nota:** Você também pode usar uma conta de rede LDAP existente que esteja configurada em sua impressora.

- Endereço do servidor

---

- Número da porta do servidor

---

- Base de pesquisa

---

- Nome de usuário para login

---

Senha para login

\_\_\_\_\_

Atributos de LDAP

– ID do usuário

\_\_\_\_\_

– ID selo

\_\_\_\_\_

– Informações do usuário, opcional

\_\_\_\_\_

Você tem as seguintes informações para configurar a validação do cartão de serviço de identificação:

Endereço do Provedor de serviço de identificação

\_\_\_\_\_

Endereço do Provedor de serviço de crachá

\_\_\_\_\_

# Configuração do aplicativo

## 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.

## Configurar o aplicativo como método de login padrão

- 1 No Embedded Web Server, clique em **Configurações > Segurança > Métodos de login**.
- 2 Clique em **Alterar** ao lado do Método de login do painel de controle padrão.
- 3 No menu Painel de controle, selecione **Autenticação de cartão**.
- 4 Clique em **Salvar**.

## Configurar validação do cartão baseada na impressora

Use a validação baseada na impressora ao validar os usuários por meio de uma impressora principal.

- 1 No Embedded Web Server, navegue até a página de configuração do aplicativo:  
**Aplicativos > Autenticação por crachá > Configurar**
- 2 Na seção Autenticação do usuário, defina Validação de cartão como **Baseada na impressora**.  
**Nota:** A configuração Verificar certificado é aplicável apenas ao serviço de identidade e à validação do serviço da Web.
- 3 Na seção Configurações baseadas na impressora, faça o seguinte:
  - a Selecione uma função para a impressora.
    - **Principal** - a impressora mantém a lista dos usuários registrados.
    - **Backup** - Se a impressora principal estiver off-line, a impressora de backup assume a função da impressora principal até que a impressora principal fique on-line novamente.
    - **Cliente** - a impressora não armazena informações do usuário. Para validar as credenciais do usuário, é necessário uma impressora principal ou uma impressora de backup.

### Notas:

- Se você tiver uma impressora, defina-a como a impressora principal.
- Se você tiver duas impressoras, defina uma como a impressora principal e a outra como a impressora de backup.
- Se você tiver três ou mais impressoras, defina uma como a impressora principal, outra como a impressora de backup e o restante como impressora de cliente.

- b Digite o nome do host ou endereço IP da impressora principal e da impressora de backup.

**Notas:**

- Ao definir uma impressora de backup, o nome de host ou o endereço IP da impressora é obrigatório.
- Ao definir impressoras cliente, os nomes de host ou os endereços IP da impressora principal e das impressoras de backup serão obrigatórios.
- Antes de atribuir uma impressora cliente a uma nova impressora principal, exclua-a da antiga impressora principal.

4 Clique em **Salvar**.

## Configuração da validação do cartão pelo serviço da Web

Use a validação pelo serviço da Web ao validar usuários por meio de um servidor LDD.

1 No Embedded Web Server, navegue até a página de configuração do aplicativo:

**Aplicativos > Autenticação por crachá > Configurar**

2 Na seção Autenticação do usuário, defina Validação de cartão como **Serviço da Web**.

3 Selecione **Verificar certificado** para validar todas as conexões com o servidor. Se a opção Verificar certificado não estiver selecionada, a autoridade de certificações não será validada.

4 No menu Modo de verificação, selecione **cadeia** ou **par**.

**Nota:** O valor padrão é Cadeia.

5 Carregue o Certificado SSL do servidor para se conectar de forma segura ao servidor.

6 No campo Hosts para verificação, digite os nomes de hosts adicionais (que não sejam o URL padrão do servidor) para verificar as entradas do certificado. Use vírgulas para múltiplos nomes de hosts.

**Nota:** Por padrão, a lista de permissões contém apenas o URL do servidor. No campo Hosts para verificação, digite os nomes de hosts adicionais para incluí-los na lista de permissões.

7 Na seção Configurações do serviço da Web, digite o URL do servidor LDD.

8 Se necessário, ajuste o tempo limite de conexão com o servidor.

9 Defina a interface de registro. Selecione uma das seguintes opções:

- **Versão 1** – Somente o ID do crachá e o ID do usuário são exibidos na caixa de diálogo Informações do crachá.
- **Versão 2** - As informações a seguir são exibidas na caixa de diálogo Informações do crachá:
  - ID do crachá
  - ID do usuário
  - endereço IP
  - Nome do host

10 Defina a interface de pesquisa. Para registrar quando e onde o crachá foi utilizado pela última vez, selecione **Versão 2**.

11 Clique em **Salvar**.

## Como configurar a validação de cartão por LDAP

Use a validação por LDAP ao validar usuários por meio de um servidor LDAP.

**1** No Embedded Web Server, navegue até a página de configuração do aplicativo:

**Aplicativos > Autenticação por crachá > Configurar**

**2** Na seção Autenticação do usuário, defina Validação de cartão como **LDAP**.

**Nota:** A configuração Verificar certificado é aplicável apenas ao serviço de identidade e à validação do serviço da Web.

**3** Na seção Configuração do servidor LDAP, defina as configurações.

**Nota:** Se a opção **Usar o catálogo de endereços** estiver selecionada, o aplicativo usará as configurações de LDAP já definidas nas contas de rede da impressora. Se existirem diversas contas LDAP configuradas na impressora, o aplicativo seleciona o nome da configuração baseado na ordem alfabética. Nomes de configuração começados com letras maiúsculas são selecionados antes dos nomes com letra minúscula.

- **Endereço do servidor** - Digite o endereço do servidor do LDAP.
- **Porta do servidor** - Insira o número da porta do LDAP.
- **Usar SSL** - Selecione essa opção para ativar uma conexão segura.
- **Base de pesquisa** - Digite o nó no servidor do LDAP onde a conta do usuário reside. Você pode digitar diversas bases de pesquisa, separadas por vírgula.
- **Nome de usuário para login** - Digite o nome de usuário da conta do LDAP. Em algumas configurações de servidor do LDAP, são necessárias as credenciais do usuário.
- **Senha para login** - Digite a senha da conta do LDAP. Em algumas configurações de servidor do LDAP, são necessárias as credenciais do usuário.

**4** Na seção Atributos do LDAP, ajuste as configurações.

- **ID do usuário** - Digite o atributo do LDAP buscado pelo aplicativo ao autenticar credenciais do usuário. Por exemplo, **samaccountname**, **uid**, **cn** ou um atributo definido pelo usuário.
- **ID do crachá** - Insira o atributo do LDAP para autenticação de usuários com seus números de crachás atribuídos. Por exemplo, **employeeNumber**.
- **Informações do usuário** - Digite as informações do outro usuário que podem ser recuperadas pelo aplicativo no servidor do LDAP.
- **Atributo de associação do grupo** - Insira o atributo do LDAP necessário para a pesquisa do grupo.
- **Lista do grupo** - Digite o grupo do LDAP ao qual a conta do usuário pertence. Os grupos especificados são adicionados à lista de permissões do grupo do aplicativo, onde você pode definir os controles de acesso específicos para cada grupo. Você pode digitar diversos nomes de grupo, separados por vírgula.

**5** Clique em **Salvar**.

## Configurando a validação do cartão de serviço de identificação

Use a validação do cartão por Serviço de identificação ao validar usuários através de um Provedor de serviço de identificação.

- 1 No Embedded Web Server, navegue até a página de configuração do aplicativo:  
**Aplicativos > Autenticação por crachá > Configurar**
- 2 Na seção Autenticação do usuário, defina Validação de cartão como **Serviço de identidade**.
- 3 Selecione **Verificar certificado** para validar todas as conexões com o servidor. Se a opção Verificar certificado não estiver selecionada, a autoridade de certificações não será validada.
- 4 No menu Modo de verificação, selecione **cadeia** ou **par**.  
**Nota:** O valor padrão é Cadeia.
- 5 Carregue o Certificado SSL do servidor para se conectar de forma segura ao servidor.
- 6 No campo HostsParaVerificação, digite os nomes de hosts adicionais (que não sejam o URL padrão do servidor) para verificar as entradas do certificado. Use vírgulas para múltiplos nomes de hosts.  
**Nota:** Por padrão, a lista de permissões contém apenas o URL do servidor. No campo HostsParaVerificação, digite os nomes de hosts adicionais para incluí-los na lista de permissões.
- 7 Na seção Configurações do serviço de identidade, digite o nome do host ou o endereço IP do provedor de serviço de identidade.
- 8 Digite o nome do host ou endereço IP do Provedor de serviço de crachá.
- 9 Defina a Política de Acesso de Aplicativo.
  - **Continuar** - Continua usando a impressora, mesmo se houver uma falha no servidor do Serviço de identificação.
  - **Falhar** - Retorna para a tela de login se a conexão com o servidor do Serviço de identificação falhar.
- 10 Se você tiver uma ID do cliente e um Segredo do cliente do Provedor de serviço de identificação, digite essas informações nos campos correspondentes.
- 11 Ajuste os limites de tempo da rede e do soquete.
- 12 Carregue o Certificado SSL do servidor para se conectar de forma segura ao servidor.
- 13 Para permitir que usuários façam o login na impressora usando uma conta de serviço separada, selecione **Usar conta de serviço**, depois, insira as credenciais da conta de serviço.
- 14 Defina Registro de cartão como **Serviço de identidade**.
- 15 Clique em **Salvar**.

## Configurar autenticação por PIN

Antes de começar, certifique-se de que suas credenciais estejam definidas nas configurações da conta local ou de rede da impressora.

**1** No Embedded Web Server, navegue até a página de configuração do aplicativo:

**Aplicativos > Autenticação por crachá > Configurar**

**2** Na seção de Autenticação de usuário, na seção de Login com PIN, selecione **Ativar login com PIN**.

**3** Selecione **Exibir na proteção de tela** para exibir o botão Login com PIN na proteção de tela.

**4** Na seção de Definições do PIN, no menu Credenciais exigidas, selecione um método de login.

- **ID do usuário e PIN** - Requer um nome de usuário e PIN para autenticação.
- **Somente PIN** - Requer um PIN para autenticação.

**Nota:** Se o método Somente PIN for selecionado, não será possível registrar um novo PIN ou atualizar um existente.

**5** Digite o endereço do servidor Web onde os PINs estão salvos.

**6** Se necessário, digite o texto de login com PIN e, em seguida, defina o comprimento mínimo do PIN.

**Nota:** Se o campo de texto de login com PIN estiver em branco, o texto de login com PIN padrão será exibido. O texto de login com PIN padrão é **Insira suas credenciais de usuário para fazer login**.

**7** Se necessário, digite as mensagens de erro de PIN inválido.

**Nota:** Se os campos de texto forem deixados em branco, as mensagens de erro padrão serão exibidas. As mensagens de erro padrão são **Comprimento de PIN inválido** e **PIN inválido**.

**8** Se necessário, ajuste os limites de tempo da rede e do soquete.

**Nota:** O valor padrão para tempo limite de rede e tempo limite do soquete é de 15 segundos.

**9** Clique em **Salvar**.

## Atribuir um método de login para registro de cartão

Antes de começar, certifique-se de que suas credenciais estejam definidas nas configurações da conta local ou de rede da impressora.

**1** No Embedded Web Server, navegue até a página de configuração do aplicativo:

**Aplicativos > Autenticação por crachá > Configurar**

**2** Na seção Autenticação do usuário, no menu Registro de cartão, selecione um método de login.

**Nota:** Se quiser usar o Kerberos, o Active Directory ou o LDAP+GSSAPI, selecione um domínio. Se o método de login tiver diversos domínios, o domínio selecionado será o domínio padrão exibido durante o registro do cartão.

**3** Clique em **Salvar**.

## Atribuir um método de login para login manual

Antes de começar, certifique-se de que suas credenciais estejam definidas nas configurações da conta local ou de rede da impressora.

**1** No Embedded Web Server, navegue até a página de configuração do aplicativo:

**Aplicativos > Autenticação por crachá > Configurar**

**2** Na seção Autenticação de Usuário, na seção Configurações de Login Manual, defina **Login Manual** de acordo com seu método preferido de login.

**Notas:**

- Se o Login manual estiver definido para Serviço de identidade, e a opção Usar conta de serviço estiver ativada, então os usuários não precisarão inserir suas credenciais manualmente. O aplicativo usa a conta de serviços para efetuar login.
- Se quiser usar o Kerberos, o Active Directory ou o LDAP+GSSAPI, selecione um domínio. Se o método de login selecionado possuir vários domínios, o domínio selecionado é o domínio padrão exibido no momento do login manual.

**3** Selecione **Exibir na proteção de tela** para exibir o botão Login Manual no protetor de tela.

**4** Clique em **Salvar**.

## Configurar a autenticação do administrador

**1** No Embedded Web Server, navegue até a página de configuração do aplicativo:

**Aplicativos > Autenticação por crachá > Configurar**

**2** Na seção Autenticação de usuário, na seção Configurações de login manual, defina **Login de admin** com seu método preferencial de login.

**Nota:** Certifique-se de ter configurado uma conta de administrador local para a impressora e de ter configurado as permissões para o Grupo de administradores de dispositivos. Por padrão, funções e menus não são permitidos para este grupo.

**3** Selecione um grupo autorizado que possa usar o recurso de login de administrador.

**Nota:** Essa configuração é aplicável somente a contas de nome de usuário e nome de usuário e senha.

**4** Selecione **Exibir na proteção de tela** para exibir o botão Login com admin no protetor de tela.

**5** Clique em **Salvar**.

## Exibindo domínios para contas de usuário

O recurso Utilizar Domínio Selecionado será aplicável somente se os métodos de login para registro de cartão e login manual forem Kerberos, Active Directory ou LDAP+GSSAPI. Esse recurso também será aplicável somente se a validação de cartão for definida para serviço da Web ou com base na impressora.

Para registro do cartão, se o recurso estiver ativado, o ID do crachá que está registrado está no formato nomeusuário@domínio.

Para login manual, se o recurso estiver ativado, o nome do usuário exibido no painel de controle da impressora está no formato nomeusuário@domínio.

Essas configurações não se aplicam a login por PIN nem a registro com PIN.

Para ativar esse recurso, faça o seguinte:

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

**Aplicativos > Autenticação por crachá > Configurar**

**2** Na seção Configurações Avançadas, selecione **Utilizar domínio selecionado**.

**3** Clique em **Salvar**.

## Configurar tela de login

**Nota:** Certifique-se de que a definição da proteção de tela do aplicativo de Personalização da exibição esteja desativada. Para obter mais informações, consulte o *Guia do administrador de Personalização da exibição*.

**1** No Embedded Web Server, navegue até a página de configuração do aplicativo:

**Aplicativos > Autenticação por crachá > Configurar**

**2** Na seção Configurações da tela de login, realize um destes procedimentos:

- Para personalizar a mensagem de login, selecione **Usar texto de login personalizado** e, em seguida, digite a mensagem.
- Definir a cor personalizada do texto de login para preto ou branco.
- Para alterar o plano de fundo da tela de login, selecione **Utilizar imagem personalizada para tela de login** e, em seguida, faça o upload do arquivo de imagem.
- Para personalizar a mensagem para login manual, insira a mensagem no campo Texto de login manual.
- Para personalizar a mensagem para login manual, insira a mensagem no campo Texto de login de admin.
- Ativar as funções de cópia e fax sem efetuar login.
- Desative o aviso se nenhum leitor de cartão estiver conectado.

**3** Na seção de Definições da tela de bloqueio, selecione o local do texto de login e, então, insira o nome do perfil ou o ID do aplicativo. O perfil é iniciado automaticamente após o login.

**4** Na seção Perfil personalizado, insira o nome do perfil ou o ID da função do aplicativo ou da impressora e, então, insira o nome personalizado para o ícone. Se necessário, selecione **Usar ícone personalizado** e, em seguida, faça o upload do arquivo de imagem.

**5** Clique em **Salvar**.

**Nota:** A tela de login pode ser desativada somente em ambientes que usem o Serviço de identidade.

### Ativando o acesso público a funções de cópia e fax

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

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

**3** Expanda **Acesso da função** e, em seguida, selecione **Função de cópia** e **Função de fax**.

**4** Clique em **Salvar**.

## Proteger o acesso a funções e aplicativos individuais

Para exigir que os usuários realizem a autenticação antes de acessar um aplicativo ou uma função de impressora, faça o seguinte:

### Restringir acesso público a aplicativos ou funções

- 1 No Embedded Web Server, clique em **Configurações > Segurança > Métodos de login**.
- 2 Na seção Público, clique em **Gerenciar permissões**.
- 3 Expanda uma ou mais categorias e, em seguida, desmarque o aplicativo ou a função que deseja proteger.
- 4 Clique em **Salvar**.

### Gerenciar permissões do grupo

**Nota:** Se o recurso Login de admin está ativado, configure as permissões do Grupo de administradores de dispositivos.

- 1 Na seção Métodos de login adicionais, clique em **Gerenciar permissões** ao lado de Autenticação por cartão.
- 2 Selecione um grupo cujas permissões você queira gerenciar.

**Nota:** A lista mostra os grupos adicionados na Lista do grupo LDAP na página de configuração do aplicativo.

- 3 Expanda uma ou mais categorias e, em seguida, marque o aplicativo ou a função que deseja tornar acessível.
- 4 Clique em **Salvar**.

#### Notas:

- Durante o login, o aplicativo aplica as permissões do grupo ao qual o usuário pertence. Se o usuário pertencer a diversos grupos, o aplicativo unifica todas as permissões. Por exemplo, somente cópias são permitidas para o Grupo A e somente o envio de fax é permitido para o Grupo B. Se o usuário pertencer a ambos os grupos, o aplicativo permite que o usuário faça cópias e envie fax.
- As permissões do grupo do método de login atribuído para registro por cartão e login manual devem ter as mesmas permissões do grupo configuradas no aplicativo.

## Configurar tempo de espera para desconexão das credenciais

Você pode definir um período de tempo para que a impressora interrompa uma conexão bem-sucedida. Se utilizar seu cartão dentro do período especificado, você permanecerá conectado. Se utilizar seu cartão após o temporizador ter expirado, você será desconectado.

Se estiver logado e outro usuário fizer o login usando um cartão, você será desconectado imediatamente e o outro usuário será logado. Esse comportamento ainda entra em vigor mesmo se o temporizador do tempo de espera para desconexão das credenciais estiver ativo.

**1** No Embedded Web Server, navegue até a página de configuração do aplicativo:

**Aplicativos > Autenticação por crachá > Configurar**

**2** Na seção Configurações avançadas, defina o tempo de espera para desconexão das credenciais.

**3** Clique em **Salvar**.

## Importação e exportação de um arquivo de configuração

Importar arquivos de configuração substitui as configurações existentes do aplicativo.

**1** No Embedded Web Server, navegue até a página de configuração do aplicativo:

**Aplicativos > Autenticação por crachá > Configurar**

**2** Clique em **Configuração de importação/exportação**.

**3** Execute um dos seguintes procedimentos:

- Navegue até o arquivo de configuração e clique em **Importar**.
- Clique em **Exportar**.

## Gerenciar o aplicativo

Para validação do cartão baseada na impressora, é possível gerenciar as impressoras de cliente e as contas de usuário na página de status do aplicativo.

### Notas:

- A página de status do aplicativo está disponível somente com o uso da autenticação com base na impressora.
- Se uma função não for atribuída à impressora esta aparece como Não Configurada na página de status do aplicativo. Certifique-se de definir a função da impressora. Para mais informações, consulte "[Configurar validação do cartão baseada na impressora](#)" na página 8.

## Acessar a página de status do aplicativo

Use a página de status para monitorar a atividade da impressora.

**1** No Embedded Web Server, clique em **Aplicativos > Iniciar aplicativos > Autenticação de cartão**.

**2** Observe as seguintes informações:

- **Status** - mostra o status de atividade da impressora.
  - **Não configurada** - nenhuma impressora foi configurada.
  - **Off-line** - nenhuma comunicação ou atividade de impressora foi realizada.
  - **On-line** - a impressora está ativa.
- **Tempo de atividade** - período de tempo em que o aplicativo está sendo executado.
- **(esta impressora)** - a impressora atual.
- **Última atividade** - a última atividade da impressora principal.
- **Número de usuários** - o número total de usuários registrados.
- **Status de registro** - indica se a impressora está off-line ou on-line.
- **Última sincronização com a principal** - a última vez em que a impressora de backup atualizou-se com a impressora principal.
- **Último contato com a principal** - a última vez em que a impressora de backup comunicou-se com a impressora principal.
- **Última sincronização como principal** - a última vez em que a impressora de backup funcionou como impressora principal.
- **Última atividade como principal** - a última atividade da impressora de backup funcionando como a impressora principal.
- **Duração como principal** - quanto tempo a impressora de backup funcionou como a impressora principal.
- **Atendido no momento por** - a impressora de cliente em contato recente com a impressora principal ou de backup.
- **Última atividade com backup** - a última vez em que a impressora de cliente esteve em contato com a impressora de backup.

## Gerenciar impressoras de cliente e contas de usuário

**Nota:** Este recurso é exibido somente quando uma impressora funciona como a principal.

- 1 No Embedded Web Server, clique em **Aplicativos > Iniciar aplicativos > Autenticação de cartão**.
- 2 Na seção Clientes, execute um dos seguintes procedimentos:

### Adicionar impressoras de cliente

- a Clique em **Adicionar clientes**.
- b Digite o endereço IP da impressora de cliente e, em seguida, clique em **Adicionar clientes**.

#### Notas:

- Use vírgulas para separar diversos endereços IP.
- Use um asterisco como o último octeto para pesquisar vários endereços IP. Por exemplo, digite **10.194.1.\***.

### Excluir impressoras de cliente

- a Na lista Clientes, selecione uma ou mais impressoras de cliente.
- b Clique em **Excluir clientes**.

**Nota:** Não será possível excluir impressoras de cliente se o aplicativo estiver off-line ou não tiver sido instalado.

## Excluir contas de usuário

- 1 No Embedded Web Server, clique em **Aplicativos > Iniciar aplicativos > Autenticação de cartão**.
- 2 Na seção Principal, clique em **Excluir usuários**.
- 3 Digite o ID do usuário.  
**Nota:** Use vírgulas para separar diversos IDs de usuário.
- 4 Clique em **Excluir**.

## Reatribuir funções da impressora

### Configurar nova impressora principal

- 1 No Embedded Web Server da nova impressora principal, navegue até a página de configurações do aplicativo:  
**Aplicativos > Autenticação por crachá > Configurar**
- 2 Clique em **Autenticação de usuário** e, em seguida, na seção Configurações baseadas na impressora, defina a função para **Principal**.
- 3 Digite o nome do host ou endereço IP da impressora de backup.
- 4 Clique em **Salvar**.

## Atribuir a impressora de backup à nova impressora principal

- 1 No Embedded Web Server da impressora de backup, navegue até a página de configurações do aplicativo:  
**Aplicativos > Autenticação por crachá > Configurar**
- 2 Clique em **Autenticação de usuário** e, em seguida, na seção Configurações baseadas na impressora, defina a função para **Backup**.
- 3 Digite o nome do host ou endereço IP da nova impressora principal.
- 4 Clique em **Salvar**.

## Reatribuindo uma impressora do cliente

- 1 No Embedded Web Server da impressora principal atual, clique em **Aplicativos > Iniciar aplicativos > Autenticação de cartão**.
- 2 Na seção Clientes, exclua a impressora de cliente.
- 3 Execute um dos seguintes procedimentos:

### Adicionar a impressora de cliente usando a página de configuração do aplicativo

- a No Embedded Web Server da impressora de cliente, navegue até a página de configurações do aplicativo:  
**Aplicativos > Autenticação por crachá > Configurar**
- b Clique em **Autenticação de usuário** e, em seguida, na seção Configurações baseadas na impressora, defina a função para **Cliente**.
- c Digite os nomes do host ou endereços IP da nova impressora principal e da nova impressora de backup.
- d Clique em **Salvar**.

### Adicionar a impressora de cliente usando a página de status da impressora principal

- a No Embedded Web Server da nova impressora principal, clique em **Aplicativos > Iniciar aplicativos > Autenticação de cartão**.
- b No seção Clientes, clique em **Adicionar clientes**.
- c Digite o endereço IP da impressora de cliente.
- d Clique em **Adicionar clientes**.

# Uso do aplicativo

## Registrar usuários

- 1 Encoste seu cartão no leitor de cartões.
- 2 No painel de controle da impressora, insira suas credenciais.

**Nota:** Se estiver usando o Kerberos, o Active Directory ou LDAP+GSSAPI para o registro do cartão, selecione um domínio.

- 3 Toque em **Registrar**.

**Nota:** Ao concluir o registro, você será conectado automaticamente. Se utilizar seu cartão dentro do período especificado no tempo de espera para desconexão, você permanecerá conectado. Para fazer o logout, pressione o botão de início ou toque no nome de usuário no canto superior direito do painel de controle da impressora e, então, confirme o logout. Para obter mais informações, consulte "[Configurar tempo de espera para desconexão das credenciais](#)" na página 15.

## Como registrar um PIN

- 1 No painel de controle da impressora, toque em **Login com PIN**.
- 2 Toque em  > **Registrar PIN**.
- 3 Siga as instruções exibidas no visor.

**Nota:** Para alterar um PIN existente, toque em **Alterar PIN**.

## Efetuar login na impressora manualmente

- 1 No painel de controle da impressora, toque em:
  - **Login com PIN**
  - **Login manual**
  - **Login de admin**

**Nota:** Se você selecionar **Login do administrador**, não será possível recuperar outras informações sobre o usuário do servidor LDAP.

- 2 Digite suas credenciais de login.

**Nota:** Se você estiver usando o Kerberos ou o Active Directory ou o LDAP+GSSAPI para efetuar login manualmente, selecione um domínio.

- 3 Siga as instruções exibidas no visor.

# 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

## Erro de autenticação

Experimente uma ou mais das seguintes opções:

### Aumente o tempo limite da impressora

Se estiver usando um Serviço de identificação como o método de validação de cartão, a impressora poderá precisar de mais tempo para se comunicar com o Provedor de serviço de identificação.

- 1 No Embedded Web Server, clique em **Definições** > **Dispositivo**.
- 2 Faça o seguinte:

#### Ajuste o tempo limite da tela

- a Clique em **Preferências**.
- b Aumente o valor do Tempo limite da tela.
- c Clique em **Salvar**.

#### Ajuste o tempo limite do Modo de suspensão

- a Clique em **Gerenciamento de alimentação**.
- b Aumente o valor do Modo de suspensão.
- c Clique em **Salvar**.

### Verifique se a impressora está conectada à rede

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

### **Certifique-se de que o servidor de segurança esteja on-line e não ocupado**

Para obter mais informações, entre em contato com o administrador do sistema.

## **Usuário bloqueado**

### **Atualizar o tempo de bloqueio e o número permitido de falhas de login**

O usuário pode ter atingido o número máximo permitido de falhas de login.

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

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

**Nota:** Aguarde o tempo de bloqueio até que as novas configurações tenham sido validadas.

## **Não é possível registrar uma impressora cliente**

Experimente uma ou mais das seguintes opções:

### **Verifique se a impressora principal ou de backup está on-line**

Para obter mais informações, consulte "[Acessar a página de status do aplicativo](#)" na página 17.

### **Certifique-se de que a impressora principal e a de backup estejam configuradas corretamente**

Para obter mais informações, consulte "[Configurar validação do cartão baseada na impressora](#)" na página 8.

### **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.

## **Não é possível conectar ao servidor LDAP**

Experimente uma ou mais das seguintes opções:

### **Certifique-se de que as definições de LDAP estejam configuradas corretamente**

Para obter mais informações, consulte "[Como configurar a validação de cartão por LDAP](#)" na página 10.

### **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.

## Algumas configurações não aparecem na página de configurações

Experimente uma ou mais das seguintes opções:

### **Certifique-se de usar o navegador web recomendado**

Para obter mais informações, consulte o arquivo *Leia-me*.

### **Ao utilizar o Explorer, certifique-se de não exibir sites da intranet em Exibição de compatibilidade**

Para obter mais informações, consulte as informações de ajuda do navegador.

### **Entre em contato com o seu representante da Lexmark**

## O usuário não possui privilégios de acesso

Experimente uma ou mais das seguintes opções:

### **Ativar as permissões do método de login atribuído para registro de cartão e login manual.**

- 1 No Embedded Web Server, clique em **Configurações > Segurança > Métodos de login**.
- 2 Clique em **Gerenciar grupos/permissões** ao lado do método login atribuído para registro de cartão e login manual.
- 3 Ativar as permissões que são idênticas às permissões de Autenticação de cartão.
- 4 Clique em **Salvar**.

### **Entre em contato com o seu representante da Lexmark**

## Não é possível encontrar informações do domínio.

A opção Utilizar Domínio Selecionado está ativada no aplicativo, mas o método de login atribuído para login manual ou registro de cartão não requer seleção de domínio. Por exemplo, contas locais ou LDAP. Os métodos de login que exigem seleção de domínio são Kerberos, Active Directory e LDAP+GSSAPI.

Experimente uma ou mais das seguintes opções:

### **Desativar seleção de domínio**

- 1 No Embedded Web Server, navegue até a página de configuração do aplicativo:  
**Aplicativos > Autenticação por crachá > Configurar**
- 2 Na seção Configurações Avançadas, desmarque **Utilizar domínio selecionado**.
- 3 Clique em **Salvar**.

### **Alterar o método de login**

**1** No Embedded Web Server, navegue até a página de configuração do aplicativo:

**Aplicativos > Autenticação por crachá > Configurar**

**2** Na seção Autenticação de Usuário, altere o método de login para registro de cartão e login manual para Kerberos ou Active Directory ou LDAP + GSSAPI.

**3** Clique em **Salvar**.

**Entre em contato com o seu representante da Lexmark**

## Perguntas frequentes

### Por que não posso adicionar ou excluir uma impressora de cliente quando uma impressora de backup funciona como a impressora principal?

Só é possível excluir ou adicionar uma impressora de cliente quando a impressora principal está on-line.

### Posso remover uma impressora de cliente mesmo se a impressora principal estiver off-line e reatribuí-la à sua nova impressora principal?

Sim. Faça o seguinte:

- 1 Reinstale o aplicativo da impressora de cliente.
- 2 Defina a função como impressora de cliente e configure-a para suas novas impressoras principal e de backup. Para obter mais informações, consulte "[Configurar validação do cartão baseada na impressora](#)" na página 8.

### Por que não estou visualizando um botão de Cópia ou Fax na tela de bloqueio mesmo com a função de cópia ou fax habilitada sem fazer login?

O botão de Cópia ou Fax não será exibido se o controle de acesso para a função de Cópia ou Fax não estiver configurado. Para obter mais informações, consulte "[Configurar tela de login](#)" na página 14.

### Como limitar o acesso público à página de configurações de todos os aplicativos?

- 1 No Embedded Web Server, clique em **Configurações** > **Segurança** > **Métodos de login**.
- 2 Na seção Pública, clique em **Gerenciar permissões**.
- 3 Expanda **Gerenciamento de dispositivos** e, em seguida, desmarque a opção **Configuração dos aplicativos**.
- 4 Clique em **Salvar**.
- 5 No Embedded Web Server, clique em **Configurações** > **Segurança** > **Métodos de login**.
- 6 Clique em **Gerenciar permissões** ou **Gerenciar grupos/permissões** ao lado do método de login que você deseja configurar.
- 7 Clique no grupo para o qual você deseja conceder acesso à página de configurações de todos os aplicativos.

**8** Expanda **Gerenciamento de dispositivos** e verifique se a opção **Configuração dos aplicativos** está selecionada.

**9** Clique em Salvar.

# Avisos

## Aviso de edição

Dezembro de 2020

**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 COMERCIALIZABILIDADE 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 suporte técnico da Lexmark, vá até <http://support.lexmark.com>.

Para informações sobre a política de privacidade da Lexmark que rege o uso deste produto, vá até [www.lexmark.com/privacy](http://www.lexmark.com/privacy).

Para informações sobre suprimentos e downloads, vá até [www.lexmark.com](http://www.lexmark.com).

© 2016 Lexmark International, Inc.

**Todos os direitos reservados.**

## Marcas comerciais

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

Todas as outras marcas comerciais pertencem a seus respectivos proprietários.

# Índice

## A

- acesso
  - página de status 17
- acesso ao Embedded Web Server 8
- adição
  - impressoras cliente 18
  - usuários 20
- adicionar contas locais 12
- Algumas configurações não aparecem na página de configurações 23
- alterar um PIN 20
- aplicativos
  - proteção 15
- arquivo de configuração
  - importando ou exportando 16
- atribuir um método de login 12
- atribuir um método de login para login manual 13
- autenticação
  - como configurar 8
- autenticação do administrador
  - como configurar 13
- autenticação por crachá
  - método de login padrão 8
- Autenticação por PIN
  - como configurar 12

## C

- como configurar
  - Autenticação por PIN 12
  - nova impressora de backup 18
  - nova impressora principal 18
  - tela de login 14
  - tempo de espera para desconexão das credenciais 15
  - Validação de cartão por LDAP 10
  - validação do cartão baseada na impressora 8
  - Validação do cartão de serviço de identificação 11
  - validação do cartão pelo serviço da Web 9
- como exportar um arquivo de configuração 16

- como importar um arquivo de configuração 16
- como registrar um PIN 20
- configuração de autenticação do administrador 13
- configuração de domínios
  - métodos de login 13
- contas de usuário
  - excluir 18
  - migrar 18
- contas locais
  - adição 12
- controles de acesso 15

## E

- efetuar login na impressora manualmente 20
- Embedded Web Server
  - acesso 8
- erro de autenticação 21
- erro do aplicativo 21
- excluir
  - contas de usuário 18
  - impressoras cliente 18
- exibindo domínios para contas de usuário 13

## F

- função de cópia
  - utilizar sem efetuar login 14
- função de fax
  - utilizar sem efetuar login 14
- funções
  - proteção 15
- funções da impressora
  - reatribuir 18

## H

- histórico de alterações 4

## I

- impressoras cliente
  - adição 18
  - excluir 18
  - migrar 18

## L

- lista de verificação
  - prontidão para implantação 6
- lista de verificação da prontidão para implantação 6
- login
  - manual 20
  - PIN 20
- login com PIN 20
- login manual 20
  - atribuir um método de login 13

## M

- método de login padrão 8
- migrar
  - contas de usuário 18
  - impressoras cliente 18

## N

- não é possível conectar ao servidor LDAP 22
- não é possível encontrar informações do domínio. 23
- não é possível registrar uma impressora cliente 22

## O

- o usuário está bloqueado 22
- o usuário não possui privilégios de acesso 23

## P

- página de status
  - acesso 17
- perguntas frequentes 25
- Perguntas frequentes 25
- PIN
  - registro 20
- proteção
  - aplicativos 15
  - funções da impressora 15

## R

- reatribuir funções da impressora 18
- registro de usuários 20

**S**

solução de problemas

Algumas configurações não aparecem na página de configurações 23

erro de autenticação 21

erro do aplicativo 21

não é possível conectar ao servidor LDAP 22

não é possível encontrar informações do domínio. 23

não é possível registrar uma impressora cliente 22

o usuário está bloqueado 22

o usuário não possui privilégios de acesso 23

**T**

tela de login

como configurar 14

tempo de espera para

desconexão das credenciais

como configurar 15

**U**

usuários

adição 20

registro 20

utilizar a função de cópia sem

efetuar login 14

utilizar a função de fax sem

efetuar login 14

**V**

Validação de cartão por LDAP

como configurar 10

validação do cartão baseada na impressora

como configurar 8

Validação do cartão de serviço de identificação

como configurar 11

validação do cartão pelo serviço da Web

como configurar 9

visão geral 5