



Autenticação por crachá

Guia do administrador

Conteúdo

Visão geral.....	4
Configuração dos pré-requisitos.....	5
Acesso ao Servidor da Web Incorporado.....	5
Adicionando uma conta de usuário interna.....	5
Criação de grupos para contas de usuário interno.....	5
Criando um modelo de segurança.....	6
Configurando controles de acesso.....	6
Configuração do aplicativo.....	8
Acessando a página de configurações do aplicativo.....	8
Configurar a autenticação do administrador.....	8
Configurar tela de login.....	8
Autenticação com base na impressora.....	9
Autenticação de serviço da Web.....	10
Autenticação de serviço de identidade.....	12
Autenticação por PIN.....	13
autenticação LDAP.....	14
Configuração das preferências do aplicativo.....	15
Exibindo domínios para contas de usuário.....	15
Exportando ou importando um arquivo de configuração.....	16
Gerenciar o aplicativo.....	17
Acessar a página de status do aplicativo.....	17
Gerenciando contas de usuário e impressoras de cliente.....	17
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

Perguntas frequentes.....	25
Avisos.....	27
Índice.....	28

Visão geral

Use o aplicativo para proteger o acesso a uma impressora usando uma leitora de cartões. Depois de um toque, as credenciais do usuário 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 Provedores de serviço de identidade, dependendo da autenticação definida pela organização.

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

Configuração dos pré-requisitos

Talvez sejam necessários direitos administrativos para configurar o aplicativo.

Acesso ao Servidor da Web Incorporado

- 1 Obtenha o endereço IP da impressora. Execute um dos seguintes procedimentos:
 - Localize o endereço IP na tela inicial da impressora.
 - Visualize o endereço IP na seção TCP/IP do menu Rede/Portas.
- 2 Abra o navegador da Web e digite o endereço IP da impressora.

Adicionando uma conta de usuário interna

Uma conta de usuário interna é necessária ao utilizar a autenticação com base na impressora.

- 1 No Embedded Web Server, clique em **Configurações** ou **Configuração**.
- 2 Dependendo do modelo da sua impressora, faça o seguinte:
 - Clique em **Segurança > Configuração de segurança > Contas internas > Adicionar uma conta interna**.
 - Clique em **Segurança > Editar configurações de segurança > Contas internas > Adicionar uma conta interna**.
- 3 Digite as informações da conta e clique em **Enviar**.
- 4 Se necessário, a partir da seção Gerenciar contas internas, digite um nome de bloco de construção personalizado e especifique as credenciais de usuário necessárias.
- 5 Clique em **Enviar**.

Criação de grupos para contas de usuário interno

- 1 No Embedded Web Server, clique em **Configurações** ou **Configuração**.
- 2 Dependendo do modelo da sua impressora, faça o seguinte:
 - Clique em **Segurança > Configuração de segurança > Contas internas > Configuração de grupos para uso com contas internas**.
 - Clique em **Segurança > Editar configurações de segurança > Contas internas > Configuração de grupos para uso com contas internas**.
- 3 Insira o nome de um grupo e clique em **Adicionar**.
- 4 Adicionar contas internas ao grupo.
- 5 Clique em **Enviar**.

Criando um modelo de segurança

Um modelo de segurança é composto por blocos de construção de segurança, como contas internas, Kerberos, LDAP, LDAP+GSSAPI e Active Directory. Esses modelos são aplicados ao controle de acesso para proteger as funções e os aplicativos da impressora.

- 1 No Embedded Web Server, clique em **Configurações** ou **Configuração**.
- 2 Dependendo do modelo da sua impressora, faça o seguinte:
 - Clique em **Segurança** > **Configuração de segurança** > **Modelo de Segurança** > **Adicionar um modelo de segurança**.
 - Clique em **Segurança** > **Editar configurações de segurança** > **Modelos de segurança** > **Adicionar um modelo de segurança**.
- 3 Digite um nome de modelo de segurança e selecione uma das seguintes configurações de autenticação:
 - Para autenticação com base na impressora em uma configuração isolada, selecione um bloco de construção de conta interna.
 - Para autenticação com base em impressora com Liberação de impressão sem servidor do Gerenciamento de impressão Lexmark (LPM) em uma configuração do Active Directory, selecione um bloco de construção LDAP+GSSAPI.
 - Para autenticação LDAP, selecione um bloco de construção LDAP.
- 4 Clique em **Salvar modelo**.

Nota: Para modificar um modelo de segurança existente, clique no modelo de segurança e adicione ou modifique uma autorização para o modelo.

Configurando controles de acesso

Nota: Ao usar o recurso **Login de admin**, verifique se você configurou o modelo de segurança para contas internas. Para obter mais informações, consulte "[Criando um modelo de segurança](#)" na página 6.

- 1 No Embedded Web Server, clique em **Configurações** ou **Configuração**.
- 2 Dependendo do modelo da sua impressora, faça o seguinte:
 - Clique em **Segurança** > **Configuração de segurança** > **Controles de acesso**.
 - Clique em **Segurança** > **Editar configurações de segurança** > **Controles de acesso**.
- 3 Clique em **Aplicativos do dispositivo** ou **Soluções de dispositivo** e faça o seguinte:
 - Defina Aplicativo 1 ou Solução 1 para uma conta interna ou LDAP+GSSAPI ou modelo de segurança do Active Directory.
 - Defina Aplicativo 2 ou Solução 2 para o modelo de segurança do aplicativo.

Nota: O modelo de segurança do aplicativo é o modelo com CardAuth como configuração de autenticação. Para obter mais informações, consulte "[Criando um modelo de segurança](#)" na página 6.
 - Defina Aplicativo 3 ou Solução 3 para um modelo de segurança LDAP.

Notas:

- Se a liberação de impressão LPM estiver instalada, defina o controle de acesso de liberação de impressão para o modelo de segurança do aplicativo.

- As impressoras de Framework de Soluções Embarcadas (eSF) versão 2.x precisam do aplicativo Gerente de segurança eSF para configurar o controle da acesso. Para obter uma lista dessas impressoras, consulte o arquivo *Leiamé*.

4 Clique em **Enviar**.

Configuração do aplicativo

Antes de começar, faça o seguinte:

- Desative o descanso de tela e qualquer aplicativo de autenticação existente.
- Instale o seguinte:
 - Instalador de Autenticação por crachá
 - Driver do leitor de cartão
 - Leitor de cartão
 - Gerente de segurança eSF

Nota: As impressoras eSF versão 2.x precisam do aplicativo Gerente de segurança eSF para configurar o controle da acesso. Para obter uma lista dessas impressoras, consulte o arquivo *Leiamé*.

Acessando a página de configurações do aplicativo

- 1 No Embedded Web Server, clique em **Configurações** ou **Configuração**.
- 2 Dependendo do modelo da sua impressora, faça o seguinte:
 - Clique em **Apps > Gerenc. de apps**.
 - Clique em **Soluções de dispositivo > Soluções (eSF)**.
 - Clique em **Soluções incorporadas**.
- 3 Clique em **Autenticação de cartão > Configurar**.

Configurar a autenticação do administrador

Nota: Ao usar o recurso **Login de admin**, verifique se você configurou o modelo de segurança para contas internas, PIN e senha. Para obter mais informações, consulte "[Criando um modelo de segurança](#)" na página 6.

- 1 No Embedded Web Server, acesse a página de configuração do aplicativo.
- 2 Da seção Autenticação de usuário, defina **Controle de acesso de login de administrador** com seu método preferencial de login.

Notas:

- Certifique-se de que o controle de acesso selecionado esteja configurado com um modelo de segurança. Para obter mais informações, consulte "[Criando um modelo de segurança](#)" na página 6.
- Selecionar **Desativado** esconde a opção **Login de administrador** do painel da impressora.

- 3 Clique em **Aplicar**.

Configurar tela de login

A tela de login pode ser configurada para fazer o seguinte:

- Permite que os usuários usem as funções de cópia e fax sem efetuar login.
- Permite que os usuários selecionem o método de login a ser usado.

- Adicione um plano de fundo da tela de login e personalize a mensagem de login.
- Desative o aviso se nenhum leitor de cartão estiver conectado.

1 Usando o Embedded Web Server, acesse a página de configuração do aplicativo.

2 A partir da seção Tela de login, configure as definições.

Nota: para obter mais informações sobre cada definição, use a ajuda que pode ser visualizada com o mouse.

3 Clique em **Aplicar**.

Ativando as funções de cópia ou fax sem efetuar login

Se "Permitir cópia sem login" ou "Permitir fax sem login" for ativado, faça o seguinte:

1 No Embedded Web Server, clique em **Configurações** ou **Configuração**.

2 Dependendo do modelo da sua impressora, faça o seguinte:

- Clique em **Segurança** > **Configuração de segurança** > **Controles de acesso** > **Acesso de função**.
- Clique em **Segurança** > **Editar configurações de segurança** > **Controles de acesso**.

3 Defina a função de cópia ou fax para **Sem segurança**.

4 Clique em **Enviar**.

Autenticação com base na impressora

Utilize a autenticação com base na impressora ao validar os usuários por meio de uma impressora principal.

Configurando a autenticação de usuário com base na impressora

Antes de começar, verifique se:

- O controle de acesso ao Aplicativo 1 ou Solução 1 é definido para uma conta interna ou LDAP+GSSAPI ou modelo de segurança do Active Directory.
- O controle de acesso ao Aplicativo 2 ou Solução 2 é definido para o modelo de segurança do aplicativo.

Nota: Para obter mais informações, consulte "[Configurando controles de acesso](#)" na página 6.

1 No Embedded Web Server, acesse a página de configuração do aplicativo.

2 A partir da seção Tela de login, defina o método de login para **Cartão ou login manual**.

3 A partir da seção Autenticação de usuário, faça o seguinte:

- Defina a validação de cartão para **Baseada na impressora**.
- Defina o controle de acesso de registro do cartão para **Aplicativo 1** ou **Solução 1**.
- Defina o controle de acesso de login manual para **Aplicativo 1** ou **Solução 1**.
- Defina o controle de acesso da sessão para **Aplicativo 2** ou **Solução 2**.

Notas:

- Se o controle de acesso de registro do cartão for definido para **Nenhum**, não será possível registrar seu cartão na impressora.

- A definição do controle de acesso de login manual para **Nenhum** exigirá somente um cartão para fazer login mesmo se o método de login for definido para **Cartão ou login manual**.
- Para obter mais informações em cada configuração, consulte a ajuda do mouse.

4 Clique em **Aplicar**.

Como configurar a função da impressora

Nota: Uma impressora de cliente requer uma impressora principal e uma impressora de backup.

- 1** No Embedded Web Server, acesse a página de configuração do aplicativo.
- 2** A partir da seção Validação de cartão baseada em impressora, 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.

- 3** Digite os nomes do host ou o 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 **Aplicar**.

Autenticação de serviço da Web

Utilize a autenticação de serviço da Web ao validar usuários por meio de um servidor LDD.

Configurando a autenticação de usuário do serviço da Web

Antes de começar, certifique-se de que o controle de acesso ao Aplicativo 2 ou Solução 2 seja definido para o modelo de segurança do aplicativo. Para mais informações, consulte "[Configurando controles de acesso](#)" na página 6.

- 1** Usando o Embedded Web Server, acesse a página de configuração do aplicativo.
- 2** Na seção Tela de login, defina Método de login como **Login manual ou com crachá**.

3 Na seção Autenticação do usuário, faça o seguinte:

- Defina Validação de crachá como **Serviço da Web**.
- Defina Controle de acesso de registro de crachá e Controle de acesso do login manual de acordo com o controle de acesso de sua preferência.
- Defina Controle de acesso da sessão como **Aplicativo 2** ou **Solução 2**.

Notas:

- Se Controle de acesso de registro de crachá estiver definido como **Nenhum**, não será possível registrar seu crachá na impressora.
- A definição de Controle de acesso do login manual como **Nenhum** exigirá somente um crachá para fazer login mesmo se Método de login estiver definido como **Login manual ou com crachá**.
- para obter mais informações sobre cada definição, use a ajuda que pode ser visualizada com o mouse.

4 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.

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

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

Nota: O valor padrão é Cadeia.

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

7 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.

8 Clique em **Aplicar**.

Configurando definições do serviço da Web

1 No Embedded Web Server, acesse a página de configuração do aplicativo.

2 A partir da seção Configurações de serviço da Web, configure as definições.

Nota: Para obter mais informações em cada definição, consulte a ajuda do mouse.

3 Clique em **Aplicar**.

Autenticação de serviço de identidade

Utilize a autenticação de serviço de identidade ao validar usuários por meio de um servidor de Serviço de Identidade, como o servidor Software como Serviço (SaaS) LPM.

Configurando a autenticação de usuário do serviço de identidade

Antes de começar, certifique-se de que o controle de acesso ao Aplicativo 2 ou Solução 2 seja definido para o modelo de segurança do aplicativo. Para mais informações, consulte "[Configurando controles de acesso](#)" na página 6.

- 1 Usando o Embedded Web Server, acesse a página de configuração do aplicativo.
- 2 Na seção Tela de login, defina Método de login como **Login manual ou com crachá**.
- 3 Na seção Autenticação do usuário, faça o seguinte:
 - Defina Validação de crachá como **Serviço de identidade**.
 - Defina Controle de acesso de registro de crachá como **Serviço de identidade**.
 - Defina Controle de acesso do login manual como **Serviço de identidade**.
 - Defina Controle de acesso da sessão como **Aplicativo 2** ou **Solução 2**.

Notas:

- Se Controle de acesso de registro de crachá estiver definido como **Nenhum**, não será possível registrar seu crachá na impressora.
 - A definição de Controle de acesso do login manual como **Nenhum** exigirá somente um crachá para fazer login mesmo se Método de login estiver definido como **Login manual ou com crachá**.
 - para obter mais informações sobre cada definição, use a ajuda que pode ser visualizada com o mouse.
- 4 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.
Nota: A configuração Verificar certificado é aplicável apenas ao serviço de identidade e à validação do serviço da Web.
 - 5 No menu Modo de verificação, selecione **cadeia** ou **par**.
Nota: O valor padrão é Cadeia.
 - 6 Carregue o Certificado SSL do servidor para se conectar de forma segura ao servidor.
 - 7 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.
 - 8 Clique em **Aplicar**.

Configurando definições do serviço de identidades

- 1 No Embedded Web Server, acesse a página de configuração do aplicativo.
- 2 Se necessário, a partir da seção Definições do serviço de identidades, selecione **Ativar tela ociosa**.
Nota: As impressoras eSF versão 2.x precisarão do aplicativo Gerente de segurança eSF quando **Ativar tela ociosa** estiver habilitado. Para obter uma lista dessas impressoras, consulte o arquivo *Leiam*.
- 3 Digite o nome do host ou endereço IP do Provedor de serviço de identidades.
- 4 Se necessário, digite o nome do host ou endereço IP do Provedor de serviço de crachá.
- 5 Carregue o certificado SSL do servidor para se conectar de forma segura ao servidor.
- 6 Se você tiver uma ID do cliente e um Segredo do cliente do Provedor de serviço de identificação, digite essas informações nos campos correspondentes.
- 7 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.
- 8 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.
- 9 Clique em **Aplicar**.

Autenticação por PIN

Configurando autenticação do usuário PIN

Antes de começar, certifique-se de que o controle de acesso ao Aplicativo 2 ou Solução 2 seja definido para o modelo de segurança do aplicativo. Para obter mais informações, consulte "[Configurando controles de acesso](#)" na página 6.

- 1 No Embedded Web Server, acesse a página de configuração do aplicativo.
- 2 A partir da seção Tela de login, defina o método de login para uma opção que seja compatível com autenticação por PIN.
- 3 A partir da seção Autenticação de usuário, faça o seguinte:
 - Defina a validação do cartão de acordo com seu método de autenticação preferido.
 - Defina o controle de acesso de registro do cartão de acordo com seu controle de acesso preferido.
 - Defina o controle de acesso de PIN para **Aplicativo 1** ou **Solução 1**.
 - Defina o controle de acesso de login manual de acordo com seu controle de acesso preferido.
 - Defina o controle de acesso da sessão para **Aplicativo 2** ou **Solução 2**.

Notas:

- Se o controle de acesso por PIN for definido para **Nenhum**, não será possível registrar seu PIN na impressora.

- Para obter mais informações em cada configuração, consulte a ajuda do mouse.

4 Clique em **Aplicar**.

Configurando definições de PIN

- 1** No Embedded Web Server, acesse a página de configuração do aplicativo.
- 2** 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.
- 3** Digite o endereço do servidor da Web e selecione o comprimento mínimo do PIN.
- 4** Digite as mensagens de erro de PIN inválido.
- 5** Clique em **Aplicar**.

autenticação LDAP

Utilize a autenticação LDAP ao validar usuários por meio de um servidor LDAP.

Configurando autenticação do usuário LDAP

Antes de começar, verifique se:

- O controle de acesso ao Aplicativo 2 ou Solução 2 é definido para o modelo de segurança do aplicativo.
- O controle de acesso ao Aplicativo 3 ou Solução 3 é definido para um modelo de segurança LDAP.

Nota: Para obter mais informações, consulte "[Configurando controles de acesso](#)" na página 6.

- 1** No Embedded Web Server, acesse a página de configuração do aplicativo.
- 2** A partir da seção Tela de login, defina o método de login para **Cartão ou login manual**.
- 3** A partir da seção Autenticação de usuário, faça o seguinte:
 - Defina a validação de cartão para **LDAP**.
 - Defina o controle de acesso de registro do cartão para **Aplicativo 3** ou **Solução 3**.
 - Defina o controle de acesso de login manual para **Aplicativo 3** ou **Solução 3**.
 - Defina o controle de acesso da sessão para **Aplicativo 2** ou **Solução 2**.

Notas:

- Se o controle de acesso de registro do cartão for definido para **Nenhum**, não será possível registrar seu cartão na impressora.
- A definição do controle de acesso de login manual para **Nenhum** exigirá somente um cartão para fazer login mesmo se o método de login for definido para **Cartão ou login manual**.
- Para obter mais informações em cada configuração, consulte a ajuda do mouse.

4 Clique em **Aplicar**.

Configurando definições LDAP

1 No Embedded Web Server, acesse a página de configuração do aplicativo.

2 Na seção Configurações LDAP, configure as definições.

Notas:

- 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.
- Para obter mais informações em cada configuração, consulte a ajuda do mouse.

3 Clique em **Aplicar**.

Configuração das preferências do aplicativo

1 No Embedded Web Server, acesse a página de configuração do aplicativo.

2 Experimente uma ou mais das seguintes opções:

- Para personalizar a tela inicial da impressora, defina as configurações de tela inicial.
- Para exibir as mensagens de registro, a partir da seção Configurações avançadas, selecione **Mostrar mensagem de introdução de registro** e **Mostrar mensagem de conclusão de registro**.
- Para ouvir um *signal sonoro* depois de um login efetuado com êxito, a partir da seção Configurações avançadas, selecione **Ativar bipe para login bem-sucedido** e ajuste a frequência do sinal sonoro.
- Para utilizar um perfil depois de um login efetuado com êxito, a partir da seção Configurações avançadas, no campo Perfil de login, digite um nome de perfil.

Nota: Para obter mais informações em cada configuração, consulte a ajuda do mouse.

3 Clique em **Aplicar**.

Visualizando perfis disponíveis

1 No Embedded Web Server, clique em **Configurações** ou **Configuração**.

2 Clique em **Gerenciar atalhos** > **Gerenciar atalhos de perfil**.

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 Embedded Web Server, acesse a página de configuração do aplicativo.
- 2 Na seção Configurações Avançadas, selecione **Utilizar domínio selecionado**.
- 3 Clique em **Aplicar**.

Exportando ou importando um arquivo de configuração

- 1 No Embedded Web Server, acesse a página de configuração do aplicativo.
- 2 Exporte ou importe o arquivo de configuração.

Notas:

- Se ocorrer um erro **JVM sem memória**, você deverá repetir a exportação até o arquivo de configuração ser salvo.
- Se o tempo limite se esgotar e uma tela em branco for exibida, você deverá atualizar o navegador da Web e, em seguida, clicar em **Aplicar**.

Gerenciar o aplicativo

Nota: A página de status do aplicativo está disponível somente com o uso da autenticação com base na impressora.

Acessar a página de status do aplicativo

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

- 1 A partir do Embedded Web Server, clique em **Aplicativos > Autenticação de cartão**.
- 2 Observe as seguintes informações:
 - **Status** - mostra o status de atividade da impressora.
 - **Não configurada**—a impressora não foi configurada.
 - **Off-line** - nenhuma comunicação ou atividade de impressora foi realizada.
 - **On-line** - a impressora está ativa.
 - **Tempo de atividade**—Indica o período de execução do aplicativo.
 - **(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**—indica 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.

Gerenciando contas de usuário e impressoras de cliente

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

- 1 No Embedded Web Server, acesse a página de status do aplicativo.
- 2 Tente um dos seguintes métodos:

Excluir contas de usuário

- a Na seção Principal, clique em **Excluir usuários**.
- b Digitar um ou mais IDs de usuário e excluí-los.

Adicionar impressoras de cliente

- a No seção Clientes, clique em **Adicionar clientes**.
- b Digitar um ou mais endereços IP da impressora e adicioná-los.

Excluir impressoras de cliente

Nota: Não será possível excluir impressoras de cliente quando a impressora principal estiver off-line ou quando o aplicativo for desinstalado.

- a A partir da seção Clientes, selecione uma ou mais impressoras de cliente.
- b Clique em **Excluir clientes**.

Reatribuir funções da impressora

- 1 Configure uma nova impressora principal.
 - a A partir do Embedded Web Server da nova impressora principal, acesse a página de configurações do aplicativo.
 - b A partir da seção Validação do cartão baseada na impressora, defina a função para **Principal**.
 - c Digite o nome do host ou endereço IP da impressora de backup.
 - d Clique em **Aplicar**.
- 2 Atribua a impressora de backup à nova impressora principal.
 - a A partir do Embedded Web Server da impressora de backup, acesse a página de configurações do aplicativo.
 - b A partir da seção Validação de cartão baseada em impressora, digite o nome do host ou endereço IP da nova impressora principal.
 - c Clique em **Aplicar**.
- 3 Exclua a impressora do cliente da impressora principal atual.
 - a A partir do Embedded Web Server da impressora principal atual, acesse a página de status do aplicativo.
 - b Na seção Clientes, exclua a impressora de cliente.
- 4 Reatribua a impressora de cliente à nova impressora principal. Execute um dos seguintes procedimentos:

Utilizando a página de configurações do aplicativo

- a A partir do Embedded Web Server da impressora de cliente, acesse a página de configurações do aplicativo.
- b A partir da seção Validação do cartão baseada na impressora, defina a função para **Cliente**.
- c Digite o nome do host ou endereço IP da nova impressora principal.

Nota: Certifique-se de que o nome do host ou endereço IP da impressora de backup esteja correto.

- d Clique em **Aplicar**.

Utilizando a página de status da impressora principal

- a** A partir do Embedded Web Server da nova impressora principal, acesse a página de status do aplicativo.
- b** No seção Clientes, clique em **Adicionar clientes**.
- c** Digite o endereço IP da impressora de cliente e, em seguida, adicione-a.

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 Siga as instruções exibidas no visor.

Como registrar um PIN

Antes de começar, certifique-se de que o método de login esteja definido para oferecer suporte à autenticação por PIN.

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

Efetuar login na impressora manualmente

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

Nota: Ao selecionar **Login de admin**, não é possível recuperar outras informações sobre o usuário do servidor LDAP.

- 2 Digite suas credenciais de login.

Nota: Se você estiver usando Kerberos, Active Directory®, ou LDAP + GSSAPI para login manual, 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 registro do sistema

- 1 No Embedded Web Server, clique em **Configurações** ou **Configuração**.
- 2 Dependendo do modelo da sua impressora, faça o seguinte:
 - Clique em **Apps > Gerenc. de apps**.
 - Clique em **Soluções de dispositivo > Soluções (eSF)**.
 - Clique em **Soluções incorporadas**.
- 3 Clique em **Sistema > Log**.
- 4 Selecione e envie os filtros apropriados.
- 5 Analise o registro e solucione o problema.

Entre em contato com o seu representante da Lexmark

O aplicativo não é executado com a versão atualizada da Liberação de impressão SaaS

Experimente uma ou mais das seguintes opções:

Certifique-se de que a Liberação de impressão esteja configurada apropriadamente

Se você tiver atualizado o aplicativo de Gerenciamento de impressão SaaS para Liberação de impressão v2.0 ou posterior, certifique-se de desativar o descanso de tela. Atribua o controle de acesso de autenticação de cartão à Liberação de impressão e certifique-se de que a Liberação de impressão esteja configurada apropriadamente. Para obter mais informações, consulte o *Guia do Administrador de Liberação de Impressão*.

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 **Configurações** ou **Configuração**.
- 2 Clique em **Definições gerais > Tempos limite**.
- 3 Aumente o tempo limite da tela e do modo de suspensão.
- 4 Clique em **Enviar**.

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

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

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

- 1 Dependendo do modelo da impressora, a partir do Embedded Web Server, siga uma das seguintes opções:
 - Clique em **Configurações > Segurança > Configurações de segurança variadas > Restrições de login**.
 - Clique em **Configuração > Segurança**.
- 2 Aumente o tempo de bloqueio e o número permitido de falhas de login ou a espera para desconexão automática.
- 3 Clique em **Enviar**.

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 "[Configurando a autenticação de usuário com base na impressora](#)" na página 9.

Certifique-se de não exceder 23 impressoras de cliente registradas

Para obter mais informações, consulte "[Gerenciando contas de usuário e impressoras de cliente](#)" na página 17.

Entre em contato com o seu representante da Lexmark

Não é possível validar o cartão

Experimente uma ou mais das seguintes opções:

Defina o Método de login como Cartão ou Login manual

- 1 No Embedded Web Server, acesse a página de configuração do aplicativo.
- 2 A partir da seção Tela de login, defina o método de login para **Cartão ou login manual**.
- 3 Clique em **Aplicar**.

Entre em contato com o seu representante da Lexmark

Não é possível encontrar informações do domínio

Experimente uma ou mais das seguintes opções:

Alguns métodos de login para login manual ou registro de cartão, como contas locais ou LDAP, não exigem seleção de domínio. Os métodos de login que exigem seleção de domínio são Kerberos, Active Directory e LDAP+GSSAPI.

Desativar seleção de domínio

- 1 No Embedded Web Server, acesse a página de configuração do aplicativo.
- 2 Na seção Configurações Avançadas, desmarque **Utilizar domínio selecionado**.
- 3 Clique em **Aplicar**.

Alterar o método de login

- 1 No Embedded Web Server, acesse a página de configuração do aplicativo.
- 2 A partir da seção Autenticação de usuário, defina o controle de acesso de registro do cartão e o controle de acesso de login manual para **Aplicativo 1** ou **Solução 1**.
- 3 Clique em **Aplicar**.

Entre em contato com o seu representante da Lexmark

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 "[Configurando definições LDAP](#)" na página 15.

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.

Será possível remover uma impressora do cliente e transferi-la para sua nova impressora principal se a impressora principal atual estiver off-line?

Sim, faça o seguinte:

- 1 A partir do Embedded Web Server da impressora do cliente, reinstale o aplicativo.
- 2 Defina a função como impressora de cliente e configure-a para suas novas impressoras principal e de backup. Para obter mais informações, consulte "[Como configurar a função da impressora](#)" na página 10.

E se eu desinstalar acidentalmente o aplicativo da impressora?

- 1 A partir do Embedded Web Server, reinstale o aplicativo.
- 2 Defina uma função para a impressora. Para obter mais informações, consulte "[Como configurar a função da impressora](#)" na página 10.

Nota: Certifique-se de configurar a impressora principal, a impressora de backup e as impressoras de cliente consecutivamente.

- 3 Dependendo da função, configure a impressora.

Notas:

- Se o aplicativo for reinstalado em uma impressora principal, atribua-a para sua impressora de backup.
- Se o aplicativo for reinstalado em uma impressora de backup, atribua-a para sua impressora principal.
- Se o aplicativo for reinstalado em uma impressora de cliente, atribua-a para sua impressora principal e sua impressora de backup.
- Para obter mais informações, consulte "[Reatribuir funções da impressora](#)" na página 18.

Por que não estou visualizando um botão de cópia ou fax na tela de bloqueio mesmo tendo ativado essas funções sem fazer login?

Defina o controle de acesso da função de cópia ou fax para **Sem segurança**. Para obter mais informações, consulte "[Configurar tela de login](#)" na página 8.

O que ocorrerá se eu tiver os mesmos controles de acesso para controle de acesso de login manual e para controle de acesso de sessão?

Para acessar as funções da impressora a partir da tela inicial, será necessário inserir as credenciais ao fazer login manualmente.

Posso ter diferentes controles de acesso para controle de acesso de login manual e para validação de cartão?

Sim, exceto quando utilizar autenticação de Serviço de identidade e depois definir o Controle de acesso de login manual e a Validação de cartão como **Serviço de identidade**.

Por que o recurso Login de admin não funciona com contas de rede?

O recurso **Login de admin** é aplicável apenas aos modelos de segurança de Contas Internas, PIN e Senha.

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.

Para informações sobre suprimentos e downloads, vá até www.lexmark.com.

© 2014 Lexmark International, Inc.

Todos os direitos reservados.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

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

- acessando a página de configuração 8
- acesso
 - página de status 17
- acesso ao Embedded Web Server 5
- adição
 - impressoras cliente 17
 - usuários 20
- adicionando uma conta de usuário interna 5
- arquivo de configuração
 - exportando ou importando 16
- ativando um sinal sonoro depois do login 15
- atribuindo a impressora de backup 18
- autenticação de usuário com base na impressora
 - como configurar 9
- autenticação de usuário do serviço da Web
 - como configurar 10
- Autenticação de usuário do serviço de identidade
 - como configurar 12
- autenticação do administrador
 - como configurar 8
- Autenticação do usuário do PIN
 - como configurar 13
- Autenticação do usuário LDAP
 - como configurar 14

C

- como configurar
 - impressoras 10
 - método de login 8
 - tela de login 8
- como exportar um arquivo de configuração 16
- como importar um arquivo de configuração 16
- como registrar um PIN 20
- configuração das preferências do aplicativo 15
- configuração de autenticação do administrador 8

- configuração de controles de acesso 6
- configuração de domínios
 - métodos de login 15
- configurando a autenticação de usuário com base na impressora 9
- configurando a autenticação de usuário do serviço da Web 10
- configurando a autenticação de usuário do serviço de identidade 12
- configurando autenticação do usuário LDAP 14
- configurando autenticação do usuário PIN 13
- configurando definições de PIN 14
- configurando definições do serviço da Web 11
- configurando definições do serviço de identidades 13
- configurando definições LDAP 15
- configurando uma nova impressora principal 18
- configurar grupos para uma conta interna de usuário 5
- contas de usuário
 - excluir 17
- contas de usuário internas
 - adição 5
 - agrupamento 5
- controles de acesso
 - como configurar 6
- criação de modelos de segurança 6

D

- definições de LDAP
 - como configurar 15
- definições de PIN
 - como configurar 14
- definições do serviço da Web
 - como configurar 11
- Definições do Serviço de identidade
 - como configurar 13

E

- efetuar login na impressora manualmente 20
- Embedded Web Server
 - acesso 5
- erro de autenticação 22
- erro do aplicativo 21
- excluir
 - contas de usuário 17
 - impressoras cliente 17
- exibindo domínios para contas de usuário 15

F

- funções da impressora
 - reatribuir 18

I

- impressora de backup
 - atribuição 18
 - como configurar 10
- impressora principal
 - como configurar 10
- impressoras
 - como configurar 10
- impressoras cliente
 - adição 17
 - como configurar 10
 - excluir 17
 - migrar 18

L

- login
 - manual 20
 - PIN 20
- login com PIN 20
- login manual 20

M

- mensagens de registro
 - configuração 15
- método de login
 - como configurar 8
- migrar
 - impressoras cliente 18
- modelos de segurança
 - criação 6

N

não é possível conectar ao servidor LDAP 24
não é possível encontrar informações do domínio. 23
não é possível registrar uma impressora cliente 22
não é possível validar o cartão 23
nova impressora principal como configurar 18

O

o usuário está bloqueado 22

P

página de configurações do aplicativo
 acesso 8
página de status
 acesso 17
perfil de login
 usando 15
perguntas frequentes 25
PIN
 registro 20
preferências do aplicativo
 configuração 15

R

reatribuir funções da impressora 18
registro de usuários 20

S

solução de problemas
 erro de autenticação 22
 erro do aplicativo 21
 não é possível conectar ao servidor LDAP 24
 não é possível encontrar informações do domínio. 23
 não é possível registrar uma impressora cliente 22
 não é possível validar o cartão 23
 o usuário está bloqueado 22

T

tela de login
 como configurar 8

U

usuários
 adição 20
 registro 20
utilizando a função de cópia sem efetuar login 8
utilizando a função de fax sem efetuar login 8
utilizando um perfil de login 15

V

visão geral 4