Guia de Recursos de Segurança

Índice

Introdução

Definições das observações

Nós usamos os símbolos e convenções a seguir ao longo de todo este Manual do Usuário:

IMPORTANTE	IMPORTANTE indica uma situação de risco em potencial que, se não for evitada, pode causar danos à propriedade ou perda de funcionalidade do produto.
OBSERVAÇÃO	OBSERVAÇÃO especifica o ambiente de operação, condições para instalação ou condições especiais de uso.
	Os ícones de dica apresentam informações importantes e referências complementares.
Negrito	O estilo negrito identifica os botões do painel de controle do equipamento ou da tela do computador.
Itálico	O estilo itálico destaca itens importantes ou o direciona a um tópico relacionado.

Informações relacionadas

- Introdução

Marcas comerciais

Adobe® e Reader® são marcas registradas ou marcas comerciais da Adobe Systems Incorporated nos Estados Unidos e/ou em outros países.

Toda empresa cuja titularidade de software é mencionada neste manual possui um Contrato de Licença de Software específico para os programas de sua propriedade.

Todos os nomes comerciais e de produtos de empresas que aparecem em produtos Brother, em documentos relacionados e em outros materiais são marcas comerciais ou marcas registradas dessas respectivas empresas.

Informações relacionadas

- Introdução

Direitos autorais

Informações relacionadas

- Introdução

Antes de usar recursos de segurança de rede

Seu equipamento emprega alguns dos mais recentes protocolos de segurança de rede e criptografia disponíveis atualmente. Esses recursos de rede podem ser integrados ao seu plano geral de segurança de rede para reforçar a proteção de dados e evitar o acesso não autorizado ao equipamento.

Recomendamos que desabilite os protocolos FTP e TFTP. O acesso ao equipamento com o uso desses protocolos não é seguro.

Informações relacionadas

- Introdução
  - Desative protocolos desnecessários

Desative protocolos desnecessários

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

   A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.
4. Clique em **Rede** > **Rede** > **Protocolo** na barra de navegação à esquerda.

   Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ☰.
5. Desmarque todas as caixas de seleção de protocolos desnecessários para desativá-los.
6. Clique em **Enviar**.
7. Reinicie o equipamento Brother para ativar a configuração.

Informações relacionadas

- Antes de usar recursos de segurança de rede

Segurança de rede

- Configurar certificados para a segurança do dispositivo
- Usar SSL/TLS
- Usar SNMPv3
- Usar IPsec
- Usar a autenticação IEEE 802.1x em sua rede

Configurar certificados para a segurança do dispositivo

Você deve configurar um certificado para gerenciar seu equipamento em rede com segurança usando SSL/TLS. Você precisa utilizar o Gerenciamento via Web para configurar um certificado.

- Visão geral dos recursos do certificado de segurança
- Como criar e instalar um certificado
- Criar um certificado autoassinado
- Criar uma Solicitação de assinatura de certificado (CSR) e instalar um certificado de uma Autoridade de Certificação (CA)
- Importar e exportar o certificado e a chave privada
- Importar e exportar um certificado da CA

Visão geral dos recursos do certificado de segurança

seu equipamento é compatível com vários certificados de segurança, o que permite uma autenticação e uma comunicação seguras com o equipamento. Os recursos do certificado de segurança a seguir podem ser usados com o equipamento:

Os recursos, opções e configurações compatíveis podem ser diferentes dependendo do modelo.

- Comunicação SSL/TLS
- Autenticação IEEE 802.1x
- IPsec

Seu equipamento oferece suporte para o seguinte:

- Certificado pré-instalado

  Seu equipamento possui um certificado pré-instalado e autoassinado. Este certificado permite utilizar a comunicação SSL/TLS sem criar ou instalar um certificado diferente.

O certificado autoassinado pré-instalado protege sua comunicação até um determinado nível. Recomendamos o uso de um certificado emitido por uma organização confiável para garantir mais segurança.

- Certificado autoassinado

  Este servidor de impressão emite seu próprio certificado. Usando esse certificado, você pode usar a comunicação SSL/TLS com facilidade, sem criar ou instalar um certificado diferente de uma autoridade de certificação.
- Certificado de uma autoridade de certificação (CA)

  Existem dois métodos para instalar um certificado de CA. Se você já possui um certificado de uma CA ou deseja usar um certificado de uma CA confiável externa:
  - Quando estiver usando uma solicitação de assinatura de certificado (CSR) a partir deste servidor de impressão.
  - Quando importar um certificado e uma chave privada.
- Certificado da CA (Autoridade de certificação)

  Para utilizar um certificado da CA que identifique a CA e possua sua própria chave privada, você precisa importar esse certificado da CA diretamente dessa autoridade, antes de configurar os recursos de segurança de rede.

- Se você utilizar a comunicação SSL/TLS, recomendamos primeiro entrar em contato com o administrador de seu sistema.
- Quando você restaura as configurações padrão de fábrica do servidor de impressão, o certificado e a chave privada que foram instalados são excluídos. Se você quiser manter o mesmo certificado e a chave privada depois de restaurar o servidor de impressora, exporte-os antes da restauração e depois reinstale-os.

Informações relacionadas

- Configurar certificados para a segurança do dispositivo

Tópicos relacionados:

- Configure a autenticação IEEE 802.1x para sua rede usando o gerenciamento via Web (navegador da Web)

Como criar e instalar um certificado

Você tem duas opções ao escolher um certificado de segurança: usar um certificado autoassinado ou usar um certificado emitido por uma Autoridade de certificação (CA).

Opção 1

Certificado autoassinado

1. Crie um certificado autoassinado usando o Gerenciamento via Web.
2. Instale o certificado autoassinado em seu computador.

Opção 2

Certificado de uma CA

1. Crie uma CSR (Solicitação de assinatura de certificado) usando o Gerenciamento via Web.
2. Instale o certificado emitido pela CA no equipamento Brother usando o Gerenciamento via Web.
3. Instale o certificado em seu computador.

Informações relacionadas

- Configurar certificados para a segurança do dispositivo

Criar um certificado autoassinado

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

   A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.
4. Clique em **Rede** > **Segurança** > **Certificado** na barra de navegação à esquerda.

   Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ≡.
5. Clique em **Criar certificado autoassinado**.
6. Insira um **Nome comum** e uma **Data válida**.
   - O **Nome comum** deve ter menos de 64 bytes. Insira um identificador, como um endereço IP, nome de nó ou nome de domínio, para ser usado quando você acessar este equipamento por meio de comunicação SSL/TLS. O nome do nó é exibido por padrão.
   - Um aviso aparecerá na tela se você usar o protocolo IPPS ou HTTPS e digitar no URL um nome diferente do **Nome comum** usado para o certificado autoassinado.
7. Selecione sua configuração na lista suspensa **Algoritmo de chave pública**.
8. Selecione sua configuração na lista suspensa **Algoritmo Digest**.
9. Clique em **Enviar**.

Informações relacionadas

- Configurar certificados para a segurança do dispositivo

Criar uma Solicitação de assinatura de certificado (CSR) e instalar um certificado de uma Autoridade de Certificação (CA)

Se você já tiver um certificado de uma Autoridade de Certificação (CA) confiável externa, poderá armazenar o certificado e a chave privada no seu equipamento e gerenciá-los usando importação e exportação. Se não tiver um certificado de uma CA externa confiável, crie uma Solicitação de assinatura de certificado (CSR), envie a CSR à CA para autenticação e instale o certificado que a CA emitirá no seu equipamento.

- Criar uma CSR (Solicitação de Assinatura de Certificado)
- Instalar um certificado no seu equipamento

Criar uma CSR (Solicitação de Assinatura de Certificado)

Uma CSR (Solicitação de assinatura de certificado) é uma solicitação enviada a uma CA (Autoridade de certificação) para autenticação das credenciais contidas no certificado.

Recomendamos que você instale um Certificado raiz da CA em seu computador antes de criar a CSR.

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.

4. Clique em **Rede** > **Segurança** > **Certificado** na barra de navegação à esquerda.

Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ☰.

5. Clique em **Criar CSR**.
6. Digite um **Nome comum** (obrigatório) e adicione outras informações sobre sua **Organização** (opcional).

- As informações de sua empresa são necessárias para que uma Autoridade de certificação possa confirmar sua identidade e comprová-la para as outras pessoas.
- O **Nome comum** deve ter menos de 64 bytes. Insira um identificador, como um endereço IP, nome de nó ou nome de domínio, para ser usado quando você acessar este equipamento por meio de comunicação SSL/TLS. O nome do nó é exibido por padrão. O **Nome comum** é obrigatório.
- Um aviso aparecerá na tela se você digitar no URL um nome diferente do Nome comum usado para o certificado.
- As opções de **Organização**, **Unidade de organização**, **Cidade/localidade** e **Estado/província** devem ter menos de 64 bytes.
- O **País/região** deve conter um código de país de dois caracteres no formato ISO 3166.
- Se estiver configurando uma extensão de certificado X.509v3, marque a caixa de seleção **Configurar partição estendida** e depois selecione **Auto. (registrar IPv4)** ou **Manual**.

7. Selecione sua configuração na lista suspensa **Algoritmo de chave pública**.
8. Selecione sua configuração na lista suspensa **Algoritmo Digest**.
9. Clique em **Enviar**.

   A CSR aparece na tela. Salve a CSR como um arquivo ou copie e cole seus dados em um formulário de CSR online oferecido por uma Autoridade de Certificação.
10. Clique em **Salvar**.

- Siga a política de sua CA quanto ao método de envio de uma CSR à CA.
- Se estiver usando a Autoridade de certificação raiz corporativa do Windows Server, recomendamos que você use o servidor web para assegurar que o modelo de certificado criará o certificado de cliente com segurança. Se estiver criando um Certificado de Cliente para um ambiente IEEE 802.1x com autenticação EAP-TLS, recomendamos que você use Usuário para o modelo de certificado.

Informações relacionadas

- Criar uma Solicitação de assinatura de certificado (CSR) e instalar um certificado de uma Autoridade de Certificação (CA)

Instalar um certificado no seu equipamento

Quando receber um certificado de uma Autoridade Certificadora (AC), siga os passos abaixo para instalá-lo no servidor de impressão:

Apenas um certificado emitido com Solicitação de Assinatura do Certificado (CSR) do seu equipamento pode ser instalado nele. Se quiser criar outra CSR, confirme se o certificado já está instalado antes de criar a nova CSR. Criar outro CSR somente após a instalação do certificado no equipamento, caso contrário, o CSR criado antes da instalação do novo CSR será inválido.

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

   A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.
4. Clique em **Rede** > **Segurança** > **Certificado** na barra de navegação à esquerda.

   Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ☰.
5. Clique em **Instalar certificado**.
6. Navegue até o arquivo que contém o certificado emitido pela CA e depois clique em **Enviar**.

   O certificado foi criado e salvo na memória do seu equipamento.

Para usar comunicação SSL/TLS, você precisa ter o Certificado raiz da CA instalado em seu computador. Entre em contato com o administrador da rede.

Informações relacionadas

- Criar uma Solicitação de assinatura de certificado (CSR) e instalar um certificado de uma Autoridade de Certificação (CA)

Importar e exportar o certificado e a chave privada

Armazene o certificado e a chave privada no seu equipamento e gerencie-os, importando e exportando-os conforme necessário.

- Importar um certificado e uma chave privada
- Exportar o certificado e a chave privada

Importar um certificado e uma chave privada

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

   A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.
4. Clique em **Rede** > **Segurança** > **Certificado** na barra de navegação à esquerda.

   Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ☰.
5. Clique em **Importar certificado e chave privada**.
6. Navegue e selecione o arquivo que deseja importar.
7. Digite a senha se o arquivo for criptografado e clique em **Enviar**.

O certificado e a chave privada são importados no seu equipamento.

Informações relacionadas

- Importar e exportar o certificado e a chave privada

Exportar o certificado e a chave privada

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

> A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.

4. Clique em **Rede** > **Segurança** > **Certificado** na barra de navegação à esquerda.

> Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ≡.

5. Clique em **Exportar** quando a **Lista de certificados** for exibida.
6. Insira a senha se quiser criptografar o arquivo.

   Se a senha for deixada em branco, o arquivo gerado não será criptografado.
7. Insira novamente a senha para confirmá-la e clique em **Enviar**.
8. Clique em **Salvar**.

O certificado e a chave privada são exportados para o seu computador.

Você também pode importar o certificado no seu computador.

Informações relacionadas

- Importar e exportar o certificado e a chave privada

Importar e exportar um certificado da CA

Você pode importar, exportar e armazenar certificados da CA no seu equipamento Brother.

- Importar um certificado da CA
- Exportar um certificado da CA

Importar um certificado da CA

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.

4. Clique em **Rede** > **Segurança** > **Certificado da CA** na barra de navegação à esquerda.

Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ≡.

5. Clique em **Importar certificado da CA**.
6. Navegue até o arquivo que você deseja importar.
7. Clique em **Enviar**.

Informações relacionadas

- Importar e exportar um certificado da CA

Exportar um certificado da CA

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.

4. Clique em **Rede** > **Segurança** > **Certificado da CA** na barra de navegação à esquerda.

Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ≡.

5. Selecione o certificado que você deseja exportar e clique em **Exportar**.
6. Clique em **Enviar**.

Informações relacionadas

- Importar e exportar um certificado da CA

Usar SSL/TLS

- Gerenciar seu equipamento em rede com segurança usando SSL/TLS
- Imprimir documentos com segurança usando SSL/TLS
- Enviar ou receber um e-mail com segurança usando SSL/TLS

Gerenciar seu equipamento em rede com segurança usando SSL/TLS

- Configurar um certificado para SSL/TLS e protocolos disponíveis
- Acessar o Gerenciamento via Web usando SSL/TLS
- Instalar o Certificado Autoassinado para Usuários do Windows como Administradores
- Configurar certificados para a segurança do dispositivo

Configurar um certificado para SSL/TLS e protocolos disponíveis

Configure um certificado no seu equipamento usando o Gerenciamento via Web antes de usar a comunicação SSL/TLS.

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

   A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.
4. Clique em **Rede** > **Rede** > **Protocolo** na barra de navegação à esquerda.

   Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ≡.
5. Clique em **Configurações do servidor HTTP**.
6. Selecione o certificado que você deseja configurar na lista suspensa **Selecionar o certificado**.
7. Clique em **Enviar**.
8. Clique em **Sim** para reiniciar o servidor de impressão.

Informações relacionadas

- Gerenciar seu equipamento em rede com segurança usando SSL/TLS

Tópicos relacionados:

- Imprimir documentos com segurança usando SSL/TLS

Acessar o Gerenciamento via Web usando SSL/TLS

Para gerenciar seu equipamento em rede com segurança, você precisa usar utilitários de gerenciamento com protocolos de segurança.

- Para usar o protocolo HTTPS, a opção HTTPS deve ser ativada no equipamento. O protocolo HTTPS está habilitado por padrão.
- Você pode alterar as configurações do protocolo HTTPS usando a tela do Gerenciamento via Web.

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

   A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.
4. Você agora pode acessar o equipamento usando HTTPS.

Informações relacionadas

- Gerenciar seu equipamento em rede com segurança usando SSL/TLS

Instalar o Certificado Autoassinado para Usuários do Windows como Administradores

- Os seguintes passos são para o Microsoft Edge. Se você usar outro navegador da web, consulte a documentação ou a ajuda on-line dele para obter instruções sobre como instalar certificados.
- Certifique-se de ter criado seu certificado autoassinado usando o Gerenciamento via Web.

1. Clique com o botão direito do mouse no ícone **Microsoft Edge** e depois clique em **Executar como administrador**.

   Se a tela **Controle de Conta de Usuário** for exibida, clique em **Sim**.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se sua conexão não for privada, clique no botão **Avançado** e depois continue na página web.
4. Se necessário, digite a senha no campo **Login** e clique em **Login**.

   A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.
5. Clique em **Rede** > **Segurança** > **Certificado** na barra de navegação à esquerda.

   Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ≡.
6. Clique em **Exportar**.
7. Para criptografar o arquivo de saída, digite uma senha no campo **Inserir senha**. Se o campo **Inserir senha** estiver em branco, seu arquivo de saída não será criptografado.
8. Digite a senha novamente no campo **Confirmar senha** e clique em **Enviar**.
9. Clique no arquivo baixado para abri-lo.
10. Quando o **Assistente para Importação de Certificados** for exibido, clique em **Avançar**.
11. Clique em **Avançar**.
12. Se necessário, digite uma senha e depois clique em **Avançar**.
13. Selecione **Colocar todos os certificados no repositório a seguir** e clique em **Procurar...**.
14. Selecione o **Autoridades de Certificação Raiz Confiáveis** e depois clique em **OK**.
15. Clique em **Avançar**.
16. Clique em **Concluir**.
17. Clique em **Sim** se a impressão digital (do polegar) estiver correta.
18. Clique em **OK**.

Informações relacionadas

- Gerenciar seu equipamento em rede com segurança usando SSL/TLS

Imprimir documentos com segurança usando SSL/TLS

- Imprimir documentos usando IPPS
- Configurar um certificado para SSL/TLS e protocolos disponíveis
- Configurar certificados para a segurança do dispositivo

Imprimir documentos usando IPPS

Para imprimir documentos com segurança com o protocolo IPP, use o protocolo IPPS.

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

   A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.
4. Clique em **Rede** > **Rede** > **Protocolo** na barra de navegação à esquerda.

   Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ≡.
5. Confirme se a caixa de seleção **IPP** está marcada.

   Se a caixa de seleção **IPP** não estiver marcada, marque a caixa de seleção **IPP** e clique em **Enviar**.

   Reinicie o equipamento para ativar a configuração.

   Depois que o equipamento for reiniciado, retorne à página do equipamento na Web, digite a senha e, na barra de navegação à esquerda, clique em **Rede** > **Rede** > **Protocolo**.
6. Clique em **Configurações do servidor HTTP**.
7. Marque a caixa de seleção **HTTPS(Port 443) (HTTPS(Porta 443))** na área **IPP** e clique em **Enviar**.
8. Reinicie o equipamento para ativar a configuração.

A comunicação usando IPPS não impede o acesso não autorizado ao servidor de impressão.

Informações relacionadas

- Imprimir documentos com segurança usando SSL/TLS

Usar SNMPv3

- Gerenciar seu equipamento de rede com segurança usando o SNMPv3

Gerenciar seu equipamento de rede com segurança usando o SNMPv3

O protocolo SNMPv3 (Simple Network Management Protocol versão 3) oferece autenticação de usuário e criptografia de dados para gerenciar dispositivos de rede com segurança.

1. Inicie o navegador da Web.
2. Digite “https://Nome comum” na barra de endereços do navegador (onde “Nome comum” é o Nome comum que você atribuiu ao certificado, o qual pode ser seu endereço IP, nome do nó ou nome do domínio).
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.

4. Clique em **Rede** > **Rede** > **Protocolo** na barra de navegação à esquerda.

Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ≡.

5. Confirme se a opção **SNMP** está habilitada e clique em **Config. avançadas**.
6. Ajuste as configurações de modo SNMPv1/v2c.

Opção	Descrição
Acesso de leitura/gravação SNMP v1/v2c	O servidor de impressão usa as versões 1 e 2c do protocolo SNMP. Você pode usar todos os aplicativos do seu equipamento neste modo. Entretanto, ele não é seguro porque não autentica o usuário e os dados não são criptografados.
Acesso somente leitura SNMP v1/v2c	O servidor de impressão usa o acesso apenas leitura das versões 1 e 2c do protocolo SNMP.
Desativado	Desative a versão 1 e a versão 2c do protocolo SNMP. Todos os aplicativos que usam SNMPv1/v2c serão restritos. Para usar aplicativos SNMPv1/v2c, use o modo **Acesso somente leitura SNMP v1/v2c** ou **Acesso de leitura/gravação SNMP v1/v2c**.

7. Ajustar as configurações do modo SNMPv3.

Opção	Descrição
Ativado	O servidor de impressão usa a versão 3 do protocolo SNMP. Para gerenciar o servidor de impressão com segurança, use o modo SNMPv3.
Desativado	Desative a versão 3 do protocolo SNMP. Todos os aplicativos que usam SNMPv3 serão restritos. Para permitir o uso de aplicativos SNMPv3, use o modo SNMPv3.

8. Clique em **Enviar**.

Se o seu equipamento exibir as opções de configuração de protocolo, selecione as opções desejadas.

9. Reinicie o equipamento para ativar a configuração.

Informações relacionadas

- Usar SNMPv3

Usar IPsec

- Introdução ao IPsec
- Configurar IPsec usando o Gerenciamento via Web
- Configurar um modelo de endereço IPsec usando o Gerenciamento via Web
- Configurar um modelo IPsec usando o Gerenciamento via Web

Introdução ao IPsec

IPsec (Segurança de Protocolo IP) é um protocolo de segurança que usa uma função opcional de Protocolo de Internet para evitar a manipulação de dados e assegurar a confidencialidade dos dados transmitidos como pacotes IP. O IPsec codifica os dados transmitidos pela rede, como os dados de impressão enviados dos computadores para uma impressora. Como os dados estão codificados na camada da rede, os aplicativos que utilizam um protocolo de nível superior utilizam o IPsec mesmo que o usuário não esteja ciente disso.

O protocolo IPsec suporta as seguintes funções:

- Transmissões de IPsec

  De acordo com as condições de configuração de IPsec, o computador conectado à rede envia e recebe dados para/do dispositivo especificado usando Ipsec. Quando os dispositivos iniciam a comunicação usando IPsec, primeiro as chaves são trocadas usando Protocolo IKE (Troca de Chave de Internet) e depois os dados criptografados são transmitidos usando as chaves.

  Além disso, o protocolo IPsec possui dois modos de operação: o modo de Transporte e o modo de Túnel. O modo de Transporte é usado principalmente para comunicações entre dispositivos, e o modo de Túnel é usado em ambientes como VPNs (Redes privadas virtuais).

  As seguintes condições são necessárias para transmissões com o protocolo IPsec:
  - Um computador que possa se comunicar usando IPsec deve estar conectado à rede.
  - Seu equipamento deve estar configurado para comunicação IPsec.
  - O computador conectado ao seu equipamento deve estar configurado para conexões IPsec.

- Configurações de IPsec

  As configurações necessárias para conexões via IPsec. Essas configurações podem ser definidas a partir do Gerenciamento via Web.

  Para definir as configurações de IPsec, é necessário utilizar o navegador em um computador conectado à rede.

Informações relacionadas

- Usar IPsec

Configurar IPsec usando o Gerenciamento via Web

As condições de conexão IPsec incluem dois **Modelo** tipos: **Endereço** e **IPsec**. Você pode configurar até dez condições de conexão.

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

   A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.
4. Clique em **Rede** > **Segurança** > **IPsec** na barra de navegação à esquerda.

   Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ☰.
5. Defina as configurações.

Opção	Descrição
Estado	Habilite ou desabilite o Ipsec.
Modo de negociação	Selecione **Modo de negociação** para IKE Fase 1. O IKE é um protocolo usado para a troca de chaves de criptografia em comunicações criptografadas que utilizam IPsec. No modo **Principal**, a velocidade de processamento é baixa, mas o nível de segurança é alto. No modo **Aggressive**, a velocidade de processamento é mais rápida que no modo **Principal**, mas o nível de segurança é mais baixo.
Todo o tráfego não IPsec	Selecione a ação a ser executada para pacotes não-IPsec. Ao usar o Web Services, você precisa selecionar **Permitir** para **Todo o tráfego não IPsec**. Se você selecionar **Remover**, o Web Services não poderá ser usado.
Bypass de transm./multicast	Selecione **Ativado** ou **Desativado**.
Bypass de protocolo	Marque as caixas de seleção das opções desejadas.
Regras	Marque a caixa de seleção **Ativado** para ativar o modelo. Quando você marcar várias caixas de seleção, as caixas de seleção com os números menores terão prioridade se as configurações das opções selecionadas forem conflitantes. Clique na lista suspensa correspondente para selecionar o **Modelo de endereço** usado para as condições da conexão IPsec. Para adicionar um **Modelo de endereço**, clique em **Adicionar modelo**. Clique na lista suspensa correspondente para selecionar o **Modelo IPsec** usado para as condições da conexão IPsec. Para adicionar um **Modelo IPsec**, clique em **Adicionar modelo**.

6. Clique em **Enviar**.

   Se o equipamento tiver que ser reiniciado para ativar as novas configurações, a tela de confirmação da reinicialização será exibida.

   Se houver um item em branco no modelo que você habilitou na tabela **Regras**, uma mensagem de erro será exibida. Confirme suas opções e clique em **Enviar** novamente.

Informações relacionadas

- Usar IPsec

Tópicos relacionados:

- Configurar certificados para a segurança do dispositivo

Configurar um modelo de endereço IPsec usando o Gerenciamento via Web

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.

4. Clique em **Rede** > **Segurança** > **Modelo de endereço IPsec** na barra de navegação à esquerda.

Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ≡.

5. Clique no botão **Excluir** para excluir um **Modelo de endereço**. Se um **Modelo de endereço** estiver sendo utilizado, ele não poderá ser excluído.
6. Clique no **Modelo de endereço** que você deseja criar. O **Modelo de endereço IPsec** é exibido.
7. Defina as configurações.

Opção	Descrição
Nome do modelo	Digite um nome para o modelo (até 16 caracteres).
Endereço IP local	• **Endereço IP** Especifique o endereço IP. Selecione **TODOS os endereços IPv4**, **TODOS os endereços IPv6**, **TODOS os links locais IPv6** ou **Personaliz.** na lista suspensa. Se você selecionar **Personaliz.** na lista suspensa, digite o endereço IP (IPv4 ou IPv6) na caixa de texto. • **Interv. de endereços IP** Digite os endereços de IP inicial e final para o intervalo de endereços IP nas caixas de texto. Se os endereços IP inicial e final não seguirem o padrão IPv4 ou IPv6, ou se o endereço IP final for menor que o endereço inicial, um erro ocorrerá. • **Endereço IP/Prefixo** Especifique o endereço IP usando a notação CIDR. Por exemplo: 192.168.1.1/24 Como o prefixo foi especificado no formato de uma máscara de subrede de 24 bits (255.255.255.0) para 192.168.1.1, os endereços 192.168.1.### são válidos.
Endereço IP remoto	• **Qualquer** Se você selecionar **Qualquer**, todos os endereços IP serão habilitados. • **Endereço IP** Digite o endereço IP especificado (IPv4 ou IPv6) na caixa de texto. • **Interv. de endereços IP** Digite o primeiro e o último endereço IP para a faixa de endereços IP. Se o primeiro e último endereço IP não forem

Opção	Descrição
	padronizados para IPv4 ou IPv6 ou se o último endereço IP for menor que o primeiro, ocorrerá um erro. • **Endereço IP/Prefixo** Especifique o endereço IP usando a notação CIDR. Por exemplo: 192.168.1.1/24 Como o prefixo foi especificado no formato de uma máscara de subrede de 24 bits (255.255.255.0) para 192.168.1.1, os endereços 192.168.1.### são válidos.

8. Clique em **Enviar**.

Se alterar as configurações do modelo que está em uso, reinicie o equipamento para ativar as novas configurações.

Informações relacionadas

- Usar IPsec

Configurar um modelo IPsec usando o Gerenciamento via Web

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

   A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.
4. Clique em **Rede** > **Segurança** > **Modelo IPsec** na barra de navegação à esquerda.

   Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ≡.
5. Clique no botão **Excluir** para excluir um **Modelo IPsec**. Se um **Modelo IPsec** estiver sendo utilizado, ele não poderá ser excluído.
6. Clique no **Modelo IPsec** que você deseja criar. A tela **Modelo IPsec** é exibida. Os campos de configuração variam de acordo com as configurações feitas por você em **Usar modelo prefixado** e **Internet Key Exchange (IKE)**.
7. No campo **Nome do modelo**, digite um nome para o modelo (no máximo 16 caracteres).
8. Se tiver selecionado **Personaliz.** na lista suspensa **Usar modelo prefixado**, selecione as opções do **Internet Key Exchange (IKE)** e depois altere as configurações, se necessário.
9. Clique em **Enviar**.

Informações relacionadas

- Usar IPsec
  - Configurações IKEv1 para um modelo IPsec
  - Configurações IKEv2 para um modelo IPsec
  - Configurações manuais para um modelo IPsec

Configurações IKEv1 para um modelo IPsec

Opção	Descrição
Nome do modelo	Digite um nome para o modelo (até 16 caracteres).
Usar modelo prefixado	Selecione **Personaliz.**, **IKEv1 alta segurança** ou **IKEv1 média segurança**. As opções de configuração variam de acordo com o modelo selecionado.
Internet Key Exchange (IKE)	O IKE é um protocolo de comunicação usado para a troca de chaves de criptografia em comunicações criptografadas que utilizam IPsec. Para que a comunicação criptografada ocorra apenas naquele momento, o algoritmo de criptografia necessário para o IPsec é determinado e as chaves de criptografia são compartilhadas. Com o IKE, as chaves de criptografia são compartilhadas por meio do método de troca de chaves Diffie-Hellman e a comunicação criptografada limitada ao IKE é realizada. Se tiver selecionado **Personaliz.** em **Usar modelo prefixado**, selecione **IKEv1**.
Tipo de autenticação	• **Diffie-Hellman Group** Este método de troca de chaves permite que chaves secretas sejam compartilhadas com segurança em uma rede desprotegida. Em vez de chaves secretas, o método de troca de chaves Diffie-Hellman usa um problema de logaritmo discreto para enviar e receber informações desprotegidas geradas a partir de um número aleatório e da chave secreta. Selecione **Grupo1**, **Grupo2**, **Grupo5** ou **Grupo14**. • **Encriptação** Selecione **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**. • **Hash** Selecione **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512**. • **SA Lifetime (Tempo de Vida da SA)** Especifica a duração da associação de segurança da IKE. Digite o tempo (segundos) e o número de quilobytes (KByte).
Encapsulating Security	• **Protocolo** Selecione **ESP**, **AH** ou **AH+ESP**. - O ESP é um protocolo para a transmissão de comunicações criptografadas usando IPsec. O protocolo ESP criptografa os dados reais (conteúdo comunicado) e inclui informações adicionais. O pacote IP é composto pelo cabeçalho e pelos dados reais criptografados, que vêm após o cabeçalho. Além dos dados criptografados, o pacote IP também inclui informações sobre o método de criptografia, a chave de criptografia, os dados de autenticação, etc. - O AH é a parte do protocolo IPsec responsável por autenticar o remetente e por impedir a manipulação dos dados, isto é, ele garante a integralidade dos dados. No pacote IP, os dados são inseridos imediatamente após o cabeçalho. Os pacotes também contêm valores de hash, que são calculados por meio de uma equação formada pelo conteúdo comunicado, a chave secreta e outros dados, para impedir a falsificação do remetente e a manipulação dos dados. Diferentemente do ESP, o conteúdo comunicado não é criptografado, e os dados são enviados e recebidos como texto simples.

Opção	Descrição
	• **Encriptação (Não disponível para a opção AH.)** Selecione **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**. • **Hash** Selecione **Nenhum**, **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512**. **Nenhum** pode ser selecionado apenas quando **ESP** é selecionado para **Protocolo**. • **SA Lifetime (Tempo de Vida da SA)** Especifique o tempo de vida da SA do IKE. Insira o tempo (em segundos) e o número de kilobytes (KByte). • **Modo de encapsulamento** Selecione **Transporte** ou **Túnel**. • **Endereço IP do roteador remoto** Digite o endereço IP (IPv4 ou IPv6) do roteador remoto. Insira essa informação apenas quando o modo **Túnel** for selecionado. A SA (Associação de Segurança) é um método de comunicação criptografada que utiliza IPsec ou IPv6 para trocar e compartilhar informações (o método de criptografia e a chave de criptografia, por exemplo) que possibilitam a criação de um canal de comunicação seguro antes da comunicação ser iniciada. SA também pode se referir a um canal virtual de comunicação criptografada que foi estabelecido. O SA usado para IPsec estabelece o método de criptografia, realiza a troca das chaves e executa a autenticação mútua de acordo com o procedimento padrão do IKE (Internet Key Exchange). O SA também é atualizado periodicamente.
Perfect Forward Secrecy (PFS)	O PFS não extrai chaves de chaves anteriores que tenham sido usadas para criptografar mensagens. Além disso, se uma chave que é usada para criptografar uma mensagem tiver sido derivada de uma chave-mãe, aquela chave-mãe não será usada para derivar outras chaves. Assim, mesmo se uma chave for comprometida, o dano será limitado apenas às mensagens que tiverem sido criptografadas com essa chave. Selecione **Ativado** ou **Desativado**.
Método de autenticação	Selecione o método de autenticação. Selecione **Chave pré-compart.** ou **Certificados**.
Chave pré-compart.	Quando a comunicação é criptografada, a chave de criptografia é trocada e compartilhada antecipadamente usando outro canal. Se você selecionou **Chave pré-compart.** para o **Método de autenticação**, digite a **Chave pré-compart.** (no máximo 32 caracteres). • **Local/Tipo de ID/ID** Selecione o tipo de ID do remetente e insira a ID. Selecione **Endereço IPv4**, **Endereço IPv6**, **FQDN**, **Endereço de e-mail** ou **Certificado** como o tipo. Se você selecionou **Certificado**, insira o nome comum do certificado no campo **ID**. • **Remoto/Tipo de ID/ID** Selecione o tipo de ID do destinatário e insira a ID. Selecione **Endereço IPv4**, **Endereço IPv6**, **FQDN**, **Endereço de e-mail** ou **Certificado** como o tipo. Se você selecionou **Certificado**, insira o nome comum do certificado no campo **ID**.
Certificado	Se tiver selecionado **Certificados** para **Método de autenticação**, selecione o certificado.

Opção	Descrição
	Você pode selecionar apenas os certificados que foram criados a partir da página **Certificado**, na tela de configuração de Segurança do Gerenciamento via Web.

Informações relacionadas

- Configurar um modelo IPsec usando o Gerenciamento via Web

Configurações IKEv2 para um modelo IPsec

Opção	Descrição
Nome do modelo	Digite um nome para o modelo (até 16 caracteres).
Usar modelo prefixado	Selecione **Personaliz.**, **IKEv2 alta segurança** ou **IKEv2 média segurança**. As opções de configuração variam de acordo com o modelo selecionado.
Internet Key Exchange (IKE)	O IKE é um protocolo de comunicação usado para a troca de chaves de criptografia em comunicações criptografadas que utilizam IPsec. Para que a comunicação criptografada ocorra apenas naquele momento, o algoritmo de criptografia necessário para o IPsec é determinado e as chaves de criptografia são compartilhadas. Com o IKE, as chaves de criptografia são compartilhadas por meio do método de troca de chaves Diffie-Hellman e a comunicação criptografada limitada ao IKE é realizada. Se tiver selecionado **Personaliz.** em **Usar modelo prefixado**, selecione **IKEv2**.
Tipo de autenticação	• **Diffie-Hellman Group** Este método de troca de chaves permite que chaves secretas sejam compartilhadas com segurança em uma rede desprotegida. Em vez de chaves secretas, o método de troca de chaves Diffie-Hellman usa um problema de logaritmo discreto para enviar e receber informações desprotegidas geradas a partir de um número aleatório e da chave secreta. Selecione **Grupo1**, **Grupo2**, **Grupo5** ou **Grupo14**. • **Encriptação** Selecione **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**. • **Hash** Selecione **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512**. • **SA Lifetime (Tempo de Vida da SA)** Especifica a duração da associação de segurança da IKE. Digite o tempo (segundos) e o número de quilobytes (KByte).
Encapsulating Security	• **Protocolo** Selecione **ESP**. O ESP é um protocolo para a transmissão de comunicações criptografadas usando IPsec. O protocolo ESP criptografa os dados reais (conteúdo comunicado) e inclui informações adicionais. O pacote IP é composto pelo cabeçalho e pelos dados reais criptografados, que vêm após o cabeçalho. Além dos dados criptografados, o pacote IP também inclui informações sobre o método de criptografia, a chave de criptografia, os dados de autenticação, etc. • **Encriptação** Selecione **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**. • **Hash** Selecione **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512**. • **SA Lifetime (Tempo de Vida da SA)** Especifique o tempo de vida da SA do IKE. Insira o tempo (em segundos) e o número de kilobytes (KByte). • **Modo de encapsulamento** Selecione **Transporte** ou **Túnel**.

Opção	Descrição
	• **Endereço IP do roteador remoto** Digite o endereço IP (IPv4 ou IPv6) do roteador remoto. Insira essa informação apenas quando o modo **Túnel** for selecionado.  A SA (Associação de Segurança) é um método de comunicação criptografada que utiliza IPsec ou IPv6 para trocar e compartilhar informações (o método de criptografia e a chave de criptografia, por exemplo) que possibilitam a criação de um canal de comunicação seguro antes da comunicação ser iniciada. SA também pode se referir a um canal virtual de comunicação criptografada que foi estabelecido. O SA usado para IPsec estabelece o método de criptografia, realiza a troca das chaves e executa a autenticação mútua de acordo com o procedimento padrão do IKE (Internet Key Exchange). O SA também é atualizado periodicamente.
Perfect Forward Secrecy (PFS)	O PFS não extrai chaves de chaves anteriores que tenham sido usadas para criptografar mensagens. Além disso, se uma chave que é usada para criptografar uma mensagem tiver sido derivada de uma chave-mãe, aquela chave-mãe não será usada para derivar outras chaves. Assim, mesmo se uma chave for comprometida, o dano será limitado apenas às mensagens que tiverem sido criptografadas com essa chave. Selecione **Ativado** ou **Desativado**.
Método de autenticação	Selecione o método de autenticação. Selecione **Chave pré-compart.**, **Certificados**, **EAP - MD5** ou **EAP - MS-CHAPv2**.  O EAP é um protocolo de autenticação que é uma extensão do protocolo PPP. Quando o EAP é usado com o IEEE802.1x, uma chave diferente é usada para autenticação do usuário durante cada sessão. As configurações a seguir são necessárias apenas quando a opção **EAP - MD5** ou **EAP - MS-CHAPv2** é selecionada em **Método de autenticação**: • **Modo** Selecione **Modo de servidor** ou **Modo de cliente**. • **Certificado** Selecione o certificado. • **Nome usuár.** Digite o nome de usuário (até 32 caracteres). • **Senha** Digite a senha (até 32 caracteres). A senha deve ser inserida duas vezes para confirmação.
Chave pré-compart.	Quando a comunicação é criptografada, a chave de criptografia é trocada e compartilhada antecipadamente usando outro canal. Se você selecionou **Chave pré-compart.** para o **Método de autenticação**, digite a **Chave pré-compart.** (no máximo 32 caracteres). • **Local/Tipo de ID/ID** Selecione o tipo de ID do remetente e insira a ID. Selecione **Endereço IPv4**, **Endereço IPv6**, **FQDN**, **Endereço de e-mail** ou **Certificado** como o tipo. Se você selecionou **Certificado**, insira o nome comum do certificado no campo **ID**. • **Remoto/Tipo de ID/ID** Selecione o tipo de ID do destinatário e insira a ID.

Opção	Descrição
	Selecione **Endereço IPv4**, **Endereço IPv6**, **FQDN**, **Endereço de e-mail** ou **Certificado** como o tipo. Se você selecionou **Certificado**, insira o nome comum do certificado no campo **ID**.
Certificado	Se tiver selecionado **Certificados** para **Método de autenticação**, selecione o certificado. Você pode selecionar apenas os certificados que foram criados a partir da página **Certificado**, na tela de configuração de Segurança do Gerenciamento via Web.

Informações relacionadas

- Configurar um modelo IPsec usando o Gerenciamento via Web

Configurações manuais para um modelo IPsec

Opção	Descrição
Nome do modelo	Digite um nome para o modelo (até 16 caracteres).
Usar modelo prefixado	Selecione **Personaliz.**.
Internet Key Exchange (IKE)	O IKE é um protocolo de comunicação usado para a troca de chaves de criptografia em comunicações criptografadas que utilizam IPsec. Para que a comunicação criptografada ocorra apenas naquele momento, o algoritmo de criptografia necessário para o IPsec é determinado e as chaves de criptografia são compartilhadas. Com o IKE, as chaves de criptografia são compartilhadas por meio do método de troca de chaves Diffie-Hellman e a comunicação criptografada limitada ao IKE é realizada. Selecione **Manual**.
Chave de autenticação (ESP, AH)	Digite os valores **Entrada/Saída**. Essas configurações são necessárias quando **Personaliz.** está selecionado para **Usar modelo prefixado**, **Manual** está selecionado para **Internet Key Exchange (IKE)** e uma configuração diferente de **Nenhum** está selecionada para **Hash** na seção **Encapsulating Security**. O número de caracteres que você pode definir varia de acordo com a configuração selecionada em **Hash**, na seção **Encapsulating Security**. Se o comprimento da chave de autenticação especificada for diferente do algoritmo hash selecionado, um erro será gerado. • **MD5**: 128 bits (16 bytes) • **SHA1**: 160 bits (20 bytes) • **SHA256**: 256 bits (32 bytes) • **SHA384**: 384 bits (48 bytes) • **SHA512**: 512 bits (64 bytes) Quando especificar a chave usando código ASCII, digite os caracteres entre aspas duplas (“).
Chave de código (ESP)	Digite os valores **Entrada/Saída**. Estas configurações são necessárias quando **Personaliz.** está selecionado para **Usar modelo prefixado**, **Manual** está selecionado para **Internet Key Exchange (IKE)**e **ESP** está selecionado para **Protocolo** em **Encapsulating Security**. O número de caracteres que você pode definir varia de acordo com a configuração selecionada em **Encriptação**, na seção **Encapsulating Security**. Se o comprimento da chave de código especificada for diferente do algoritmo de criptografia selecionado, um erro será gerado. • **DES**: 64 bits (8 bytes) • **3DES**: 192 bits (24 bytes) • **AES-CBC 128**: 128 bits (16 bytes) • **AES-CBC 256**: 256 bits (32 bytes) Quando especificar a chave usando código ASCII, digite os caracteres entre aspas duplas (“).
SPI	Esses parâmetros são usados para identificar as informações de segurança. Geralmente, um host tem múltiplas SAs (Associações de

Opção	Descrição
	segurança) para diversos tipos de comunicação IPsec. Assim, é necessário identificar a SA aplicável quando um pacote IPsec é recebido. O parâmetro SPI, que identifica a SA, está incluso no cabeçalho AH (Cabeçalho de autenticação) e ESP (Encapsulating Security Payload). Estas configurações são necessárias quando **Personaliz.** está selecionado para **Usar modelo prefixado** e **Manual** está selecionado para **Internet Key Exchange (IKE)**. Digite os valores **Entrada/Saída**. (3 a 10 caracteres)
Encapsulating Security	• **Protocolo** Selecione **ESP** ou **AH**. - O ESP é um protocolo para a transmissão de comunicações criptografadas usando IPsec. O protocolo ESP criptografa os dados reais (conteúdo comunicado) e inclui informações adicionais. O pacote IP é composto pelo cabeçalho e pelos dados reais criptografados, que vêm após o cabeçalho. Além dos dados criptografados, o pacote IP também inclui informações sobre o método de criptografia, a chave de criptografia, os dados de autenticação, etc. - O AH é a parte do protocolo IPsec responsável por autenticar o remetente e por impedir a manipulação dos dados (ele garante a integralidade dos dados). No pacote IP, os dados são inseridos imediatamente após o cabeçalho. Os pacotes também contêm valores de hash, que são calculados por meio de uma equação formada pelo conteúdo comunicado, a chave secreta e outros dados para impedir a falsificação do remetente e a manipulação dos dados. Diferentemente do ESP, o conteúdo comunicado não é criptografado, e os dados são enviados e recebidos como texto simples. • **Encriptação (Não disponível para a opção AH.)** Selecione **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**. • **Hash** Selecione **Nenhum**, **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512**. **Nenhum** pode ser selecionado apenas quando **ESP** é selecionado para **Protocolo**. • **SA Lifetime (Tempo de Vida da SA)** Especifique o tempo de vida da SA do IKE. Insira o tempo (em segundos) e o número de kilobytes (KByte). • **Modo de encapsulamento** Selecione **Transporte** ou **Túnel**. • **Endereço IP do roteador remoto** Digite o endereço IP (IPv4 ou IPv6) do roteador remoto. Insira essa informação apenas quando o modo **Túnel** for selecionado.

Opção	Descrição
	A SA (Associação de Segurança) é um método de comunicação criptografada que utiliza IPsec ou IPv6 para trocar e compartilhar informações (o método de criptografia e a chave de criptografia, por exemplo) que possibilitam a criação de um canal de comunicação seguro antes da comunicação ser iniciada. SA também pode se referir a um canal virtual de comunicação criptografada que foi estabelecido. O SA usado para IPsec estabelece o método de criptografia, realiza a troca das chaves e executa a autenticação mútua de acordo com o procedimento padrão do IKE (Internet Key Exchange). O SA também é atualizado periodicamente.

Informações relacionadas

- Configurar um modelo IPsec usando o Gerenciamento via Web

Usar a autenticação IEEE 802.1x em sua rede

- O que é a autenticação IEEE 802.1x?
- Configure a autenticação IEEE 802.1x para sua rede usando o gerenciamento via Web (navegador da Web)
- Métodos de autenticação IEEE 802.1x

O que é a autenticação IEEE 802.1x?

A IEEE 802.1x é uma norma IEEE que limita o acesso de dispositivos de rede não autorizados. Seu equipamento Brother envia um pedido de autenticação para um servidor RADIUS (servidor de autenticação) através de seu ponto de acesso ou hub. Após sua solicitação ser confirmada pelo servidor RADIUS, seu equipamento pode acessar a rede.

Informações relacionadas

- Usar a autenticação IEEE 802.1x em sua rede

Configure a autenticação IEEE 802.1x para sua rede usando o gerenciamento via Web (navegador da Web)

- Se você configurar seu equipamento usando a autenticação EAP-TLS, deve instalar o certificado de cliente emitido por uma CA antes de iniciar a configuração. Entre em contato com o administrador de sua rede sobre o certificado de cliente. Se você instalou mais de um certificado, recomendamos anotar o nome do certificado que deseja usar.
- Antes de verificar o certificado do servidor, você deve importar o certificado de CA emitido pela CA que assinou o certificado do servidor. Entre em contato com o seu administrador de rede ou com o seu provedor de serviços de Internet (ISP) para confirmar se é necessário importar um certificado de CA.

Você também pode configurar a autenticação IEEE 802.1x usando o assistente de configuração sem fio no painel de controle (rede sem fio).

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.

4. Clique em **Rede** na barra de navegação à esquerda.

Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ☰.

5. Siga uma destas opções:
   - Para redes cabeadas

     Clique em **Com fio** > **Autenticação 802.1x com fio**.
   - Para redes sem fio

     Clique em **Sem fio** > **Sem fio (Empresarial)**.
6. Configure as configurações da autenticação IEEE 802.1x.

- Para habilitar a autenticação IEEE 802.1x para redes cabeadas, selecione **Ativado** para **Estado 802.1x com fio** na página **Autenticação 802.1x com fio**.
- Se estiver usando a autenticação **EAP-TLS**, selecione o certificado de cliente instalado (exibido com o nome do certificado) que será verificado na lista suspensa **Certificado do cliente**.
- Se você selecionar a autenticação **EAP-FAST**, **PEAP**, **EAP-TTLS** ou **EAP-TLS**, selecione o método de verificação na lista suspensa **Verificação do certificado do servidor**. Verifique o certificado do servidor usando o certificado de CA, previamente importado no equipamento, emitido pela CA que assinou o certificado do servidor.

Selecione um dos seguintes métodos de verificação na lista suspensa **Verificação do certificado do servidor**:

Opção	Descrição
S/ verificação	O certificado do servidor é sempre confiável. A verificação não é realizada.
Certif. de CA	Método de verificação para confirmar a credibilidade da CA emissora do certificado do servidor, usando o certificado de CA emitido pela CA que assinou o certificado do servidor.
Certif. de CA + IDServidor	Método de verificação para confirmar o valor do nome comum [1] do certificado do servidor e também a credibilidade da CA emissora do certificado do servidor.

7. Ao concluir a configuração, clique em **Enviar**.

   Para redes cabeadas: ao concluir a configuração, conecte o equipamento à rede IEEE 802.1x suportada. Aguarde alguns minutos e imprima o Relatório de configurações de rede para verificar o <**Wired IEEE 802.1x**> status.

Opção	Descrição
Success	A função rede cabeada IEEE 802.1x está habilitada e a autenticação foi realizada com sucesso.
Failed	A função rede cabeada IEEE 802.1x está habilitada, mas houve falha na autenticação.
Desl.	A função rede cabeada IEEE 802.1x não está disponível.

Informações relacionadas

- Usar a autenticação IEEE 802.1x em sua rede

Tópicos relacionados:

- Visão geral dos recursos do certificado de segurança
- Configurar certificados para a segurança do dispositivo

1 A verificação do nome comum compara o nome comum do certificado do servidor com a sequência de caracteres configurada para o **ID do serv.**. Antes de usar este método, entre em contato com seu administrador do sistema para saber o nome comum do certificado do servidor e, em seguida, configure o valor **ID do serv.**.

Métodos de autenticação IEEE 802.1x

EAP-FAST

O EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling) é um método desenvolvido pela Cisco Systems, Inc., que usa um ID de usuário e uma senha para autenticação e algoritmos de chave simétrica para conseguir um processo de autenticação encapsulado.

Seu equipamento Brother é compatível com os seguintes métodos de autenticação interna:

- EAP-FAST/NENHUM
- EAP-FAST/MS-CHAPv2
- EAP-FAST/GTC

EAP-MD5 (rede cabeada)

O EAP-MD5 (Extensible Authentication Protocol-Message Digest Algorithm 5) usa um ID de usuário e uma senha para autenticação de desafio/resposta.

PEAP

O PEAP (Protected Extensible Authentication Protocol) é uma versão do método EAP desenvolvido pela Cisco Systems, Inc., Microsoft Corporation e RSA Security. O PEAP cria um túnel SSL (Secure Sockets Layer)/TLS (Transport Layer Security) criptografado entre um cliente e um servidor de autenticação para o envio de uma ID de usuário e uma senha. O PEAP oferece autenticação mútua entre o servidor e o cliente.

Seu equipamento Brother é compatível com os seguintes métodos de autenticação interna:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

O EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security) foi desenvolvido pela Funk Software e a Certicom. O EAP-TTLS cria um túnel SSL criptografado semelhante ao do PEAP entre um cliente e um servidor de autenticação para o envio de uma ID de usuário e uma senha. O EAP-TTLS oferece autenticação mútua entre o servidor e o cliente.

Seu equipamento Brother é compatível com os seguintes métodos de autenticação interna:

- EAP-TTLS/CHAP
- EAP-TTLS/MS-CHAP
- EAP-TTLS/MS-CHAPv2
- EAP-TTLS/PAP

EAP-TLS

O EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) requer autenticação por certificado digital tanto no cliente quanto no servidor de autenticação.

Informações relacionadas

- Usar a autenticação IEEE 802.1x em sua rede

Autenticação do Usuário

- Usar Autenticação Active Directory
- Usar a Autenticação LDAP
- Usar o Secure Function Lock 3.0 (Bloqueio Seguro de Função 3.0)

Usar Autenticação Active Directory

- Introdução à Autenticação Active Directory
- Configurar a Autenticação Active Directory usando o Gerenciamento via Web
- Fazer login para alterar as configurações do equipamento usando o painel de controle (Autenticação Active Directory)

Introdução à Autenticação Active Directory

A autenticação Active Directory limita o uso do seu equipamento. Se a Autenticação Active Directory estiver habilitada, o painel de controle do equipamento ficará bloqueado. Você só conseguirá alterar as configurações do equipamento após inserir uma ID de usuário e uma senha.

A Autenticação Active Directory oferece os seguintes recursos:

Os recursos, opções e configurações compatíveis podem ser diferentes dependendo do modelo.

- Armazena dados de impressão recebidos
- Armazena dados de fax recebidos
- Obtém o endereço de e-mail no servidor Active Directory a partir da sua ID de usuário, quando dados digitalizados são enviados a um servidor de e-mail.

  Para usar este recurso, selecione a opção **Ativado** para a configuração de **Obter end. de e-mail** e **LDAP + kerberos** ou o método de autenticação **LDAP + NTLMv2**. Seu endereço de e-mail será definido como o remetente quando o equipamento enviar dados digitalizados a um servidor de e-mail, ou será definido como o destinatário se você quiser enviar os dados digitalizados ao seu endereço de e-mail.

Quando a Autenticação Active Directory é habilitada, o equipamento armazena todos os dados de faxes recebidos. Após fazer login, o equipamento imprime os dados de fax armazenados.

Você pode alterar as configurações da autenticação Active Directory usando o Gerenciamento via Web.

Informações relacionadas

- Usar Autenticação Active Directory

Configurar a Autenticação Active Directory usando o Gerenciamento via Web

A autenticação Active Directory suporta autenticação Kerberos e NTLMv2. Você precisa configurar o protocolo SNTP (servidor de horário da rede) e o servidor DNS para autenticação.

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.

4. Na barra de navegação esquerda, clique em **Administrador** > **Função de restrição de usuário** ou **Gerenciamento de restrição**.

Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ≡.

5. Selecione **Autenticação do Active Directory**.
6. Clique em **Enviar**.
7. Clique em **Autenticação do Active Directory**.
8. Defina as seguintes configurações:

Os recursos, opções e configurações compatíveis podem ser diferentes dependendo do modelo.

Opção	Descrição
Armaz. de dados de RX de fax	Selecione esta opção para armazenar dados de fax recebidos. Você pode imprimir todos os dados de fax recebidos após fazer login no equipamento.
Lembrar ID de usuário	Selecione esta opção para salvar sua ID de usuário.
Endereço do servidor Active Directory	Digite o endereço IP ou o nome do servidor (por exemplo, ad.exemplo.com) do Active Directory.
Nome de domínio do Active Directory	Insira o nome do domínio do Diretório Ativo.
Protocolo e método de autenticação	Selecione o protocolo e o método de autenticação.
SSL/TLS	Selecione a opção **SSL/TLS**.
Porta do servidor LDAP	Digite o número da porta para conectar o servidor do Active Directory via LDAP (disponível somente para o método de autenticação **LDAP + kerberos** ou **LDAP + NTLMv2**).
Pesquisar raiz LDAP	Digite a raiz de pesquisa do LDAP (disponível apenas para o método de autenticação **LDAP + kerberos** ou **LDAP + NTLMv2**).

Opção	Descrição
Obter end. de e-mail	Selecione esta opção para obter o endereço de e-mail do usuário conectado a partir do servidor Active Directory. (disponível apenas para **LDAP + kerberos** ou o método de autenticação **LDAP + NTLMv2**)
Obter diretório inicial do usuário	Selecione esta opção para definir seu diretório base como o destino da função Digitalizar para Rede. (disponível apenas para **LDAP + kerberos** ou o método de autenticação **LDAP + NTLMv2**)

9. Clique em **Enviar**.

Informações relacionadas

- Usar Autenticação Active Directory

Fazer login para alterar as configurações do equipamento usando o painel de controle (Autenticação Active Directory)

Quando a Autenticação Active Directory estiver habilitada, o painel de controle do equipamento ficará bloqueado até você inserir sua ID de usuário e senha no painel de controle do equipamento.

1. No painel de controle do equipamento, insira a ID de usuário e a senha para fazer login.
2. Quando a autenticação for concluída corretamente, o painel de controle do equipamento é desbloqueado.

Informações relacionadas

- Usar Autenticação Active Directory

Usar a Autenticação LDAP

- Introdução à Autenticação LDAP
- Configurar a Autenticação LDAP usando o Gerenciamento via Web
- Fazer login para alterar as configurações do equipamento usando o painel de controle (Autenticação LDAP)

Introdução à Autenticação LDAP

A Autenticação LDAP restringe o uso de seu equipamento. Se a autenticação LDAP estiver habilitada, o painel de controle do equipamento ficará bloqueado. Você só conseguirá alterar as configurações do equipamento após inserir uma ID de usuário e uma senha.

A autenticação LDAP oferece os seguintes recursos:

Os recursos, opções e configurações compatíveis podem ser diferentes dependendo do modelo.

- Armazena dados de impressão recebidos
- Armazena dados de fax recebidos
- Obtém o endereço de e-mail no servidor LDAP a partir da sua ID de usuário, quando dados digitalizados são enviados a um servidor de e-mail.

  Para usar este recurso, selecione a opção **Ativado** para a configuração **Obter end. de e-mail**. Seu endereço de e-mail será definido como o remetente quando o equipamento enviar dados digitalizados a um servidor de e-mail, ou será definido como o destinatário se você quiser enviar os dados digitalizados ao seu endereço de e-mail.

Quando a Autenticação LDAP é habilitada, o equipamento armazena todos os dados de faxes recebidos. Após fazer login, o equipamento imprime os dados de fax armazenados.

Você pode alterar as configurações de autenticação LDAP usando o Gerenciamento via Web.

Informações relacionadas

- Usar a Autenticação LDAP

Configurar a Autenticação LDAP usando o Gerenciamento via Web

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.

4. Na barra de navegação esquerda, clique em **Administrador** > **Função de restrição de usuário** ou **Gerenciamento de restrição**.

Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ≡.

5. Selecione **Autenticação LDAP**.
6. Clique em **Enviar**.
7. Clique no menu **Autenticação LDAP**.
8. Defina as seguintes configurações:

Os recursos, opções e configurações compatíveis podem ser diferentes dependendo do modelo.

Opção	Descrição
Armaz. de dados de RX de fax	Selecione esta opção para armazenar dados de fax recebidos. Você pode imprimir todos os dados de fax recebidos após fazer login no equipamento.
Lembrar ID de usuário	Selecione esta opção para salvar sua ID de usuário.
Endereço do servidor LDAP	Digite o endereço IP ou o nome do servidor (por exemplo: ldap.exemplo.com) LDAP.
SSL/TLS	Selecione a opção **SSL/TLS** para usar LDAP sobre SSL/TLS.
Porta do servidor LDAP	Digite o número da porta do Servidor LDAP.
Pesquisar raiz LDAP	Digite o diretório raiz da pesquisa LDAP.
Atributo do nome (Chave de pesquisa)	Digite o atributo que deseja usar como chave de busca.
Obter end. de e-mail	Selecione essa opção para obter o endereço de e-mail dos usuários registrados a partir do servidor LDAP.
Obter diretório inicial do usuário	Selecione esta opção para definir seu diretório base como o destino da função Digitalizar para Rede.

9. Clique em **Enviar**.

Informações relacionadas

- Usar a Autenticação LDAP

Fazer login para alterar as configurações do equipamento usando o painel de controle (Autenticação LDAP)

Quando a Atenticação LDAP estiver habilitada, o painel de controle do equipamento ficará bloqueado até você inserir sua ID de usuário e senha no painel de controle do equipamento.

1. No painel de controle do equipamento, insira a ID de usuário e a senha para fazer login.
2. Quando a autenticação for concluída corretamente, o painel de controle do equipamento é desbloqueado.

Informações relacionadas

- Usar a Autenticação LDAP

Usar o Secure Function Lock 3.0 (Bloqueio Seguro de Função 3.0)

O Secure Function Lock 3.0 (Bloqueio Seguro de Função 3.0) aumenta a segurança restringindo as funções disponíveis no equipamento.

Antes de usar o Secure Function Lock 3.0

Use o Secure Function Lock (Bloqueio Seguro de Função) para configurar senhas, definir limites de páginas para usuários específicos e conceder acesso a algumas ou todas as funções listadas aqui.

Você pode definir e alterar as seguintes configurações do Secure Function Lock 3.0 (Bloqueio Seguro de Função 3.0) usando o Gerenciamento via Web:

Os recursos, opções e configurações compatíveis podem ser diferentes dependendo do modelo.

- **Imprimir**
- **Copiar**
- **Digit.**
- **Fax**
- **Media (Mídia)**
- **Conexão Web**
- **Aplics.**
- **Limites de página**
- **Contadores pág.**
- **ID do cartão (ID do NFC)**

Modelos de LCD com tela de toque:

Quando o bloqueio de funções seguras é ativado, o equipamento entra automaticamente no modo público e algumas das funções do equipamento ficam restritas a apenas usuários autorizados. Para acessar as funções restritas do equipamento, pressione , selecione seu nome de usuário e digite sua senha.

Informações relacionadas

- Usar o Secure Function Lock 3.0 (Bloqueio Seguro de Função 3.0)

Configurar o Secure Function Lock 3.0 usando o Gerenciamento via Web

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.

4. Na barra de navegação esquerda, clique em **Administrador** > **Função de restrição de usuário** ou **Gerenciamento de restrição**.

Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ≡.

5. Selecione **Bloqueio seguro de funções**.
6. Clique em **Enviar**.
7. Clique no menu **Funções restritas**.
8. Defina as configurações para gerenciar restrições por usuário ou por grupo.
9. Clique em **Enviar**.
10. Clique no menu **Lista de usuários**.
11. Configure a lista de usuários.
12. Clique em **Enviar**.

Você também pode alterar as configurações de bloqueio da lista de usuários no menu **Bloqueio seguro de funções**.

Informações relacionadas

- Usar o Secure Function Lock 3.0 (Bloqueio Seguro de Função 3.0)

Digitalizar usando o Secure Function Lock 3.0

Os recursos, opções e configurações compatíveis podem ser diferentes dependendo do modelo.

Configuração das restrições de digitalização (para administradores)

O Secure Function Lock 3.0 (Bloqueio Seguro de Função 3.0) permite que um administrador restrinja quais usuários terão permissão para digitalizar. Quando o recurso de escaneamento é desativado para a configuração de usuários públicos, apenas os usuários que foram marcados na caixa de seleção **Digit.** poderão digitalizar.

Utilização do recurso de digitalização (para usuários restritos)

- Para digitalizar utilizando o painel de controle do equipamento:

  Os usuários restritos precisam digitar suas senhas no painel de controle do equipamento para acessarem o modo de digitalização.
- Para digitalizar utilizando um computador:

  Os usuários restritos precisam digitar suas senhas no painel de controle do equipamento antes de escanearem em seus computadores. Se a senha não for digitada no painel de controle do equipamento, será exibida uma mensagem de erro no computador do usuário.

Se o equipamento for compatível com autenticação por cartão de proximidade, usuários com restrições também podem acessar o modo de digitalização tocando o logotipo NFC no painel de controle do equipamento com seus cartões de proximidade registrados.

Informações relacionadas

- Usar o Secure Function Lock 3.0 (Bloqueio Seguro de Função 3.0)

Configurar Modo Público para o Secure Function Lock 3.0

Use a tela do Secure Function Lock para configurar o modo Público, que limita as funções disponíveis aos usuários públicos. Os usuários públicos não precisam digitar uma senha para acessar os recursos disponibilizados pelas configurações do modo Público.

O modo público inclui trabalhos de impressão enviados por meio do Brother iPrint&Scan e do Brother Mobile Connect.

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.

4. Na barra de navegação esquerda, clique em **Administrador** > **Função de restrição de usuário** ou **Gerenciamento de restrição**.

Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ≡.

5. Selecione **Bloqueio seguro de funções**.
6. Clique em **Enviar**.
7. Clique no menu **Funções restritas**.
8. Na linha **Modo público**, marque uma caixa de seleção para permitir a função listada ou desmarque uma caixa de seleção para restringir a função listada.
9. Clique em **Enviar**.

Informações relacionadas

- Usar o Secure Function Lock 3.0 (Bloqueio Seguro de Função 3.0)

Definir as configurações da tela de início pessoal usando o Gerenciamento via Web

Como Administrador, você pode especificar as guias que os usuários podem visualizar em suas telas de início. Essas guias oferecem acesso rápido aos atalhos favoritos do usuário, que podem ser atribuídos às guias de suas telas de início por meio do painel de controle do equipamento.

Os recursos, opções e configurações compatíveis podem ser diferentes dependendo do modelo.

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.

4. Na barra de navegação esquerda, clique em **Administrador** > **Função de restrição de usuário** ou **Gerenciamento de restrição**.

Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ≡.

5. Selecione **Bloqueio seguro de funções**.
6. No campo **Config. da aba**, selecione **Pessoal** para os nomes de guias que deseja usar como sua tela de início pessoal.
7. Clique em **Enviar**.
8. Clique no menu **Funções restritas**.
9. Defina as configurações para gerenciar as restrições por usuário ou grupo.
10. Clique em **Enviar**.
11. Clique no menu **Lista de usuários**.
12. Configure a lista de usuários.
13. Na lista suspensa, selecione **Lista de usuários/funções restritas** para cada usuário.
14. Na lista suspensa **Tela inicial** de cada usuário, selecione o nome da guia.
15. Clique em **Enviar**.

Informações relacionadas

- Usar o Secure Function Lock 3.0 (Bloqueio Seguro de Função 3.0)

Recursos adicionais do Secure Function Lock 3.0

Configure os seguintes recursos na tela do Secure Function Lock:

Os recursos, opções e configurações compatíveis podem ser diferentes dependendo do modelo.

Restaurar todos os contadores

Clique em **Restaurar todos os contadores**, na coluna **Contadores pág.**, para restaurar o contador de páginas.

Exportar para arquivo CSV

Clique em **Exportar para arquivo CSV**, para exportar o contador de páginas atual e o último, incluindo informações de **Lista de usuários/funções restritas**, como um arquivo CSV.

ID do cartão (ID do NFC)

Clique no menu **Lista de usuários** e digite o ID do cartão de um usuário no campo **ID do cartão (ID do NFC)**. Você pode usar seu cartão de proximidade para autenticação.

Saída

Se a unidade de Caixa de Correio estiver instalada no equipamento, use a lista suspensa para selecionar uma bandeja de saída para cada usuário.

Último registro do contador

Clique em **Último registro do contador**, se quiser que o equipamento mantenha a contagem de páginas após o contador ser restaurado.

Restaurar contador autom.

Clique em **Restaurar contador autom.** para configurar o intervalo de tempo desejado entre a restauração do contador de páginas. Escolha um intervalo diário, semanal ou mensal.

Informações relacionadas

- Usar o Secure Function Lock 3.0 (Bloqueio Seguro de Função 3.0)

Registrar um novo cartão de proximidade usando o painel de controle do equipamento

Você pode registrar cartões de circuito integrado (cartões de CI) em seu equipamento.

Os recursos, opções e configurações compatíveis podem ser diferentes dependendo do modelo.

1. Encoste um cartão de proximidade (cartão IC) registrado no símbolo de Near-Field Communication (NFC) localizado no painel de controle do equipamento.
2. Pressione seu ID de usuário no LCD.
3. Pressione o botão Register Card (Registrar cartão).
4. Encoste um novo cartão de proximidade no símbolo de NFC.

   O número do novo cartão de proximidade é então registrado no equipamento.
5. Pressione o botão OK.

Informações relacionadas

- Usar o Secure Function Lock 3.0 (Bloqueio Seguro de Função 3.0)

Registrar um leitor externo de cartão com chip

Quando você conectar um leitor externo de cartão de proximidade (cartão IC), use o Gerenciamento via Web para registrar o leitor de cartão. Seu equipamento suporta leitores externos de cartão com chip compatíveis com driver classe HID.

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

   A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.
4. Clique em **Administrador** > **Leitor de cartão externo** na barra de navegação à esquerda.

   Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ☰.
5. Digite as informações necessárias e clique em **Enviar**.
6. Reinicie o equipamento Brother para ativar a configuração.
7. Conecte o leitor de cartão ao seu equipamento.
8. Toque o cartão no leitor de cartões ao usar a autenticação do cartão.

Informações relacionadas

- Usar o Secure Function Lock 3.0 (Bloqueio Seguro de Função 3.0)

Envie ou receba e-mails com segurança

- Configure o envio e recebimento de e-mails utilizando o Gerenciamento via Web
- Enviar um e-mail com autenticação de usuário
- Enviar ou receber um e-mail com segurança usando SSL/TLS

Configure o envio e recebimento de e-mails utilizando o Gerenciamento via Web

- O recebimento de e-mails está disponível apenas em determinados modelos.
- Recomendamos a utilização do Gerenciamento via Web para configurar o envio seguro de e-mails com a autenticação do usuário ou o envio e recebimento de e-mails utilizando SSL/TLS (somente nos modelos compatíveis).

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.

4. Clique em **Rede** > **Rede** > **Protocolo** na barra de navegação à esquerda.

Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ≡.

5. No campo **Cliente POP3/IMAP4/SMTP**, clique em **Config. avançadas** e certifique-se de que o status de **Cliente POP3/IMAP4/SMTP** esteja **Ativado**.

- Os protocolos disponíveis podem variar, dependendo do equipamento.
- Se a tela de seleção **Método de autenticação** for exibida, selecione o método de autenticação e siga as instruções na tela.

6. Defina as configurações de **Cliente POP3/IMAP4/SMTP**.
   - Para confirmar se as opções de e-mail estão corretas após a configuração, envie um e-mail de teste.
   - Se você não sabe as configurações de servidor POP3/IMAP4/SMTP, entre em contato com o seu administrador da rede ou com o provedor de serviços de Internet (ISP).
7. Ao concluir, clique em **Enviar**.

   A caixa de diálogo **Configuração de envio/receb. de e-mail de teste** é exibida.
8. Siga as instruções da caixa de diálogo para testar as configurações atuais.

Informações relacionadas

- Envie ou receba e-mails com segurança

Tópicos relacionados:

- Enviar ou receber um e-mail com segurança usando SSL/TLS

Enviar um e-mail com autenticação de usuário

O equipamento envia e-mails por meio de um servidor de e-mail que requer autenticação de usuário. Esse método impede que usuários não autorizados acessem o servidor de e-mail.

Você pode enviar notificações por e-mail, relatórios por e-mail e I-Fax (disponível apenas em determinados modelos) usando a autenticação do usuário.

- Os protocolos disponíveis podem variar, dependendo do equipamento.
- Recomendamos a utilização do Gerenciamento via Web para configurar a autenticação de SMTP.

Configurações do servidor de e-mail

Você deve configurar o método de autenticação SMTP do equipamento para que ele corresponda ao método usado por seu servidor de e-mail. Para obter detalhes sobre suas configurações do servidor de e-mail, entre em contato com seu administrador de rede ou com o provedor de serviços de Internet (ISP).

Para habilitar a autenticação do servidor SMTP usando o Gerenciamento via Web, selecione seu método de autenticação em **Método de autenticação do servidor** na tela **Cliente POP3/IMAP4/SMTP**.

Informações relacionadas

- Envie ou receba e-mails com segurança

Enviar ou receber um e-mail com segurança usando SSL/TLS

Seu equipamento suporta métodos de comunicação SSL/TLS. Para usar um servidor de e-mail que utilize a comunicação SSL/TLS, você deve definir as configurações a seguir.

- O recebimento de e-mails está disponível apenas em determinados modelos.
- Recomendamos a utilização do Gerenciamento via Web para configurar o SSL/TLS.

Verificar certificado do servidor

Em **SSL/TLS**, se você escolher **SSL** ou **TLS**, a caixa de seleção **Verificar certif. do servidor** será marcada automaticamente.

- Antes de verificar o certificado do servidor, você deve importar o certificado de CA emitido pela CA que assinou o certificado do servidor. Entre em contato com o seu administrador de rede ou com o seu provedor de serviços de Internet (ISP) para confirmar se é necessário importar um certificado de CA.
- Se não for necessário verificar o certificado do servidor, desmarque a caixa de seleção **Verificar certif. do servidor**.

Número da porta

Se você selecionar **SSL** ou **TLS**, o valor de **Porta** será alterado para coincidir com o protocolo. Para alterar o número da porta manualmente, digite o número da porta depois de selecionar as configurações de **SSL/TLS**.

Você deve configurar o método de comunicação do seu equipamento para coincidir com o método usado pelo servidor de e-mail. Para obter detalhes sobre as configurações do seu servidor de e-mail, entre em contato com o administrador de rede ou com o ISP.

Na maior parte dos casos, os serviços de webmail seguro requerem as seguintes configurações:

Os recursos, opções e configurações compatíveis podem ser diferentes dependendo do modelo.

SMTP	**Porta**	587
	Método de autenticação do servidor	**SMTP-AUTH**
	SSL/TLS	**TLS**
POP3	**Porta**	995
	SSL/TLS	**SSL**
IMAP4	**Porta**	993
	SSL/TLS	**SSL**

Informações relacionadas

- Envie ou receba e-mails com segurança

Tópicos relacionados:

- Configure o envio e recebimento de e-mails utilizando o Gerenciamento via Web
- Configurar certificados para a segurança do dispositivo

Armazenamento do registro de impressão na rede

- Visão geral do armazenamento do registro de impressão na rede
- Configurar as opções do armazenamento do registro de impressão na rede usando o Gerenciamento via Web
- Usar a Configuração de detecção de erro do armazenamento do registro de impressão na rede
- Usar o armazenamento do registro de impressão na rede com o Secure Function Lock 3.0

Visão geral do armazenamento do registro de impressão na rede

O recurso de armazenamento do registro de impressão na rede permite que você salve o arquivo do registro de impressão de seu equipamento em um servidor em rede usando o protocolo CIFS (Common Internet File System). Você pode gravar a ID, o tipo de trabalho de impressão, o nome do trabalho, o nome de usuário, a data, a hora e o número de páginas impressas para cada trabalho de impressão. O CIFS é um protocolo executado por TCP/IP, possibilitando que computadores em uma rede compartilhem arquivos em uma intranet ou Internet.

As funções de impressão a seguir são gravadas no registro de impressão:

Os recursos, opções e configurações compatíveis podem ser diferentes dependendo do modelo.

- Trabalhos de impressão de seu computador
- Impressão USB direta
- Cópia
- Fax recebido
- Impressão Web Connect

- O recurso de armazenamento do registro de impressão na rede é compatível com autenticação Kerberos e NTLMv2. Você precisa configurar o protocolo SNTP (servidor de horário da rede) ou configurar a data, a hora e o fuso horário corretamente no painel de controle para a autenticação.
- Você pode definir o tipo de arquivo como TXT ou CSV ao armazenar um arquivo no servidor.

Informações relacionadas

- Armazenamento do registro de impressão na rede

Configurar as opções do armazenamento do registro de impressão na rede usando o Gerenciamento via Web

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.

4. Clique em **Administrador** > **Armazenar log de impr. na rede** na barra de navegação à esquerda.

Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ☰.

5. No campo **Log de impressão**, clique em **Ativado**.
6. Defina as seguintes configurações:

Os recursos, opções e configurações compatíveis podem ser diferentes dependendo do modelo.

Opção	Descrição
Caminho da pasta da rede	Digite a pasta de destino na qual seu registro de impressão será armazenado no servidor CIFS (por exemplo: \\NomeDoComputador\PastaCompartilhada).
Nome arq.	Digite o nome de arquivo que você deseja usar para o registro de impressão (no máximo 32 caracteres).
Tipo arq.	Selecione a opção **TXT** ou **CSV** para o tipo de arquivo do registro de impressão.
Fonte de tempo para log	Selecione a fonte de hora para o registro de impressão.
Método de autentic.	Selecione o método de autenticação necessário para acessar o servidor CIFS: **Auto**, **Kerberos**, ou **NTLMv2**. O Kerberos é um protocolo de autenticação que permite que dispositivos ou indivíduos provem sua identidade aos servidores de rede de forma segura e usando o recurso de login único. O NTLMv2 é o método de autenticação usado pelo Windows para se conectar aos servidores. • **Auto**: se você selecionar **Auto**, NTLMv2 será usado como o método de autenticação. • **Kerberos**: selecione a opção **Kerberos** para usar apenas a autenticação Kerberos. • **NTLMv2**: selecione a opção **NTLMv2** para usar apenas a autenticação NTLMv2. • Para a autenticação **Kerberos** e **NTLMv2**, você também precisa definir as configurações de **Data e hora** ou configurar o protocolo SNTP (servidor de horário da rede) e o servidor DNS. • Você pode também definir as configurações de data e hora no painel de controle do equipamento.

Opção	Descrição
Nome usuário	Digite o nome de usuário para a autenticação (no máximo 96 caracteres). Se o nome de usuário for parte de um domínio, informe-o com o formato usuário@domínio ou domínio\usuário.
Senha	Digite a senha para a autenticação (no máximo 32 caracteres).
Endereço do servidor Kerberos (se necessário)	Digite o endereço do host (por exemplo: kerberos.exemplo.com; com no máximo 64 caracteres) ou o endereço IP (por exemplo: 192.168.56.189) do centro de distribuição de chaves (KDC).
Config. de detecção de erro	Escolha qual medida deverá ser tomada quando o registro de impressão não puder ser armazenado no servidor devido a um erro de rede.

7. No campo **Status da conexão**, confirme o status do último registro.

Você também pode confirmar o status do erro no LCD do equipamento.

8. Clique em **Enviar** para exibir a página **Log de impressão de teste para rede**.

   Para testar suas configurações, clique em **Sim** e vá para a próxima etapa.

   Para ignorar o teste, clique em **Não**. Suas configurações serão enviadas automaticamente.
9. O equipamento testará suas configurações.
10. Se suas configurações forem aceitas, a mensagem **Teste OK** será exibida na tela.

    Se a mensagem **Erro no teste** for exibida, selecione todas as configurações e clique em **Enviar** para exibir novamente a página de teste.

Informações relacionadas

- Armazenamento do registro de impressão na rede

Usar a Configuração de detecção de erro do armazenamento do registro de impressão na rede

Use as Configurações de detecção de erro para determinar a ação a ser tomada quando o registro de impressão não pode ser armazenado no servidor devido a um erro de rede.

1. Inicie o navegador da Web.
2. Digite “https://machine's IP address” na barra de endereços do seu navegador (onde “endereço IP do equipamento” é o endereço IP de seu equipamento).

   Por exemplo:

   https://192.168.1.2

   O endereço IP do seu equipamento pode ser encontrado no Relatório de Configurações de Rede.
3. Se necessário, digite a senha no campo **Login** e clique em **Login**.

A senha padrão para gerenciamento das configurações deste equipamento está localizada na parte traseira ou base do equipamento, identificada como “**Pwd**”. Altere a senha padrão seguindo as instruções na tela quando fizer o primeiro login.

4. Clique em **Administrador** > **Armazenar log de impr. na rede** na barra de navegação à esquerda.

Se a barra de navegação à esquerda não estiver visível, inicie a navegação a partir de ☰.

5. Na seção **Config. de detecção de erro**, selecione a opção **Cancelar impr.** ou **Ignorar log e imprimir**.

Os recursos, opções e configurações compatíveis podem ser diferentes dependendo do modelo.

Opção	Descrição
Cancelar impr.	Se você selecionar a opção **Cancelar impr.**, os trabalhos de impressão serão cancelados quando o registro de impressão não puder ser armazenado no servidor. Mesmo se você selecionar a opção **Cancelar impr.**, seu equipamento imprimirá um fax recebido.

Ignorar log e imprimir	Se você selecionar a opção **Ignorar log e imprimir**, o equipamento imprimirá a documentação mesmo se o registro de impressão não puder ser armazenado no servidor.
	
	Quando a função de armazenamento do registro de impressão for restabelecido, o registro de impressão será gravado da seguinte forma:
	
	`Id, Type, Job Name, User Name, Date, Time, Print Pages`
	`1, Print(xxxxxxx), “Document01.doc”, “user01”, 03/03/20xx, 14:01:32, 52`
	`2, Print(xxxxxxx), “Document02.doc”, “user01”, 03/03/20xx, 14:45:30, ?` (a)
	`3, <Error>, ?, ?, ?, ?, ?` (b)
	`4, Print(xxxxxxx), “Report01.xls”, “user02”, 03/03/20xx, 19:30:40, 4`
	
	a. Se o registro de impressão não puder ser armazenado ao final da impressão, o número de páginas impressas não será gravado.
	b. Se o registro de impressão não puder ser armazenado no início e ao final da impressão, o registro de impressão do trabalho não será gravado. Quando a função for recuperada, o erro será refletido no registro.

6. Clique em **Enviar** para exibir a página **Log de impressão de teste para rede**.

   Para testar suas configurações, clique em **Sim** e vá para a próxima etapa.

Para ignorar o teste, clique em **Não**. Suas configurações serão enviadas automaticamente.

7. O equipamento testará suas configurações.
8. Se suas configurações forem aceitas, a mensagem **Teste OK** será exibida na tela.

   Se a mensagem **Erro no teste** for exibida, selecione todas as configurações e clique em **Enviar** para exibir novamente a página de teste.

Informações relacionadas

- Armazenamento do registro de impressão na rede

Usar o armazenamento do registro de impressão na rede com o Secure Function Lock 3.0

Quando o Secure Function Lock 3.0 (Bloqueio Seguro de Função 3.0) está ativo, os nomes dos usuários registrados para cópia, recepção de fax, impressão Web Connect e impressão USB direta são gravados no relatório de armazenamento do registro de impressão na rede. Quando a autenticação Active Directory estiver habilitada, o nome do usuário será gravado no relatório de armazenamento do registro de impressão na rede:

Os recursos, opções e configurações compatíveis podem ser diferentes dependendo do modelo.

```
Id, Type, Job Name, User Name, Date, Time, Print Pages
1, Copy, -, -, 04/04/20xx, 09:05:12, 3
2, Fax, -, -, 04/04/20xx, 09:45:30, 5
3, Copy, -, "Bob", 04/04/20xx, 10:20:30, 4
4, Fax, -, "Bob", 04/04/20xx, 10:35:12, 3
5, USB Direct, -, "John", 04/04/20xx, 11:15:43, 6
```

Informações relacionadas

- Armazenamento do registro de impressão na rede

www.brotherearth.com

BRA
Versão 0