Guia de Recursos de Segurança

Informações Importantes de Segurança

- A senha padrão para gerenciar as configurações desta máquina está localizada na parte inferior da máquina e marcada como **"Pwd:"**. Recomendamos alterar imediatamente a senha padrão para proteger sua máquina contra acesso não autorizado.
- Ao conectar sua máquina a uma rede externa como a Internet, certifique-se de que seu ambiente de rede esteja protegido por um firewall separado ou por outros meios, para evitar vazamento de informações devido a configurações inadequadas ou acesso não autorizado por terceiros mal intencionados.
- Se houver um sinal nas proximidades, a LAN sem fio permite que você faça uma conexão LAN livremente. No entanto, se as configurações de segurança não estiverem configuradas corretamente, o sinal poderá ser interceptado por terceiros mal intencionados, podendo resultar em:
  - Roubo de informações pessoais ou confidenciais
  - Transmissão indevida de informações para pessoas que se passam por usuários autorizados
  - Vazamento de conteúdos de comunicação transcritos que foram interceptados

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** 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 e, em seguida, configure as definições.
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 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.
Off	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