# Guia de recursos de segurança

© 2025 Brother Industries, Ltd. Todos os direitos reservados.

# Informações importantes para segurança

- A palavra-passe predefinida para gerir as definições deste equipamento encontra-se na parte inferior do equipamento com a indicação “**Pwd**”. Recomendamos que altere imediatamente a palavra-passe predefinida para proteger o equipamento de acessos não autorizados.
- Quando ligar o equipamento a uma rede externa, como a Internet, certifique-se de que o seu ambiente de rede está protegido por uma firewall separada ou outro meio para evitar fugas de informações devido a definições inadequadas ou a acesso não autorizado por terceiros mal-intencionados.
- Se existir um sinal nas proximidades, a rede sem fios permite-lhe efetuar livremente uma ligação LAN. No entanto, se as definições de segurança não estiverem configuradas corretamente, o sinal pode ser intercetado por terceiros mal-intencionados, o que pode resultar em:
  - Furto de informações pessoais ou confidenciais
  - Transmissão inadequada de informações a terceiros que se façam passar por indivíduos específicos
  - Difusão de conteúdos de comunicação transcritos que foram intercetados

## Informações relacionadas

- Rede

# Configurar certificados para segurança do equipamento

É necessário configurar um certificado para gerir o seu equipamento de rede em segurança utilizando SSL/TLS. Tem de utilizar a gestão baseada na Web para configurar um certificado.

# Descrição geral das funções de certificados de segurança

O equipamento suporta a utilização de vários certificados de segurança, o que permite uma autenticação e comunicação seguras com o equipamento. É possível utilizar com o equipamento as seguintes funções de certificados de segurança:

As funções, opções e definições suportadas podem diferir em função do modelo.

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

O seu equipamento suporta o seguinte:

- Certificado pré-instalado

  O equipamento tem um certificado autoassinado pré-instalado. Este certificado permite-lhe utilizar a comunicação SSL/TLS sem criar ou instalar um certificado diferente.

O certificado autoassinado pré-instalado protege a comunicação até um certo nível. Recomendamos que utilize um certificado que seja emitido por uma organização de confiança para obter mais segurança.

- Certificado auto-assinado

  Este servidor de impressão emite o seu próprio certificado. Se utilizar este certificado, pode utilizar facilmente a comunicação SSL/TLS sem criar ou instalar um certificado diferente de uma AC.

- Certificado de uma autoridade de certificação (AC)

  Existem dois métodos de instalação de um certificado de uma AC. Se já tem um certificado de uma AC ou se pretender utilizar um certificado de uma AC externa de confiança:

  - Quando utilizar uma CSR (solicitação de assinatura de certificado) a partir deste servidor de impressão.
  - Quando importar um certificado e uma chave privada.

- Certificado da autoridade de certificação (AC)

  Para utilizar um certificado da AC, que identifica a AC e possui uma chave privada própria, tem de importar esse certificado da AC a partir da mesma antes de configurar as funções de segurança da rede.

- Se pretender utilizar a comunicação SSL/TLS, recomendamos que contacte primeiro o administrador do sistema.
- Quando repõe as predefinições de fábrica do servidor de impressão, o certificado e a chave privada que estão instalados são apagados. Se pretender manter o mesmo certificado e a chave privada depois de repor o servidor de impressão, exporte-os antes da reposição e reinstale-os.

## Informações relacionadas

- Configurar certificados para segurança do equipamento

**Tópicos relacionados:**

- Configurar a autenticação IEEE 802.1x para uma rede utilizando a gestão baseada na Web (browser da Web)

# Como criar e instalar um certificado

Existem duas opções para o certificado de segurança: utilizar um certificado auto-assinado ou utilizar um certificado de uma Autoridade de Certificados (CA).

## Opção 1

## Certificado auto-assinado

1. Crie um certificado auto-assinado utilizando a Gestão Baseada na Web.
2. Instale o certificado auto-assinado no computador.

## Opção 2

## Certificado de uma CA

1. Crie um Pedido de Assinatura de Certificado (CSR) utilizando a Gestão Baseada na Web.
2. Instale o certificado emitido pela CA no equipamento Brother utilizando a gestão baseada na Web.
3. Instale o certificado no computador.

## Informações relacionadas

- Configurar certificados para segurança do equipamento

# Criar um certificado auto-assinado

1. Inicie o seu browser.
2. Introduza "https://endereço IP do equipamento" na barra de endereço do seu browser (em que "endereço IP do equipamento" é o endereço IP do seu equipamento).

   Por exemplo:

   https://192.168.1.2

   Pode encontrar o endereço IP do equipamento no relatório de configuração da rede.
3. Se necessário, introduza a palavra-passe no campo **Iniciar sessão** e clique em **Iniciar sessão**.

   A palavra-passe predefinida para gerir as definições deste equipamento encontra-se na parte posterior ou na base do equipamento com a indicação “**Pwd**”. Altere a palavra-passe predefinida seguindo as instruções no ecrã quando iniciar sessão pela primeira vez.
4. Na barra de navegação do lado esquerdo, clique em **Rede** > **Segurança** > **Certificado**.

   Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ≡.
5. Clique em **Criar certificado autoassinado**.
6. Introduza um **Nome comum** e uma **Data válida**.
   - O tamanho do **Nome comum** é inferior a 64 bytes. Introduza um identificador, como um endereço IP, nome do nó ou nome do domínio, para utilizar quando aceder a este equipamento através da comunicação SSL/TLS. Por predefinição, é apresentado o nome do nó.
   - Aparecerá uma advertência se utilizar o protocolo IPPS ou HTTPS se introduzir no URL um nome diferente do **Nome comum** que foi utilizado para o certificado auto-assinado.
7. Selecione a sua definição na lista pendente **Algoritmo de chave pública**.
8. Selecione a sua definição na lista pendente **Algoritmo resumido**.
9. Clique em **Submeter**.

## Informações relacionadas

- Configurar certificados para segurança do equipamento

# Criar um pedido de assinatura de certificado (CSR) e instalar um certificado de uma autoridade de certificação (CA)

Se já tem um certificado de uma autoridade de certificação (CA) externa de confiança, pode guardar o certificado e a chave privada no equipamento e geri-los através de importação e exportação. Se não tiver um certificado de uma CA externa de confiança, crie um pedido de assinatura de certificado (CSR), envie-o para uma CA para autenticação e instale o certificado que receber de volta no equipamento.

- Criar um CSR (Certificate Signing Request)
- Instalar um certificado no equipamento

# Criar um CSR (Certificate Signing Request)

Um Pedido de Assinatura de Certificado (CSR) é um pedido que é enviado a uma Autoridade de Certificados (CA) para autenticação das credenciais contidas no certificado.

Recomendamos a instalação de um Certificado Raiz da CA no seu computador antes da criação do CSR.

1. Inicie o seu browser.
2. Introduza "https://endereço IP do equipamento" na barra de endereço do seu browser (em que "endereço IP do equipamento" é o endereço IP do seu equipamento).

   Por exemplo:

   https://192.168.1.2

   Pode encontrar o endereço IP do equipamento no relatório de configuração da rede.
3. Se necessário, introduza a palavra-passe no campo **Iniciar sessão** e clique em **Iniciar sessão**.

   A palavra-passe predefinida para gerir as definições deste equipamento encontra-se na parte posterior ou na base do equipamento com a indicação “**Pwd**”. Altere a palavra-passe predefinida seguindo as instruções no ecrã quando iniciar sessão pela primeira vez.
4. Na barra de navegação do lado esquerdo, clique em **Rede** > **Segurança** > **Certificado**.

   Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ≡.
5. Clique em **Criar CSR**.
6. Introduza um **Nome comum** (obrigatório) e adicione mais informações acerca da sua **Organização** (opcional).

   - Terá de indicar os dados da sua empresa para que uma CA possa confirmar a sua identidade e atestá-la perante terceiros.
   - O tamanho do **Nome comum** tem de ser inferior a 64 bytes. Introduza um identificador, como um endereço IP, nome do nó ou nome do domínio, para utilizar quando aceder a este equipamento através da comunicação SSL/TLS. Por predefinição, é apresentado o nome do nó. O **Nome comum** é necessário.
   - Aparecerá uma advertência se introduzir no URL um nome diferente do nome comum que foi utilizado para o certificado.
   - O tamanho de **Organização**, de **Unidade organizacional**, de **Cidade/Localidade** e de **Distrito** tem de ser inferior a 64 bytes.
   - O **País/Região** deve ser um código de país ISO 3166 com dois carateres.
   - Se estiver a configurar uma extensão de certificado X.509v3, selecione a caixa de verificação **Configurar partição expandida** e selecione **Auto (Registar IPv4)** ou **Manual**.
7. Selecione a sua definição na **Algoritmo de chave pública** lista pendente.
8. Selecione a sua definição na **Algoritmo resumido** lista pendente.
9. Clique em **Submeter**.

   O CSR aparece no seu ecrã. Guarde o CSR num ficheiro ou copie-o e cole-o no formulário de CSR online disponibilizado pela Autoridade de Certificados.
10. Clique em **Guardar**.

- Siga a política da sua CA em relação ao método de envio de um CSR para a CA.
- Se estiver a utilizar a opção Enterprise root CA do Windows Server, recomendamos que utilize o Servidor Web para o modelo de certificado para criar o Certificado de Cliente de forma segura. Se estiver a criar um Certificado de Cliente para um ambiente IEEE 802.1x com autenticação EAP-TLS, recomendamos que utilize Utilizador para o modelo do certificado.

## Informações relacionadas

- Criar um pedido de assinatura de certificado (CSR) e instalar um certificado de uma autoridade de certificação (CA)

# Instalar um certificado no equipamento

Quando receber um certificado de uma Autoridade de Certificação (CA), siga estes passos para o instalar no servidor de impressão:

> Só é possível instalar neste equipamento um certificado emitido com o pedido de assinatura de certificado (CSR) deste equipamento. Quando pretender criar outro CSR, verifique se o certificado está instalado antes de criar o novo CSR. Crie outro CSR apenas depois de instalar o certificado no equipamento, caso contrário, o CSR criado antes da instalação do novo CSR será inválido.

1. Inicie o seu browser.
2. Introduza "https://endereço IP do equipamento" na barra de endereço do seu browser (em que "endereço IP do equipamento" é o endereço IP do seu equipamento).

   Por exemplo:

   https://192.168.1.2

   Pode encontrar o endereço IP do equipamento no relatório de configuração da rede.
3. Se necessário, introduza a palavra-passe no campo **Iniciar sessão** e clique em **Iniciar sessão**.

   A palavra-passe predefinida para gerir as definições deste equipamento encontra-se na parte posterior ou na base do equipamento com a indicação “**Pwd**”. Altere a palavra-passe predefinida seguindo as instruções no ecrã quando iniciar sessão pela primeira vez.
4. Na barra de navegação do lado esquerdo, clique em **Rede** > **Segurança** > **Certificado**.

   Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ≡.
5. Clique em **Instalar certificado**.
6. Procure o ficheiro que contém o certificado emitido pela CA e clique em **Submeter**.

   O certificado está criado e guardado na memória do equipamento.

Para utilizar a comunicação SSL/TLS, é necessário instalar o certificado raiz da CA no computador. Contacte o administrador da sua rede.

## Informações relacionadas

- Criar um pedido de assinatura de certificado (CSR) e instalar um certificado de uma autoridade de certificação (CA)

# Importar e exportar o certificado e a chave privada

Guarde o certificado e a chave privada no equipamento e gira-os através de importação e exportação.

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

# Importar um certificado e uma chave privada

1. Inicie o seu browser.
2. Introduza "https://endereço IP do equipamento" na barra de endereço do seu browser (em que "endereço IP do equipamento" é o endereço IP do seu equipamento).

   Por exemplo:

   https://192.168.1.2

   Pode encontrar o endereço IP do equipamento no relatório de configuração da rede.
3. Se necessário, introduza a palavra-passe no campo **Iniciar sessão** e clique em **Iniciar sessão**.

   A palavra-passe predefinida para gerir as definições deste equipamento encontra-se na parte posterior ou na base do equipamento com a indicação “**Pwd**”. Altere a palavra-passe predefinida seguindo as instruções no ecrã quando iniciar sessão pela primeira vez.
4. Na barra de navegação do lado esquerdo, clique em **Rede** > **Segurança** > **Certificado**.

   Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ≡.
5. Clique em **Importar certificado e chave privada**.
6. Procure e selecione o ficheiro que pretende importar.
7. Introduza a palavra-passe se o ficheiro estiver encriptado e clique em **Submeter**.

O certificado e a chave privada são importados para o equipamento.

## Informações relacionadas

- Importar e exportar o certificado e a chave privada

# Exportar o certificado e a chave privada

1. Inicie o seu browser.
2. Introduza "https://endereço IP do equipamento" na barra de endereço do seu browser (em que "endereço IP do equipamento" é o endereço IP do seu equipamento).

   Por exemplo:

   https://192.168.1.2

   Pode encontrar o endereço IP do equipamento no relatório de configuração da rede.
3. Se necessário, introduza a palavra-passe no campo **Iniciar sessão** e clique em **Iniciar sessão**.

   A palavra-passe predefinida para gerir as definições deste equipamento encontra-se na parte posterior ou na base do equipamento com a indicação “**Pwd**”. Altere a palavra-passe predefinida seguindo as instruções no ecrã quando iniciar sessão pela primeira vez.
4. Na barra de navegação do lado esquerdo, clique em **Rede** > **Segurança** > **Certificado**.

   Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ≡.
5. Clique em **Exportar** que aparece com **Lista de certificados**.
6. Introduza a palavra-passe se quiser encriptar o ficheiro.

   Se utilizar uma palavra-passe em branco, a saída não é encriptada.
7. Volte a introduzir a palavra-passe para confirmar e clique em **Submeter**.
8. Clique em **Guardar**.

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

Também pode importar o certificado para o computador.

## Informações relacionadas

- Importar e exportar o certificado e a chave privada

# Importar e exportar um certificado da AC

Pode importar, exportar e armazenar certificados CA no equipamento Brother.

- Importar um certificado da AC
- Exportar um certificado da AC

# Importar um certificado da AC

1. Inicie o seu browser.
2. Introduza "https://endereço IP do equipamento" na barra de endereço do seu browser (em que "endereço IP do equipamento" é o endereço IP do seu equipamento).

   Por exemplo:

   https://192.168.1.2

   Pode encontrar o endereço IP do equipamento no relatório de configuração da rede.
3. Se necessário, introduza a palavra-passe no campo **Iniciar sessão** e clique em **Iniciar sessão**.

   A palavra-passe predefinida para gerir as definições deste equipamento encontra-se na parte posterior ou na base do equipamento com a indicação “**Pwd**”. Altere a palavra-passe predefinida seguindo as instruções no ecrã quando iniciar sessão pela primeira vez.
4. Na barra de navegação do lado esquerdo, clique em **Rede** > **Segurança** > **Certificado de AC**.

   Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ≡.
5. Clique em **Importar certificado de AC**.
6. Procure o ficheiro que pretende importar.
7. Clique em **Submeter**.

## Informações relacionadas

- Importar e exportar um certificado da AC

# Exportar um certificado da AC

1. Inicie o seu browser.
2. Introduza "https://endereço IP do equipamento" na barra de endereço do seu browser (em que "endereço IP do equipamento" é o endereço IP do seu equipamento).

   Por exemplo:

   https://192.168.1.2

   Pode encontrar o endereço IP do equipamento no relatório de configuração da rede.
3. Se necessário, introduza a palavra-passe no campo **Iniciar sessão** e clique em **Iniciar sessão**.

   A palavra-passe predefinida para gerir as definições deste equipamento encontra-se na parte posterior ou na base do equipamento com a indicação “**Pwd**”. Altere a palavra-passe predefinida seguindo as instruções no ecrã quando iniciar sessão pela primeira vez.
4. Na barra de navegação do lado esquerdo, clique em **Rede** > **Segurança** > **Certificado de AC**.

   Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ≡.
5. Selecione o certificado que pretende exportar e clique em **Exportar**.
6. Clique em **Submeter**.

## Informações relacionadas

- Importar e exportar um certificado da AC

# Utilizar o SSL/TLS

- Gerir o equipamento de rede em segurança utilizando SSL/TLS
- Imprimir documentos com segurança utilizando SSL/TLS
- Enviar ou receber uma mensagem de e-mail em segurança utilizando SSL/TLS

# Gerir o equipamento de rede em segurança utilizando SSL/TLS

- Configurar um certificado para o SSL/TLS e protocolos disponíveis
- Aceder à gestão baseada na Web utilizando o SSL/TLS
- Instalar o certificado autoassinado para utilizadores do Windows na qualidade de administrador
- Configurar certificados para segurança do equipamento

# Configurar um certificado para o SSL/TLS e protocolos disponíveis

Configure um certificado no seu equipamento utilizando a gestão baseada na Web antes de utilizar a comunicação SSL/TLS.

1. Inicie o seu browser.
2. Introduza "https://endereço IP do equipamento" na barra de endereço do seu browser (em que "endereço IP do equipamento" é o endereço IP do seu equipamento).

   Por exemplo:

   https://192.168.1.2

   Pode encontrar o endereço IP do equipamento no relatório de configuração da rede.
3. Se necessário, introduza a palavra-passe no campo **Iniciar sessão** e clique em **Iniciar sessão**.

   A palavra-passe predefinida para gerir as definições deste equipamento encontra-se na parte posterior ou na base do equipamento com a indicação “**Pwd**”. Altere a palavra-passe predefinida seguindo as instruções no ecrã quando iniciar sessão pela primeira vez.
4. Na barra de navegação do lado esquerdo, clique em **Rede** > **Rede** > **Protocolo**.

   Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ≡.
5. Clique em **Definições do Servidor HTTP**.
6. Selecione o certificado que pretende configurar na lista pendente **Selecionar o certificado**.
7. Clique em **Submeter**.
8. Clique em **Sim** para reiniciar o seu servidor de impressão.

## Informações relacionadas

- Gerir o equipamento de rede em segurança utilizando SSL/TLS

**Tópicos relacionados:**

- Imprimir documentos com segurança utilizando SSL/TLS

# Aceder à gestão baseada na Web utilizando o SSL/TLS

Para gerir o seu equipamento de rede com segurança, tem de utilizar os utilitários de gestão com protocolos de segurança.

- Para utilizar o protocolo HTTPS, é necessário ativar o HTTPS no equipamento. Por predefinição, o protocolo HTTPS está ativado.
- Pode alterar as definições de protocolo HTTPS no ecrã da gestão baseada na Web.

1. Inicie o seu browser.
2. Introduza "https://endereço IP do equipamento" na barra de endereço do seu browser (em que "endereço IP do equipamento" é o endereço IP do seu equipamento).

   Por exemplo:

   https://192.168.1.2

   Pode encontrar o endereço IP do equipamento no relatório de configuração da rede.
3. Se necessário, introduza a palavra-passe no campo **Iniciar sessão** e clique em **Iniciar sessão**.

   A palavra-passe predefinida para gerir as definições deste equipamento encontra-se na parte posterior ou na base do equipamento com a indicação “**Pwd**”. Altere a palavra-passe predefinida seguindo as instruções no ecrã quando iniciar sessão pela primeira vez.
4. Já pode aceder ao equipamento utilizando HTTPS.

## Informações relacionadas

- Gerir o equipamento de rede em segurança utilizando SSL/TLS

# Instalar o certificado autoassinado para utilizadores do Windows na qualidade de administrador

- Os passos seguintes destinam-se ao Microsoft Edge. Se utilizar outro browser da Web, consulte a documentação do seu browser ou a ajuda online para obter instruções sobre como instalar certificados.
- Certifique-se que criou o seu certificado autoassinado utilizando a gestão baseada na Web.

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

   Se aparecer o ecrã **Controlo de Conta de Utilizador**, clique em **Sim**.
2. Introduza "https://endereço IP do equipamento" na barra de endereço do seu browser (em que "endereço IP do equipamento" é o endereço IP do seu equipamento).

   Por exemplo:

   https://192.168.1.2

   Pode encontrar o endereço IP do equipamento no relatório de configuração da rede.
3. Se a sua ligação não for privada, clique no botão **Avançadas** e continue para a página da Web.
4. Se necessário, introduza a palavra-passe no campo **Iniciar sessão** e clique em **Iniciar sessão**.

   A palavra-passe predefinida para gerir as definições deste equipamento encontra-se na parte posterior ou na base do equipamento com a indicação “**Pwd**”. Altere a palavra-passe predefinida seguindo as instruções no ecrã quando iniciar sessão pela primeira vez.
5. Na barra de navegação do lado esquerdo, clique em **Rede** > **Segurança** > **Certificado**.

   Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ≡.
6. Clique em **Exportar**.
7. Para encriptar o ficheiro de saída, introduza uma palavra-passe no campo **Introduzir palavra-passe/senha**. Se o campo **Introduzir palavra-passe/senha** ficar em branco, o ficheiro produzido não será encriptado.
8. Introduza a palavra-passe novamente no campo **Voltar a escrever palavra-passe/senha** e clique em **Submeter**.
9. Clique no ficheiro descarregado para o abrir.
10. Quando aparecer **Assistente para importar certificados**, clique em **Seguinte**.
11. Clique em **Seguinte**.
12. Se necessário, introduza uma palavra-passe e clique em **Seguinte**.
13. Selecione **Colocar todos os certificados no seguinte arquivo** e clique em **Procurar...**.
14. Selecione **Autoridades de certificação de raiz fidedignas** e clique em **OK**.
15. Clique em **Seguinte**.
16. Clique em **Concluir**.
17. Clique em **Sim** se a impressão digital (dedo polegar) estiver correta.
18. Clique em **OK**.

## Informações relacionadas

- Gerir o equipamento de rede em segurança utilizando SSL/TLS

# Imprimir documentos com segurança utilizando SSL/TLS

- Imprimir documentos com IPPS
- Configurar um certificado para o SSL/TLS e protocolos disponíveis
- Configurar certificados para segurança do equipamento

# Imprimir documentos com IPPS

Para imprimir documentos de forma segura com o protocolo IPP, utilize o protocolo IPPS.

1. Inicie o seu browser.
2. Introduza "https://endereço IP do equipamento" na barra de endereço do seu browser (em que "endereço IP do equipamento" é o endereço IP do seu equipamento).

   Por exemplo:

   https://192.168.1.2

   Pode encontrar o endereço IP do equipamento no relatório de configuração da rede.
3. Se necessário, introduza a palavra-passe no campo **Iniciar sessão** e clique em **Iniciar sessão**.

   A palavra-passe predefinida para gerir as definições deste equipamento encontra-se na parte posterior ou na base do equipamento com a indicação “**Pwd**”. Altere a palavra-passe predefinida seguindo as instruções no ecrã quando iniciar sessão pela primeira vez.
4. Na barra de navegação do lado esquerdo, clique em **Rede** > **Rede** > **Protocolo**.

   Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ≡.
5. Certifique-se de que a caixa de verificação **IPP** está selecionada.

   Se a caixa de verificação **IPP** não estiver selecionada, selecione a caixa de verificação **IPP** e clique em **Submeter**.

   Reinicie o equipamento para ativar a configuração.

   Após o equipamento reiniciar, volte para a página Web do equipamento, introduza a palavra-passe e, em seguida, na barra de navegação do lado esquerdo, clique em **Rede** > **Rede** > **Protocolo**.
6. Clique em **Definições do Servidor HTTP**.
7. Selecione a caixa de verificação **HTTPS** na área **IPP** e clique em **Submeter**.
8. Reinicie o equipamento para ativar a configuração.

A comunicação através de IPPS não consegue impedir o acesso não autorizado ao servidor de impressão.

## Informações relacionadas

- Imprimir documentos com segurança utilizando SSL/TLS

# Utilizar o SNMPv3

- Gerir o equipamento de rede em segurança utilizando o SNMPv3

# Gerir o equipamento de rede em segurança utilizando o SNMPv3

O SNMPv3 (Simple Network Management Protocol version 3, protocolo simples de gestão de rede versão 3) fornece autenticação do utilizador e encriptação de dados para gerir equipamentos de rede em segurança.

1. Inicie o seu browser.
2. Digite “https://Nome Comum” na barra de endereço do seu browser (em que “Nome Comum” é o nome comum que atribuiu ao certificado; pode ser o seu endereço IP, nome de nó ou nome de domínio).
3. Se necessário, introduza a palavra-passe no campo **Iniciar sessão** e clique em **Iniciar sessão**.

A palavra-passe predefinida para gerir as definições deste equipamento encontra-se na parte posterior ou na base do equipamento com a indicação “**Pwd**”. Altere a palavra-passe predefinida seguindo as instruções no ecrã quando iniciar sessão pela primeira vez.

4. Na barra de navegação do lado esquerdo, clique em **Rede** > **Rede** > **Protocolo**.

Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ≡.

5. Certifique-se de que a definição **SNMP** está ativada e clique em **Definições avançadas**.
6. Configure as definições do modo SNMPv1/v2c.

| Opção | Descrição |
|---|---|
| **Acesso de leit./escr. SNMP v1/v2c** | O servidor de impressão utiliza a versão 1 e a versão 2c do protocolo SNMP. Pode utilizar todas as aplicações do equipamento neste modo. Contudo, isso não é seguro porque não autentica o utilizador e os dados não serão encriptados. |
| **Acesso só de leitura a SNMP v1/v2c** | O servidor de impressão utiliza o acesso só de leitura da versão 1 e da versão 2c do protocolo SNMP. |
| **Desativado** | Desative a versão 1 e a versão 2c do protocolo SNMP.<br>Todas as aplicações que utilizam SNMPv1/v2c ficarão restringidas. Para permitir a utilização de aplicações SNMPv1/v2c, utilize o modo **Acesso só de leitura a SNMP v1/v2c** ou **Acesso de leit./escr. SNMP v1/v2c**. |

7. Configure as definições do modo SNMPv3.

| Opção | Descrição |
|---|---|
| **Ativado** | O servidor de impressão utiliza a versão 3 do protocolo SNMP. Para gerir o servidor de impressão de forma segura, utilize o modo SNMPv3 e, em seguida, configure as definições. |
| **Desativado** | Desative a versão 3 do protocolo SNMP.<br>Todas as aplicações que utilizam SNMPv3 ficarão restringidas. Para permitir a utilização de aplicações SNMPv3, utilize o modo SNMPv3. |

8. Clique em **Submeter**.

Se o equipamento apresentar as opções de definição de protocolo, selecione as opções pretendidas.

9. Reinicie o equipamento para ativar a configuração.

## Informações relacionadas

- Utilizar o SNMPv3

# Utilizar a autenticação IEEE 802.1x para uma rede

- O que é a autenticação IEEE 802.1x?
- Configurar a autenticação IEEE 802.1x para uma rede utilizando a gestão baseada na Web (browser da Web)
- Métodos de Autenticação para IEEE 802.1x

# O que é a autenticação IEEE 802.1x?

IEEE 802.1x é um padrão IEEE que limita o acesso a partir de dispositivos de rede não autorizados. O equipamento Brother envia um pedido de autenticação para um servidor RADIUS (servidor de autenticação) através do ponto de acesso ou hub. Após o pedido ter sido verificado pelo servidor RADIUS, o equipamento consegue ter acesso à rede.

## Informações relacionadas

- Utilizar a autenticação IEEE 802.1x para uma rede

# Configurar a autenticação IEEE 802.1x para uma rede utilizando a gestão baseada na Web (browser da Web)

- Se configurar o equipamento utilizando a autenticação EAP-TLS, tem de instalar o certificado do cliente emitido por uma AC antes de iniciar a configuração. Contacte o administrador de rede para obter informações sobre o certificado do cliente. Se tiver instalado mais de um certificado, é recomendável tomar nota do nome do certificado que pretende utilizar.
- Antes de verificar o certificado do servidor, tem de importar o certificado da AC emitido pela AC que assinou o certificado do servidor. Contacte o administrador de rede ou o ISP (Internet Service Provider, fornecedor de serviços de Internet) para confirmar se é necessário importar um certificado da AC.

Também pode configurar a autenticação IEEE 802.1x utilizando o Assistente de Instalação Sem Fios a partir do painel de controlo (Rede sem fios).

1. Inicie o seu browser.
2. Introduza "https://endereço IP do equipamento" na barra de endereço do seu browser (em que "endereço IP do equipamento" é o endereço IP do seu equipamento).

   Por exemplo:

   https://192.168.1.2

   Pode encontrar o endereço IP do equipamento no relatório de configuração da rede.
3. Se necessário, introduza a palavra-passe no campo **Iniciar sessão** e clique em **Iniciar sessão**.

A palavra-passe predefinida para gerir as definições deste equipamento encontra-se na parte posterior ou na base do equipamento com a indicação “**Pwd**”. Altere a palavra-passe predefinida seguindo as instruções no ecrã quando iniciar sessão pela primeira vez.

4. Na barra de navegação do lado esquerdo, clique em **Rede**.

Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ≡.

5. Execute uma das seguintes ações:
   - Para a rede com fios

     Clique em **Com fios** > **Autenticação 802.1x com fios**.
   - Para a rede sem fios

     Clique em **Sem fios** > **Sem fios (empresa)**.
6. Configure as definições de autenticação de IEEE 802.1x.

- Se pretender ativar a autenticação IEEE 802.1x para redes com fios, selecione **Ativado** para **Estado 802.1x com fios** na página **Autenticação 802.1x com fios**.
- Se estiver a utilizar a autenticação **EAP-TLS**, tem de selecionar o certificado do cliente instalado (apresentado com o nome do certificado) para a verificação a partir da lista pendente **Certificado de cliente**.
- Se selecionar a autenticação **EAP-FAST**, **PEAP**, **EAP-TTLS** ou **EAP-TLS**, selecione o método de verificação na lista pendente **Verificação do certificado do servidor**. Verifique o certificado do servidor utilizando o certificado CA, importado previamente para o equipamento, que foi emitido pela autoridade de certificados (CA) que assinou o certificado do servidor.

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

| Opção | Descrição |
| --- | --- |
| **Sem verificação** | O certificado do servidor é sempre de confiança. A verificação não é efetuada. |
| **Cert. AC** | Método de verificação para atestar a fiabilidade da CA do certificado do servidor, utilizando o certificado CA emitido pela CA que assinou o certificado do servidor. |
| **Cert. AC + ID do servidor** | Método de verificação para verificar o nome comum [1] do certificado do servidor, além da fiabilidade da autoridade de certificados (CA) do certificado do servidor. |

7. Quando terminar a configuração, clique em **Submeter**.

   Para redes com fios: Após a configuração, ligue o equipamento à rede com suporte de IEEE 802.1x. Após alguns minutos, imprima o relatório da configuração de rede para verificar o estado de <**Wired IEEE 802.1x**>.

| Opção | Descrição |
| --- | --- |
| **Success** | A função de IEEE 802.1x com fios está ativada e a autenticação foi bem sucedida. |
| **Failed** | A função de IEEE 802.1x com fios está ativada, mas a autenticação falhou. |
| **Off** | A função de IEEE 802.1x com fios não está disponível. |

## Informações relacionadas

- Utilizar a autenticação IEEE 802.1x para uma rede

**Tópicos relacionados:**

- Descrição geral das funções de certificados de segurança
- Configurar certificados para segurança do equipamento

1 A verificação do nome comum compara o nome comum do certificado do servidor com os carateres da **ID do servidor**. Antes de utilizar este método, contacte o administrador de sistema para saber qual é o nome comum do certificado do servidor e, em seguida, configure a **ID do servidor**.

# Métodos de Autenticação para IEEE 802.1x

**EAP-FAST**

O protocolo EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secured Tunnel) foi desenvolvido pela Cisco Systems, Inc. e utiliza uma ID de utilizador e palavra-passe para fazer a autenticação e algoritmos de chave simétrica para obter um processo de autenticação em túnel.

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

- EAP-FAST/NONE
- EAP-FAST/MS-CHAPv2
- EAP-FAST/GTC

**EAP-MD5 (Rede com fios)**

O EAP-MD5 (Extensible Authentication Protocol-Message Digest Algorithm 5) utiliza uma ID de utilizador e uma palavra-passe para fazer uma autenticação do tipo desafio-resposta.

**PEAP**

O PEAP (Protected Extensible Authentication Protocol) é uma versão do método EAP desenvolvida pela Cisco Systems, Inc. em colaboração com a Microsoft Corporation e a RSA Security. O PEAP cria um túnel encriptado SSL (Secure Sockets Layer)/TLS (Transport Layer Security) entre um cliente e um servidor de autenticação, para enviar uma ID de utilizador e uma palavra-passe. O PEAP proporciona uma autenticação mútua entre o servidor e o cliente.

O 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 pela Certicom. O EAP-TTLS cria um túnel SSL encriptado idêntico ao do PEAP, entre um cliente e um servidor de autenticação, para enviar uma identificação de utilizador e uma palavra-passe. O EAP-TTLS proporciona uma autenticação mútua entre o servidor e o cliente.

O 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) necessita de uma autenticação certificada digital no cliente e no servidor de autenticação.

## Informações relacionadas

- Utilizar a autenticação IEEE 802.1x para uma rede