Guia de recursos de segurança

Índice

Introdução

Definições de notas

Ao longo deste Manual do Utilizador, são utilizados os seguintes símbolos e convenções:

IMPORTANTE	IMPORTANTE indica uma situação potencialmente perigosa que, se não for evitada, pode resultar em danos materiais ou perda da funcionalidade do produto.
NOTA	NOTA especifica o ambiente de funcionamento, condições de instalação ou condições especiais de utilização.
	Os ícones de sugestão indicam conselhos úteis e informação suplementar.
Negrito	O estilo negrito identifica botões do painel de controlo do equipamento ou do ecrã do computador.
Itálico	O estilo Italicized emphasizes itens importantes ou remete para um tópico relacionado.

Informações relacionadas

- Introdução

Marcas comerciais

Adobe® e Reader® são marcas comerciais registadas ou marcas comerciais da Adobe Systems Incorporated nos Estados Unidos da América e/ou noutros países.

Cada empresa cujo software é mencionado neste manual possui um Contrato de License de Software específico que abrange os seus programas.

Quaisquer denominações comerciais e nomes de produtos constantes em produtos da Brother, documentos afins e quaisquer outros materiais são marcas comerciais ou marcas comerciais registadas das respetivas empresas.

Informações relacionadas

- Introdução

Direitos de autor

Informações relacionadas

- Introdução

Antes de utilizar as funções de segurança de rede

O equipamento utiliza alguns dos mais recentes protocolos de segurança de rede e de encriptação atualmente disponíveis. Estas funções de rede podem ser integradas no plano geral de segurança da rede para o ajudar a proteger os dados e impedir o acesso unauthorized ao equipamento.

Recomendamos que desative os protocolos FTP e TFTP. Não é seguro aceder ao equipamento utilizando estes protocolos.

Informações relacionadas

- Introdução
  - Desativar protocolos desnecessários

Desativar protocolos desnecessários

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. Retire o sinal das caixas de verificação de protocolos desnecessários para os desativar.
6. Clique em **Submeter**.
7. Reinicie o equipamento Brother para ativar a configuração.

Informações relacionadas

- Antes de utilizar as funções de segurança de rede

Segurança da rede

- Configurar certificados para segurança do equipamento
- Utilizar o SSL/TLS
- Utilizar o SNMPv3
- Utilizar o IPsec
- Utilizar a autenticação IEEE 802.1x para uma 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
- Como criar e instalar um certificado
- Criar um certificado auto-assinado
- 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
- Importar e exportar um certificado da AC

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 organization 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(Porta 443)** 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 unauthorized 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. 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.
Desativado	Desative a versão 3 do protocolo SNMP. 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 o IPsec

Introdução ao IPsec

O IPsec (Internet Protocol Security, segurança do protocolo de Internet) é um protocolo de segurança que utiliza uma função opcional de protocolo de Internet para evitar a manipulação de dados e garantir a confidencialidade dos dados transmitidos como pacotes IP. O IPsec encripta os dados transportados pela rede, como dados de impressão enviados de computadores para uma impressora. Como os dados estão encriptados ao nível da camada da rede, as aplicações que utilizam um protocolo de nível superior utilizam IPsec, mesmo se o utilizador não estiver consciente da sua utilização.

O IPsec suporta as seguintes funções:

- Transmissões IPsec

  De acordo com as condições de definição de IPsec, um computador ligado à rede envia dados para o dispositivo especificado e recebe dados do mesmo utilizando IPsec. Quando os dispositivos começam a comunicar utilizando IPsec, são primeiro trocadas chaves utilizando IKE (Internet Key Exchange, troca de chaves da Internet) e depois os dados encriptados são transmitidos utilizando as chaves.

  Além disso, o IPsec possui dois modos de funcionamento: o modo de transporte e o modo de túnel. O modo de Transporte é utilizado principalmente para comunicações entre dispositivos, enquanto o modo Túnel é utilizado em ambientes do tipo VPN (Virtual Private Network).

  Para transmissões IPsec, são necessárias as seguintes condições:
  - Um computador ligado à rede e que consiga comunicar utilizando IPsec.
  - O equipamento está configurado para comunicação IPsec.
  - O computador ligado ao equipamento está configurado para ligações IPsec.

- Definições de IPsec

  Definições que são necessárias para as ligações com IPsec. Estas definições podem ser configuradas através da Gestão Baseada na Web.

  Para configurar as definições de IPsec, é necessário utilizar um browser num computador que esteja ligado à rede.

Informações relacionadas

- Utilizar o IPsec

Configurar o IPsec utilizando a Gestão Baseada na Web

As condições de ligação IPsec incluem dois tipos de **Modelo**: **Endereço** e **IPsec**. Pode configurar até 10 condições de ligação.

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** > **IPsec**.

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

Opção	Descrição
Estado	Ativar ou desativar o IPsec.
Modo de negociação	Selecione **Modo de negociação** para IKE Phase 1. IKE é um protocolo utilizado para troca de chaves de encriptação, que possibilitam a comunicação encriptada utilizando IPsec. No modo **Principal**, a velocidade de processamento é baixa, mas a segurança é elevada. No modo **Agressivo**, a velocidade de processamento é mais rápida do que no modo **Principal**, mas a segurança é mais fraca.
Todo o tráfego não IPsec	Selecione a ação a tomar para os pacotes não IPsec. Quando utilizar os Serviços Web, tem de selecionar **Permitir** para **Todo o tráfego não IPsec**. Se selecionar **Remover**, não pode utilizar os Serviços Web.
Ignorar difusão/multicast	Selecione **Ativado** ou **Desativado**.
Ignorar protocolo	Selecione as caixas de verificação da opção ou das opções que pretender.
Regras	Selecione a caixa de verificação **Ativado** para ativar o modelo. Se selecionar várias caixas de verificação, as que tiverem números menores têm prioridade se ocorrer algum conflito entre as definições das caixas de verificação selecionadas. Clique na lista pendente correspondente para selecionar o **Modelo de endereço** que será utilizado para as condições de ligação IPsec. Para adicionar um **Modelo de endereço**, clique em **Adicionar modelo**. Clique na lista pendente correspondente para selecionar o **Modelo IPsec** que será utilizado para as condições de ligação IPsec. Para adicionar um **Modelo IPsec**, clique em **Adicionar modelo**.

6. Clique em **Submeter**.

   Se for necessário reiniciar o equipamento para ativar as novas definições, aparece um ecrã de confirmação de reinício.

Se existir um item em branco no modelo que tiver ativado na tabela **Regras**, aparece uma mensagem de erro. Confirme as suas escolhas e clique novamente em **Submeter**.

Informações relacionadas

- Utilizar o IPsec

Tópicos relacionados:

- Configurar certificados para segurança do equipamento

Configurar um Modelo de Endereço de IPsec utilizando a 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. Na barra de navegação do lado esquerdo, clique em **Rede** > **Segurança** > **Modelo de endereço IPsec**.

   Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ≡.
5. Clique no botão **Apagar** para eliminar um **Modelo de endereço**. Não é possível eliminar um **Modelo de endereço** que esteja a ser utilizado.
6. Clique no **Modelo de endereço** que pretende criar. Aparece o **Modelo de endereço IPsec**.
7. Configure as definições.

Opção	Descrição
Nome do modelo	Digite um nome para o modelo (até 16 carateres).
Endereço local de IP	• **Endereço IP** Especifique o endereço IP. Selecione **TODOS os endereços IPv4**, **TODOS os endereços IPv6**, **TODAS as ligações locais IPv6** ou **Persnl** na lista pendente. Se selecionar **Persnl** na lista pendente, introduza o endereço IP (IPv4 ou IPv6) na caixa de texto. • **Intervalo de endereço IP** Introduza os endereços IP inicial e final do intervalo de endereços IP nas caixas de texto. Se os endereços IP inicial e final não forem standardized para IPv4 ou IPv6, ou se o endereço IP final for inferior ao endereço inicial, ocorrerá um erro. • **Endereço IP/Prefixo** Especifique o endereço IP utilizando a notação CIDR. Por exemplo: 192.168.1.1/24 Uma vez que o prefixo está especificado na forma de máscara de sub-rede de 24 bits (255.255.255.0) para 192.168.1.1, os endereços válidos são todos os 192.168.1.###.
Endereço IP remoto	• **Qualquer** Se selecionar **Qualquer**, todos os endereços IP são possíveis. • **Endereço IP** Introduza o endereço IP especificado (IPv4 ou IPv6) na caixa de texto. • **Intervalo de endereço IP** Introduza os endereços IP inicial e final do intervalo de endereços IP. Se os endereços IP inicial e final não forem standardized para IPv4 ou IPv6, ou se o endereço IP final for inferior ao endereço inicial, ocorre um erro.

Opção	Descrição
	• **Endereço IP/Prefixo** Especifique o endereço IP utilizando a notação CIDR. Por exemplo: 192.168.1.1/24 Uma vez que o prefixo está especificado na forma de máscara de sub-rede de 24 bits (255.255.255.0) para 192.168.1.1, os endereços válidos são todos os 192.168.1.###.

8. Clique em **Submeter**.

Quando alterar as definições do modelo que está a ser utilizado, reinicie o equipamento para ativar a configuração.

Informações relacionadas

- Utilizar o IPsec

Configurar um Modelo de IPsec utilizando a 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. Na barra de navegação do lado esquerdo, clique em **Rede** > **Segurança** > **Modelo IPsec**.

   Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ≡.
5. Clique no botão **Apagar** para eliminar um **Modelo IPsec**. Não é possível eliminar um **Modelo IPsec** que esteja a ser utilizado.
6. Clique no **Modelo IPsec** que pretende criar. Aparece o ecrã **Modelo IPsec**. Os campos de configuração dependem das definições de **Utilizar modelo com prefixo** e **Internet Key Exchange (IKE)** que selecionar.
7. No campo **Nome do modelo**, introduza um nome para este modelo (até 16 carateres).
8. Se selecionou **Persnl** na lista pendente **Utilizar modelo com prefixo**, selecione as opções do **Internet Key Exchange (IKE)** e altere as definições se necessário.
9. Clique em **Submeter**.

Informações relacionadas

- Utilizar o IPsec
  - Definições de IKEv1 para um Modelo de IPsec
  - Definições de IKEv2 para um Modelo de IPsec
  - Definições manuais para um Modelo de IPsec

Definições de IKEv1 para um Modelo de IPsec

Opção	Descrição
Nome do modelo	Introduza um nome para o modelo (até 16 carateres).
Utilizar modelo com prefixo	Selecione **Persnl**, **Alta segurança de IKEv1** ou **Segurança média de IKEv1**. Os itens de definição dependem do modelo selecionado.
Internet Key Exchange (IKE)	IKE é um protocolo de comunicação utilizado para troca de chaves de encriptação, que possibilitam a comunicação encriptada utilizando IPsec. Para efetuar a comunicação encriptada apenas nessa vez, é determinado o algoritmo de encriptação necessário para o IPsec e as chaves de encriptação são partilhadas. No caso do IKE, a troca das chaves de encriptação é efetuada com o método de troca de chaves Diffie-Hellman e segue-se a comunicação encriptada que diz respeito exclusivamente ao IKE. Se tiver selecionado **Persnl** em **Utilizar modelo com prefixo**, selecione **IKEv1**.
Tipo de autenticação	• **Diffie-Hellman Group** Este método de troca de chaves permite a troca segura de chaves secretas numa rede não protegida. O método de troca de chaves Diffie-Hellman utiliza um problema logarítmico discreto, e não a chave secreta, para enviar e receber a informação aberta que foi gerada utilizando um número aleatório e a 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**. • **Duração de SA** Especifique a validade da associação de segurança IKE. Introduza o tempo (segundos) e a quantidade de quilobytes (KByte).
Segurança encapsulada	• **Protocolo** Selecione **ESP**, **AH** ou **AH+ESP**. - ESP é um protocolo de comunicação encriptada por IPsec. O ESP encripta a carga útil (conteúdo comunicado) e acrescenta informações adicionais. O pacote IP é composto pelo cabeçalho e pela carga útil encriptada que sucede ao cabeçalho. Além da carga útil encriptada, o pacote IP também inclui informação relativa ao método de encriptação e à chave de encriptação, os dados de autenticação, etc. - O AH é a parte do protocolo IPsec que autentica o remetente e impede a manipulação (garante que os dados estão completos) dos dados. No pacote IP, os dados são colocados imediatamente após o cabeçalho. Além disso, os pacotes incluem valores de hash, que são calculados com uma equação a partir dos conteúdos comunicados, da chave secreta e de outros itens, com o objetivo de impedir a falsificação do remetente e a manipulação dos dados. Ao contrário do ESP, os conteúdos comunicados não são encriptados e os dados são enviados e recebidos na forma de texto simples. • **Encriptação (Não disponível para a opção AH.)** Selecione **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**.

Opção	Descrição
	• **Hash** Selecione **Nenhum**, **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512**. **Nenhum** pode ser selecionado apenas quando **ESP** estiver selecionado em **Protocolo**. • **Duração de SA** Especificar o tempo de vida da SA do IKE. Introduza o tempo (segundos) e o número de kilobytes (KByte). • **Modo de encapsulamento** Selecione **Transporte** ou **Túnel**. • **Endereço IP do router remoto** Introduza o endereço IP (IPv4 ou IPv6) do router remoto. Introduza esta informação apenas quando o modo **Túnel** estiver selecionado. SA (Security Association) é um método de comunicação encriptada por IPsec ou IPv6, que troca e partilha informação, como o método de encriptação e a chave de encriptação, para estabelecer um canal de comunicação segura antes do início da comunicação. O SA também pode aplicar-se a um canal virtual de comunicação encriptada que tenha sido estabelecido. O SA utilizado com o IPsec estabelece o método de encriptação, troca as chaves e efetua a autenticação mútua de acordo com o procedimento standard do IKE (Internet Key Exchange). Além disso, o SA é atualizado periodicamente.
Perfect Forward Secrecy (PFS)	O PFS não deriva chaves a partir de chaves anteriores que tenham sido utilizadas para encriptar mensagens. Além disso, se uma chave que é utilizada para encriptar uma mensagem tiver sido derivada de uma chave ascendente, essa chave ascendente não é utilizada para derivar outras chaves. Assim, mesmo que uma chave seja comprometida, os danos serão limitados às mensagens que tenham sido encriptadas com essa chave. Selecione **Ativado** ou **Desativado**.
Método de autenticação	Selecione o método de autenticação. Selecione **Chave pré-partilhada** ou **Certificados**.
Chave pré-partilhada	Quando encriptar a comunicação, a chave de encriptação é trocada e partilhada previamente utilizando outro canal. Se tiver selecionado **Chave pré-partilhada** como **Método de autenticação**, introduza a **Chave pré-partilhada** (até 32 carateres). • **Local/Tipo de ID/ID** Selecione o tipo de ID do remetente e introduza a ID. Selecione **Endereço IPv4**, **Endereço IPv6**, **FQDN**, **Endereço de e-mail** ou **Certificado** para o tipo. Se tiver selecionado **Certificado**, introduza o nome comum do certificado no campo **ID**. • **Remoto/Tipo de ID/ID** Selecione o tipo de ID do destinatário e introduza a ID. Selecione **Endereço IPv4**, **Endereço IPv6**, **FQDN**, **Endereço de e-mail** ou **Certificado** para o tipo. Se tiver selecionado **Certificado**, introduza o nome comum do certificado no campo **ID**.
Certificado	Se tiver selecionado **Certificados** para **Método de autenticação**, selecione o certificado.

Opção	Descrição
	Pode selecionar apenas os certificados que tenham sido criados através da página **Certificado** do ecrã de configuração de segurança da Gestão baseada na Web.

Informações relacionadas

- Configurar um Modelo de IPsec utilizando a Gestão Baseada na Web

Definições de IKEv2 para um Modelo de IPsec

Opção	Descrição
Nome do modelo	Introduza um nome para o modelo (até 16 carateres).
Utilizar modelo com prefixo	Selecione **Persnl**, **Alta segurança de IKEv2** ou **Segurança média de IKEv2**. Os itens de definição dependem do modelo selecionado.
Internet Key Exchange (IKE)	IKE é um protocolo de comunicação utilizado para troca de chaves de encriptação, que possibilitam a comunicação encriptada utilizando IPsec. Para efetuar a comunicação encriptada apenas nessa vez, é determinado o algoritmo de encriptação necessário para o IPsec e as chaves de encriptação são partilhadas. No caso do IKE, a troca das chaves de encriptação é efetuada com o método de troca de chaves Diffie-Hellman e segue-se a comunicação encriptada que diz respeito exclusivamente ao IKE. Se tiver selecionado **Persnl** em **Utilizar modelo com prefixo**, selecione **IKEv2**.
Tipo de autenticação	• **Diffie-Hellman Group** Este método de troca de chaves permite a troca segura de chaves secretas numa rede não protegida. O método de troca de chaves Diffie-Hellman utiliza um problema logarítmico discreto, e não a chave secreta, para enviar e receber a informação aberta que foi gerada utilizando um número aleatório e a 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**. • **Duração de SA** Especifique a validade da associação de segurança IKE. Introduza o tempo (segundos) e a quantidade de quilobytes (KByte).
Segurança encapsulada	• **Protocolo** Selecione **ESP**. ESP é um protocolo de comunicação encriptada por IPsec. O ESP encripta a carga útil (conteúdo comunicado) e acrescenta informações adicionais. O pacote IP é composto pelo cabeçalho e pela carga útil encriptada que sucede ao cabeçalho. Além da carga útil encriptada, o pacote IP também inclui informação relativa ao método de encriptação e à chave de encriptação, os dados de autenticação, etc. • **Encriptação** Selecione **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**. • **Hash** Selecione **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512**. • **Duração de SA** Especificar o tempo de vida da SA do IKE. Introduza o tempo (segundos) e o número de kilobytes (KByte). • **Modo de encapsulamento** Selecione **Transporte** ou **Túnel**.

Opção	Descrição
	• **Endereço IP do router remoto** Introduza o endereço IP (IPv4 ou IPv6) do router remoto. Introduza esta informação apenas quando o modo **Túnel** estiver selecionado. SA (Security Association) é um método de comunicação encriptada por IPsec ou IPv6, que troca e partilha informação, como o método de encriptação e a chave de encriptação, para estabelecer um canal de comunicação segura antes do início da comunicação. O SA também pode aplicar-se a um canal virtual de comunicação encriptada que tenha sido estabelecido. O SA utilizado com o IPsec estabelece o método de encriptação, troca as chaves e efetua a autenticação mútua de acordo com o procedimento standard do IKE (Internet Key Exchange). Além disso, o SA é atualizado periodicamente.
Perfect Forward Secrecy (PFS)	O PFS não deriva chaves a partir de chaves anteriores que tenham sido utilizadas para encriptar mensagens. Além disso, se uma chave que é utilizada para encriptar uma mensagem tiver sido derivada de uma chave ascendente, essa chave ascendente não é utilizada para derivar outras chaves. Assim, mesmo que uma chave seja comprometida, os danos serão limitados às mensagens que tenham sido encriptadas com essa chave. Selecione **Ativado** ou **Desativado**.
Método de autenticação	Selecione o método de autenticação. Selecione **Chave pré-partilhada**, **Certificados**, **EAP - MD5** ou **EAP - MS-CHAPv2**. O EAP é um protocolo de autenticação que constitui uma extensão do PPP. Quando se utiliza EAP com IEEE802.1x, é utilizada uma chave diferente em cada sessão para a autenticação de utilizadores. As seguintes definições são necessárias apenas quando estiver selecionado **EAP - MD5** ou **EAP - MS-CHAPv2** em **Método de autenticação**: • **Modo** Selecione **Modo servidor** ou **Modo cliente**. • **Certificado** Selecione o certificado. • **Nome do utiliz.** Digite o nome de utilizador (até 32 carateres). • **Palavra-passe/Senha** Digite a palavra-passe (até 32 carateres). A palavra-passe tem de ser introduzida duas vezes para confirmação.
Chave pré-partilhada	Quando encriptar a comunicação, a chave de encriptação é trocada e partilhada previamente utilizando outro canal. Se tiver selecionado **Chave pré-partilhada** como **Método de autenticação**, introduza a **Chave pré-partilhada** (até 32 carateres). • **Local/Tipo de ID/ID** Selecione o tipo de ID do remetente e introduza a ID. Selecione **Endereço IPv4**, **Endereço IPv6**, **FQDN**, **Endereço de e-mail** ou **Certificado** para o tipo. Se tiver selecionado **Certificado**, introduza o nome comum do certificado no campo **ID**. • **Remoto/Tipo de ID/ID** Selecione o tipo de ID do destinatário e introduza a ID.

Opção	Descrição
	Selecione **Endereço IPv4**, **Endereço IPv6**, **FQDN**, **Endereço de e-mail** ou **Certificado** para o tipo. Se tiver selecionado **Certificado**, introduza o nome comum do certificado no campo **ID**.
Certificado	Se tiver selecionado **Certificados** para **Método de autenticação**, selecione o certificado. Pode selecionar apenas os certificados que tenham sido criados através da página **Certificado** do ecrã de configuração de segurança da Gestão baseada na Web.

Informações relacionadas

- Configurar um Modelo de IPsec utilizando a Gestão Baseada na Web

Definições manuais para um Modelo de IPsec

Opção	Descrição
Nome do modelo	Introduza um nome para o modelo (até 16 carateres).
Utilizar modelo com prefixo	Selecione **Persnl**.
Internet Key Exchange (IKE)	IKE é um protocolo de comunicação utilizado para troca de chaves de encriptação, que possibilitam a comunicação encriptada utilizando IPsec. Para efetuar a comunicação encriptada apenas nessa vez, é determinado o algoritmo de encriptação necessário para o IPsec e as chaves de encriptação são partilhadas. No caso do IKE, a troca das chaves de encriptação é efetuada com o método de troca de chaves Diffie-Hellman e segue-se a comunicação encriptada que diz respeito exclusivamente ao IKE. Selecione **Manual**.
Chave de autenticação (ESP, AH)	Introduza os valores **Entrada/Saída**. Estas definições são necessárias quando estiver selecionado **Persnl** para **Utilizar modelo com prefixo**, quando estiver selecionado **Manual** para **Internet Key Exchange (IKE)** e quando estiver selecionado algo diferente de **Nenhum** para **Hash** na secção **Segurança encapsulada**. O número de carateres que é possível definir depende da definição selecionada para **Hash** na secção **Segurança encapsulada**. Se o comprimento da chave de autenticação especificada for diferente do algoritmo de chave do documento selecionado, irá ocorrer um erro. • **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 em “ASCII Code” (Código ASCII), inclua os carateres em aspas duplas (").
Chave de código (ESP)	Introduza os valores **Entrada/Saída**. Estas definições são necessárias quando a opção **Persnl** está selecionada para **Utilizar modelo com prefixo**, **Manual** está selecionada para **Internet Key Exchange (IKE)** e **ESP** está selecionada para **Protocolo** em **Segurança encapsulada**. O número de carateres que é possível definir depende da definição selecionada para **Encriptação** na secção **Segurança encapsulada**. Se o comprimento da chave de código especificada for diferente do algoritmo de encriptação selecionado, irá ocorrer um erro. • **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 em “ASCII Code” (Código ASCII), inclua os carateres em aspas duplas (").

Opção	Descrição
SPI	Estes parâmetros servem para identificar a informação de segurança. Normalmente, um host tem múltiplas SAs (associações de segurança) para diversos tipos de comunicação IPsec. Assim, é necessário identificar a SA aplicável quando é recebido um pacote IPsec. O parâmetro SPI, que identifica a SA, é incluído no cabeçalho AH (cabeçalho de autenticação) e no cabeçalho ESP (dados de segurança encapsuladores). Estas definições são necessárias quando estiver selecionado **Persnl** para **Utilizar modelo com prefixo** e quando estiver selecionado **Manual** para **Internet Key Exchange (IKE)**. Introduza os valores **Entrada/Saída**. (3-10 carateres)
Segurança encapsulada	• **Protocolo** Selecione **ESP** ou **AH**. - ESP é um protocolo de comunicação encriptada por IPsec. O ESP encripta a carga útil (conteúdo comunicado) e acrescenta informações adicionais. O pacote IP é composto pelo cabeçalho e pela carga útil encriptada que sucede ao cabeçalho. Além da carga útil encriptada, o pacote IP também inclui informação relativa ao método de encriptação e à chave de encriptação, os dados de autenticação, etc. - O AH é a parte do protocolo IPsec que autentica o remetente e impede a manipulação dos dados (garante que os dados estão completos). No pacote IP, os dados são colocados imediatamente após o cabeçalho. Além disso, os pacotes incluem valores de hash, que são calculados com uma equação a partir dos conteúdos comunicados, da chave secreta e de outros itens, com o objetivo de impedir a falsificação do remetente e a manipulação dos dados. Ao contrário do ESP, os conteúdos comunicados não são encriptados e os dados são enviados e recebidos na forma de 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** estiver selecionado em **Protocolo**. • **Duração de SA** Especificar o tempo de vida da SA do IKE. Introduza o tempo (segundos) e o número de kilobytes (KByte). • **Modo de encapsulamento** Selecione **Transporte** ou **Túnel**. • **Endereço IP do router remoto** Introduza o endereço IP (IPv4 ou IPv6) do router remoto. Introduza esta informação apenas quando o modo **Túnel** estiver selecionado.

Opção	Descrição
	SA (Security Association) é um método de comunicação encriptada por IPsec ou IPv6, que troca e partilha informação, como o método de encriptação e a chave de encriptação, para estabelecer um canal de comunicação segura antes do início da comunicação. O SA também pode aplicar-se a um canal virtual de comunicação encriptada que tenha sido estabelecido. O SA utilizado com o IPsec estabelece o método de encriptação, troca as chaves e efetua a autenticação mútua de acordo com o procedimento standard do IKE (Internet Key Exchange). Além disso, o SA é atualizado periodicamente.

Informações relacionadas

- Configurar um Modelo de IPsec utilizando a Gestão Baseada na Web

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 unauthorized. 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.
Desl.	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 tunneled.

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

Autenticação do utilizador

- Utilizar a autenticação Active Directory
- Utilizar a autenticação por LDAP
- Utilizar o Secure Function Lock 3.0

Utilizar a autenticação Active Directory

- Introdução à autenticação Active Directory
- Configurar a autenticação Active Directory utilizando a Gestão Baseada na Web
- Iniciar sessão para alterar as definições do equipamento através do painel de controlo do equipamento (autenticação Active Directory)

Introdução à autenticação Active Directory

A autenticação Active Directory restringe a utilização do seu equipamento. Se a autenticação Active Directory estiver ativada, o painel de controlo do equipamento está bloqueado. Não é possível alterar as definições do equipamento enquanto não for introduzida uma identificação de utilizador e uma palavra-passe.

A autenticação Active Directory oferece as seguintes funcionalidades:

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

- Guarda os dados de impressão recebidos
- Guarda os dados de fax recebidos
- Obtém o endereço de e-mail a partir do servidor Active Directory com base na sua ID de utilizador quando os dados digitalizados são enviados para um servidor de e-mail.

  Para utilizar esta função, selecione a opção **Lig.** para a definição **Obter endereço de e-mail** e **LDAP + kerberos** ou o método de autenticação **LDAP + NTLMv2**. O seu endereço de e-mail será o remetente quando o equipamento enviar dados digitalizados para um servidor de e-mail, ou será o destinatário se pretender enviar os dados digitalizados para o seu próprio endereço de e-mail.

Quando a autenticação Active Directory estiver ativada, o equipamento guarda todos os faxes recebidos. Após o utilizador iniciar sessão, o equipamento imprime todos os faxes recebidos.

Pode alterar as definições da autenticação Active Directory utilizando a gestão baseada na Web.

Informações relacionadas

- Utilizar a autenticação Active Directory

Configurar a autenticação Active Directory utilizando a Gestão Baseada na Web

A autenticação Active Directory suporta autenticação Kerberos e autenticação NTLMv2. É necessário configurar o protocolo SNTP (servidor de tempo da rede) e um servidor DNS para a autenticação.

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 **Administrador** > **Função de restrição de utilizador** ou **Gestão de restrições**.

   Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ☰.
5. Selecione **Autenticação Active Directory**.
6. Clique em **Submeter**.
7. Clique em **Autenticação Active Directory**.
8. Configure as definições que se seguem:

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

Opção	Descrição
Armazenar dados de receção de fax	Selecione esta opção para guardar os dados de fax recebidos. Pode imprimir todos os dados de fax recebidos após iniciar sessão no equipamento.
Memorizar ID de utilizador	Selecione esta opção para guardar a sua identificação de utilizador.
Endereço do servidor do Active Directory	Introduza o endereço IP ou o nome do servidor (for example: ad.example.com) Active Directory.
Nome de domínio do Active Directory	Introduza o nome de domínio do Active Directory.
Protocolo e método de autenticação	Selecione o protocolo e o método de autenticação.
SSL/TLS	Selecione a opção **SSL/TLS**.
Porta do servidor LDAP	Introduza o número da porta para estabelecer a ligação ao servidor de Active Directory através de LDAP (disponível apenas para o método de autenticação **LDAP + kerberos** ou **LDAP + NTLMv2**).
Raiz de pesquisa do LDAP	Introduza a raiz de procura do LDAP (disponível apenas para o método de autenticação **LDAP + kerberos** ou **LDAP + NTLMv2**).

Opção	Descrição
Obter endereço de e-mail	Selecione esta opção para obter o endereço de correio eletrónico do utilizador com sessão iniciada a partir do servidor Active Directory. (disponível apenas para o método de autenticação **LDAP + kerberos** ou **LDAP + NTLMv2**)
Obter diretório raiz do utilizador	Selecione esta opção para obter o seu diretório inicial e utilizá-lo como destino da função de digitalização para rede. (disponível apenas para o método de autenticação **LDAP + kerberos** ou **LDAP + NTLMv2**)

9. Clique em **Submeter**.

Informações relacionadas

- Utilizar a autenticação Active Directory

Iniciar sessão para alterar as definições do equipamento através do painel de controlo do equipamento (autenticação Active Directory)

Quanto a autenticação Active Directory está ativada, o painel de controlo do equipamento fica bloqueado até que introduza a sua identificação de utilizador e a sua palavra-passe no painel de controlo do equipamento.

1. No painel de controlo do equipamento, introduza a identificação de utilizador e a palavra-passe para iniciar sessão.
2. Quando a autenticação é bem-sucedida, o painel de controlo do equipamento é desbloqueado.

Informações relacionadas

- Utilizar a autenticação Active Directory

Utilizar a autenticação por LDAP

- Introdução à autenticação LDAP
- Configurar a autenticação LDAP utilizando a Gestão Baseada na Web
- Iniciar sessão para alterar as definições do equipamento através do painel de controlo do equipamento (autenticação por LDAP)

Introdução à autenticação LDAP

A autenticação de LDAP restringe a utilização do seu equipamento. Se a autenticação LDAP estiver ativada, o painel de controlo do equipamento é bloqueado. Não é possível alterar as definições do equipamento enquanto não for introduzida uma identificação de utilizador e uma palavra-passe.

A autenticação LDAP oferece as seguintes funcionalidades:

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

- Guarda os dados de impressão recebidos
- Guarda os dados de fax recebidos
- Obtém o endereço de e-mail a partir do servidor LDAP com base no nome de utilizador quando os dados digitalizados são enviados para um servidor de e-mail.

  Para utilizar esta função, selecione a opção **Lig.** para a definição **Obter endereço de e-mail**. O seu endereço de e-mail será o remetente quando o equipamento enviar dados digitalizados para um servidor de e-mail, ou será o destinatário se pretender enviar os dados digitalizados para o seu próprio endereço de e-mail.

Quando a autenticação LDAP estiver ativada, o equipamento guarda todos os faxes recebidos. Após o utilizador iniciar sessão, o equipamento imprime todos os faxes recebidos.

Pode alterar as definições da autenticação LDAP utilizando a gestão baseada na Web.

Informações relacionadas

- Utilizar a autenticação por LDAP

Configurar a autenticação LDAP utilizando a 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. Na barra de navegação do lado esquerdo, clique em **Administrador** > **Função de restrição de utilizador** ou **Gestão de restrições**.

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

5. Selecione **Autenticação LDAP**.
6. Clique em **Submeter**.
7. Clique no menu **Autenticação LDAP**.
8. Configure as definições que se seguem:

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

Opção	Descrição
Armazenar dados de receção de fax	Selecione esta opção para guardar os dados de fax recebidos. Pode imprimir todos os dados de fax recebidos após iniciar sessão no equipamento.
Memorizar ID de utilizador	Selecione esta opção para guardar a sua identificação de utilizador.
Endereço do servidor LDAP	Introduza o endereço IP ou o nome de servidor do servidor LDAP (por exemplo: ldap.exemplo.com).
SSL/TLS	Selecione a opção **SSL/TLS** para utilizar LDAP com SSL/TLS.
Porta do servidor LDAP	Introduza o número da porta do servidor LDAP.
Raiz de pesquisa do LDAP	Introduza o diretório raiz da pesquisa LDAP.
Nome do atributo (Chave de pesquisa)	Introduza o atributo que pretende utilizar como chave de procura.
Obter endereço de e-mail	Selecione esta opção para obter o endereço de correio eletrónico do utilizador com sessão iniciada a partir do servidor LDAP.
Obter diretório raiz do utilizador	Selecione esta opção para obter o seu diretório inicial e utilizá-lo como destino da função de digitalização para rede.

9. Clique em **Submeter**.

Informações relacionadas

- Utilizar a autenticação por LDAP

Iniciar sessão para alterar as definições do equipamento através do painel de controlo do equipamento (autenticação por LDAP)

Quando a Autenticação por LDAP está ativada, o painel de controlo do equipamento fica bloqueado até que seja introduzida uma identificação de utilizador e uma palavra-passe no painel de controlo do equipamento.

1. No painel de controlo do equipamento, introduza a identificação de utilizador e a palavra-passe para iniciar sessão.
2. Quando a autenticação é bem-sucedida, o painel de controlo do equipamento é desbloqueado.

Informações relacionadas

- Utilizar a autenticação por LDAP

Utilizar o Secure Function Lock 3.0

O Secure Function Lock 3.0 (Bloqueio de funções de segurança) aumenta a segurança ao restringir as funções disponíveis no equipamento.

Antes de utilizar o Secure Function Lock 3.0

Utilize o Secure Function Lock (Bloqueio de funções de segurança) para configurar palavras-passe, definir limites de página do utilizador específicos e conceder acesso a algumas ou a todas as funções aqui indicadas.

Pode configurar e alterar as definições seguintes do Secure Function Lock 3.0 (Bloqueio de funções de segurança) utilizando a gestão baseada na Web:

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

- **Imprimir**
- **Copiar**
- **Digitalizar**
- **Fax**
- **Suporte**
- **Web Connect**
- **Aplicações**
- **Limites de página**
- **Contadores de pág.**
- **ID do cartão (ID NFC)**

Modelos de LCD com ecrã tátil:

Quando o Secure Function Lock (Bloqueio de funções de segurança) está ativado, o equipamento entra automaticamente no Modo Público e algumas das suas funções ficam restritas apenas a utilizadores authorized. Para aceder às funções restritas do equipamento, prima , selecione o seu nome de utilizador e introduza a palavra-passe.

Informações relacionadas

- Utilizar o Secure Function Lock 3.0

Configurar o Secure Function Lock 3.0 utilizando a 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. Na barra de navegação do lado esquerdo, clique em **Administrador** > **Função de restrição de utilizador** ou **Gestão de restrições**.

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

5. Selecione **Proteger bloqueio de função**.
6. Clique em **Submeter**.
7. Clique no menu **Funções restritas**.
8. Configure as definições para gerir restrições por utilizador ou por grupo.
9. Clique em **Submeter**.
10. Clique no menu **Lista de utilizadores**.
11. Configure a lista de utilizadores.
12. Clique em **Submeter**.

Além disso, pode alterar as definições de bloqueio da lista de utilizadores no menu **Proteger bloqueio de função**.

Informações relacionadas

- Utilizar o Secure Function Lock 3.0

Digitalizar utilizando o Secure Function Lock 3.0

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

Definir restrições à digitalização (para administradores)

O Secure Function Lock 3.0 (Bloqueio de funções de segurança) permite que o administrador restrinja os utilizadores que podem digitalizar. Quando a função de digitalização está desativada para a definição de utilizador público, apenas os utilizadores que têm a caixa de verificação **Digitalizar** marcada podem digitalizar.

Utilizar a função de digitalização (para utilizadores sob restrições)

- Para digitalizar utilizando o painel de controlo do equipamento:

  Os utilizadores restritos têm de introduzir as respetivas palavras-passe no painel de controlo do equipamento para acederem ao modo de digitalização.
- Para digitalizar a partir de um computador:

  Os utilizadores restritos têm de introduzir as respetivas palavras-passe no painel de controlo do equipamento antes de digitalizarem a partir dos seus computadores. Se a palavra-passe não for introduzida no painel de controlo do equipamento, aparece uma mensagem de erro no computador do utilizador.

Se o equipamento suportar a autenticação com cartão IC, os utilizadores restritos também poderão aceder ao modo de digitalização tocando com os seus cartões IC registados no símbolo NFC do painel de controlo do equipamento.

Informações relacionadas

- Utilizar o Secure Function Lock 3.0

Configurar o Modo Público do Secure Function Lock 3.0

Utilize o ecrã do Secure Function Lock para configurar o Modo Público, que limita as funções disponíveis para os utilizadores públicos. Os utilizadores públicos não precisam de introduzir uma palavra-passe para aceder às funções que ficam disponíveis através das definições do Modo Público.

O Modo Público inclui trabalhos de impressão enviados através de Brother iPrint&Scan e Brother Mobile Connect.

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 **Administrador** > **Função de restrição de utilizador** ou **Gestão de restrições**.

   Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ≡.
5. Selecione **Proteger bloqueio de função**.
6. Clique em **Submeter**.
7. Clique no menu **Funções restritas**.
8. Na linha **Modo público**, selecione uma caixa de verificação para permitir ou desmarque uma caixa de verificação para restringir a função indicada.
9. Clique em **Submeter**.

Informações relacionadas

- Utilizar o Secure Function Lock 3.0

Configurar as definições de ecrã inicial pessoal utilizando a Gestão baseada na Web

Como Administrador, pode especificar os separadores que os utilizadores podem ver nos respetivos ecrãs pessoais. Estes separadores permitem um acesso rápido aos atalhos favorite dos utilizadores, que podem atribuir aos respetivos separadores do ecrã inicial pessoal a partir do painel de controlo do equipamento.

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

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 **Administrador** > **Função de restrição de utilizador** ou **Gestão de restrições**.

   Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ☰.
5. Selecione **Proteger bloqueio de função**.
6. No campo **Definições de separadores**, selecione **Pessoal** para os nomes de separador que pretende utilizar no seu ecrã inicial pessoal.
7. Clique em **Submeter**.
8. Clique no menu **Funções restritas**.
9. Configure as definições para gerir as restrições por utilizador ou grupo.
10. Clique em **Submeter**.
11. Clique no menu **Lista de utilizadores**.
12. Configure a lista de utilizadores.
13. Selecione **Lista de utilizadores/Funções restritas** na lista pendente para cada utilizador.
14. Selecione o nome do separador na lista pendente **Ecrã/Display inicial** para cada utilizador.
15. Clique em **Submeter**.

Informações relacionadas

- Utilizar o Secure Function Lock 3.0

Funções adicionais do Secure Function Lock 3.0

Configure as funções seguintes no ecrã do Secure Function Lock:

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

Repor todos os contadores

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

Exportar para ficheiro CSV

Clique em **Exportar para ficheiro CSV** para exportar o atual e último contador de páginas, incluindo informações sobre o **Lista de utilizadores/Funções restritas** num ficheiro CSV.

ID do cartão (ID NFC)

Clique no menu **Lista de utilizadores** e introduza a identificação de cartão de utilizador no campo **ID do cartão (ID NFC)**. Pode utilizar o seu cartão IC para efetuar a autenticação.

Saída

Quando a unidade de Classificador está instalada no equipamento, pode selecionar a gaveta de saída para cada utilizador na lista pendente.

Último registo do contador

Clique em **Último registo do contador** se pretender que o equipamento retenha a contagem de páginas após a reposição do contador a zero.

Reposição automática do contador

Clique em **Reposição automática do contador** para configurar o intervalo de tempo de que pretende dispor entre cada reposição do contador de páginas. Selecione um intervalo diário, semanal ou mensal.

Informações relacionadas

- Utilizar o Secure Function Lock 3.0

Registar um novo cartão IC utilizando o painel de controlo do equipamento

Pode registar cartões de circuito integrado (cartões IC) no equipamento.

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

1. Toque no símbolo da comunicação de campo próximo (NFC) do painel de controlo do equipamento com um cartão de circuito integrado registado (cartão IC).
2. Prima a sua identificação de utilizador no LCD.
3. Prima o botão de registo de cartões.
4. Toque com um novo cartão IC no símbolo NFC.

   O número do novo cartão IC é então registado no equipamento.
5. Prima o botão OK.

Informações relacionadas

- Utilizar o Secure Function Lock 3.0

Registar um leitor de cartões IC externo

Quando ligar um leitor de cartões IC (circuito integrado) externo, utilize a gestão baseada na Web para registar o leitor de cartões. O equipamento suporta leitores de cartões IC externos suportados pelo controlador de classe HID.

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 **Administrador** > **Leitor de cartões externo**.

   Se a barra de navegação do lado esquerdo não estiver visível, inicie a navegação a partir de ≡.
5. Introduza as informações necessárias e clique em **Submeter**.
6. Reinicie o equipamento Brother para ativar a configuração.
7. Ligue o leitor de cartões ao equipamento.
8. Toque com o cartão no leitor de cartões quando utilizar a autenticação por cartão.

Informações relacionadas

- Utilizar o Secure Function Lock 3.0

Enviar ou receber um e-mail em segurança

- Configurar o envio ou a receção de e-mail utilizando a gestão baseada na Web
- Enviar um e-mail com autenticação do utilizador
- Enviar ou receber uma mensagem de e-mail em segurança utilizando SSL/TLS

Configurar o envio ou a receção de e-mail utilizando a gestão baseada na Web

- A receção de e-mail só está disponível em determinados modelos.
- Recomendamos a utilização da gestão baseada na Web para configurar o envio de correio eletrónico seguro com autenticação do utilizador ou o envio e a receção de correio eletrónico utilizando SSL/TLS (apenas em modelos compatíveis).

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. No campo **POP3/IMAP4/Cliente SMTP**, clique em **Definições avançadas** e certifique-se de que o estado de **POP3/IMAP4/Cliente SMTP** é **Ativado**.

   - Os protocolos disponíveis podem diferir consoante o equipamento.
   - Se aparecer o ecrã de seleção **Método de autenticação**, selecione o método de autenticação e, em seguida, siga as instruções no ecrã.
6. Configure as definições de **POP3/IMAP4/Cliente SMTP**.
   - Verifique se as definições de e-mail estão corretas após a configuração através do envio de um e-mail de teste.
   - Se não conhecer as definições do servidor POP3/IMAP4/SMTP, contacte o administrador da rede ou o fornecedor de serviços de Internet.
7. Quando terminar, clique em **Submeter**.

   Aparece a caixa de diálogo **Testar config. de envio/rec. e-mail**.
8. Siga as instruções da caixa de diálogo para testar as definições atuais.

Informações relacionadas

- Enviar ou receber um e-mail em segurança

Tópicos relacionados:

- Enviar ou receber uma mensagem de e-mail em segurança utilizando SSL/TLS

Enviar um e-mail com autenticação do utilizador

O equipamento envia e-mails através de um servidor de correio eletrónico que exige a autenticação do utilizador. Este método impede que utilizadores unauthorized tenham acesso ao servidor de correio eletrónico.

Pode enviar uma notificação por e-mail, relatórios por e-mail e I-Fax (disponíveis apenas em determinados modelos) utilizando a autenticação do utilizador.

- Os protocolos disponíveis podem diferir consoante o equipamento.
- Recomendamos a utilização da gestão baseada na Web para configurar a autenticação SMTP.

Definições do servidor de correio eletrónico

Tem de configurar o método de autenticação SMTP do equipamento para que corresponda ao método utilizado pelo seu servidor de e-mail. Para obter mais informações sobre as definições do servidor de correio eletrónico, contacte o administrador de rede ou o ISP (Internet Service Provider, fornecedor de serviços de Internet).

Para ativar a autenticação do servidor SMTP utilizando a gestão baseada na Web, selecione o método de autenticação abaixo de **Método de autenticação do servidor** no ecrã **POP3/IMAP4/Cliente SMTP**.

Informações relacionadas

- Enviar ou receber um e-mail em segurança

Enviar ou receber uma mensagem de e-mail em segurança utilizando SSL/TLS

O equipamento suporta os métodos de comunicação SSL/TLS. Para utilizar o servidor de correio eletrónico que está a utilizar a comunicação SSL/TLS, terá de configurar as definições que se seguem.

- A receção de e-mail só está disponível em determinados modelos.
- Recomendamos a utilização da gestão baseada na Web para configurar SSL/TLS.

Verificar certificado do servidor

Em **SSL/TLS**, se selecionar **SSL** ou **TLS**, a caixa de verificação **Verif. Certif. do Servidor** será selecionada automaticamente.

- 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 fornecedor de serviços de Internet para confirmar se é necessário importar um certificado da AC.
- Se não for necessário verificar o certificado do servidor, desmarque a caixa de verificação **Verif. Certif. do Servidor**.

Número da porta

Se selecionar **SSL** ou **TLS**, o valor **Porta** será alterado para corresponder ao protocolo. Para alterar o número da porta manualmente, introduza o número da porta depois de selecionar as definições de **SSL/TLS**.

É necessário configurar o método de comunicação do equipamento para que corresponda ao método utilizado pelo seu servidor de correio eletrónico. Para obter mais informações sobre as definições do servidor de correio eletrónico, contacte o administrador de rede ou o seu ISP.

Na maioria dos casos, os serviços de Webmail seguros exigem as seguintes definições:

As funções, opções e definições suportadas podem diferir em função 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

- Enviar ou receber um e-mail em segurança

Tópicos relacionados:

- Configurar o envio ou a receção de e-mail utilizando a gestão baseada na Web
- Configurar certificados para segurança do equipamento

Guardar o registo de impressão na rede

- Descrição geral do registo de impressão de loja para rede
- Configurar as definições de Guardar Registo de Impressão na Rede utilizando a Gestão Baseada na Web
- Utilizar a definição de deteção de erros da função Guardar Registo de Impressão na Rede
- Utilizar a função Guardar Registo de Impressão na Rede com o Secure Function Lock 3.0

Descrição geral do registo de impressão de loja para rede

A função Guardar Registo de Impressão na Rede permite guardar o ficheiro do registo de impressão do seu equipamento num servidor de rede, utilizando o protocolo CIFS (Common Internet File System). Pode registar a ID, o tipo de trabalho de impressão, o nome do trabalho, o nome de utilizador, a data, a hora e o número de páginas impressas por cada trabalho de impressão. CIFS é o protocolo Common Internet File System que é executado sobre TCP/IP e permite que os computadores de uma rede partilhem ficheiros através de uma intranet ou da Internet.

No registo de impressão, são gravadas as seguintes funções de impressão:

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

- Trabalhos de impressão do seu computador
- Impressão direta USB
- Copiar
- Fax recebido
- Web Connect Print

- A função Guardar Registo de Impressão na Rede suporta a autenticação Kerberos e a autenticação NTLMv2. Tem de configurar o protocolo SNTP (servidor de tempo da rede) ou definir corretamente a data, a hora e o fuso horário no painel de controlo para a autenticação.
- Pode definir o tipo de ficheiro TXT ou CSV quando guardar um ficheiro no servidor.

Informações relacionadas

- Guardar o registo de impressão na rede

Configurar as definições de Guardar Registo de Impressão na Rede utilizando a 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. Na barra de navegação do lado esquerdo, clique em **Administrador** > **Armazenar registo de impressão na rede**.

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

5. No campo **Registo de impressão**, clique em **Lig.**.
6. Configure as definições que se seguem:

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

Opção	Descrição
Caminho da pasta de rede	Introduza a pasta de destino onde o registo de impressão será guardado no servidor CIFS (por exemplo: \\NomeDoComputador\PastaPartilhada).
Nome ficheiro	Introduza o nome de ficheiro que pretende utilizar para o registo de impressão (até 32 caracteres).
Tipo de ficheiro	Selecione a opção **TXT** ou **CSV** para obter o tipo de ficheiro de registo de impressão.
Origem de hora para registo	Selecione a fonte da hora para o registo de impressão.
Autent. Método	Selecione o método de autenticação necessário para aceder ao servidor CIFS: **Auto**, **Kerberos** ou **NTLMv2**. O Kerberos é um protocolo de autenticação que permite que dispositivos ou indivíduos provem com segurança a sua identidade junto dos servidores da rede utilizando um único início de sessão. NTLMv2 é o método de autenticação utilizado pelo Windows para iniciar sessão nos servidores. • **Auto**: Se selecionar **Auto**, será utilizado NTLMv2 no método de autenticação. • **Kerberos**: selecione a opção **Kerberos** para utilizar apenas a autenticação Kerberos. • **NTLMv2**: selecione a opção **NTLMv2** para utilizar apenas a autenticação NTLMv2. • Para a autenticação **Kerberos** e **NTLMv2**, também é necessário configurar as definições de **Data e hora** ou o protocolo SNTP (servidor de tempo da rede) e um servidor DNS. • Pode também configurar as definições de data e hora através do painel de controlo do equipamento.

Opção	Descrição
Nome do utiliz.	Introduza o nome de utilizador para a autenticação (até 96 caracteres). Se o nome de utilizador pertencer a um domínio, introduza o nome de utilizador de acordo com um dos seguintes estilos: user@domain ou domain\user.
Palavra-passe/ Senha	Introduza a palavra-passe para a autenticação (até 32 caracteres).
Endereço do servidor Kerberos (se necessário)	Introduza o endereço do anfitrião (por exemplo: kerberos.exemplo.com; até 64 caracteres) ou o endereço IP (por exemplo: 192.168.56.189) do Centro de Distribuição de Chaves (KDC).
Definição de deteção de erro	Selecione a ação a executar quando não for possível guardar o registo de impressão no servidor devido a um erro de rede.

7. No campo **Estado da ligação**, confirme o estado do último registo.

Também pode confirmar o estado de erro no LCD do equipamento.

8. Clique em **Submeter** para ver a página **Testar o registo de impressão na rede**.

   Para testar as suas definições, clique em **Sim** e avance para o passo seguinte.

   Para não fazer o teste, clique em **Não**. As suas definições serão submetidas automaticamente.
9. O equipamento testará as suas definições.
10. Se as suas definições forem aceites, aparece **Teste OK** no ecrã.

    Se aparecer **Erro no teste**, verifique todas as definições e clique em **Submeter** para ver a página de teste novamente.

Informações relacionadas

- Guardar o registo de impressão na rede

Utilizar a definição de deteção de erros da função Guardar Registo de Impressão na Rede

Utilize as definições de Deteção de Erros para determinar a ação a executar quando não for possível guardar o registo de impressão no servidor devido a um erro de rede.

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 **Administrador** > **Armazenar registo de impressão na rede**.

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

5. Na secção **Definição de deteção de erro**, selecione a opção **Cancelar impressão** ou **Ignorar registo e impressão**.

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

Opção	Descrição
Cancelar impressão	Se selecionar a opção **Cancelar impressão**, os trabalhos de impressão são canceled quando não for possível guardar o registo de impressão no servidor. Mesmo que selecione a opção **Cancelar impressão**, o equipamento imprime os faxes recebidos.

Ignorar registo e impressão	Se selecionar a opção **Ignorar registo e impressão**, o equipamento imprime o documento mesmo quando não for possível guardar o registo de impressão no servidor.
	
	Quando a função de gravação do registo de impressão já estiver disponível, o registo de impressão é 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 não for possível guardar o registo de impressão no final da impressão, o número de páginas impressas não será registado.
	b. Se não for possível guardar o registo no início nem no final da impressão, o registo de impressão do trabalho não será gravado. Quando a função voltar a estar disponível, o registo de impressão indicará a ocorrência do erro.

6. Clique em **Submeter** para ver a página **Testar o registo de impressão na rede**.

Para testar as suas definições, clique em **Sim** e avance para o passo seguinte.

Para não fazer o teste, clique em **Não**. As suas definições serão submetidas automaticamente.

7. O equipamento testará as suas definições.
8. Se as suas definições forem aceites, aparece **Teste OK** no ecrã.

   Se aparecer **Erro no teste**, verifique todas as definições e clique em **Submeter** para ver a página de teste novamente.

Informações relacionadas

- Guardar o registo de impressão na rede

Utilizar a função Guardar Registo de Impressão na Rede com o Secure Function Lock 3.0

Se o Secure Function Lock 3.0 (Bloqueio de funções de segurança) estiver ativo, os nomes dos utilizadores registados para as funções de cópia, receção de fax, impressão Web Connect e impressão direta de USB são registados no relatório Guardar registo de impressão na rede. Se a autenticação Active Directory estiver ativada, o nome de utilizador é registado no relatório da função Guardar registo de impressão na rede:

As funções, opções e definições suportadas podem diferir em função 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

- Guardar o registo de impressão na rede

brother

Brother Earth

www.brotherearth.com

POR
Versão 0