

Guia de SSL

(Secure Socket Layer)



Para encontrar informação básica sobre redes e funções de rede avançadas do equipamento Brother: >> Manual do Utilizador de Rede.

Para transferir o manual mais recente, visite o Brother Solutions Center em (<http://solutions.brother.com/>). Pode também transferir os controladores e utilitários mais recentes para a máquina, ler as secções de FAQ e sugestões para a resolução de problemas ou informar-se sobre soluções de impressão especiais através do Brother Solutions Center.

Nem todos os modelos estão disponíveis em todos os países.

Modelos aplicáveis

Este Manual do Utilizador aplica-se aos modelos seguintes.

HL-5450DN(T)/5470DW(T)/6180DW(T)

DCP-8110DN/8150DN/8155DN/8250DN/MFC-8510DN/8710DW/8910DW/8950DW(T)

Definições de notas

Ao longo do Manual do Utilizador, são utilizados os seguintes ícones:

 Nota	Notas sobre como enfrentar situações que possam surgir ou sugestões sobre o funcionamento da operação com outras funcionalidades.
----------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------

Marcas comerciais

O logótipo da Brother é uma marca comercial registada da Brother Industries, Ltd.

Microsoft, Windows, Windows Server e Internet Explorer são marcas comerciais registadas ou apenas marcas comerciais da Microsoft Corporation nos EUA e/ou noutros países.

Windows Vista é uma marca comercial registada ou apenas uma marca comercial da Microsoft Corporation nos EUA e/ou noutros países.

Todas as empresas cujo software é mencionado neste manual possuem um Contrato de Licença de Software específico para os seus programas.

Todos os nomes comerciais e nomes de produtos pertencentes a outras empresas e que apareçam nos produtos da Brother, nos respectivos documentos e noutros materiais, são marcas comerciais ou marcas comerciais registadas das respectivas empresas.

IMPORTANTE

- A utilização deste produto só está aprovada no país onde foi efectuada a aquisição. Não utilize este produto fora do país onde o adquiriu, pois pode violar os regulamentos relativos a telecomunicações sem fios e a potência eléctrica no país em questão.
- Neste manual, os ecrãs são os do modelo MFC-8950DW(T) excepto se especificado outro.
- Neste documento, Windows® XP representa o Windows® XP Professional, Windows® XP Professional x64 Edition e Windows® XP Home Edition.
- Neste documento, Windows Server® 2003 representa o Windows Server® 2003 e Windows Server® 2003 x64 Edition.
- Neste documento, Windows Server® 2008 representa o Windows Server® 2008 e Windows Server® 2008 R2.
- No presente documento, Windows Vista® representa todas as edições do Windows Vista®.
- No presente documento, Windows® 7 representa todas as edições do Windows® 7.
- Visite o Brother Solutions Center em <http://solutions.brother.com/> e clique em Manuais na página do modelo para transferir os outros manuais.

Índice

1	Introdução	1
	Descrição geral.....	1
	Breve história do SSL.....	1
	Benefícios do SSL.....	1
	Utilizar certificados para a segurança de dispositivos.....	2
2	Certificado Digital para comunicação SSL	4
	Instalação do Certificado Digital.....	4
	Criar um certificado auto-assinado.....	6
	Criar um CSR (Certificate Signing Request).....	7
	Como instalar o certificado na máquina.....	9
	Escolher o certificado.....	10
	Instalar o certificado auto-assinado ou pré-instalado em Windows Vista®, Windows® 7 e Windows Server® 2008 para utilizadores que tenham direitos de administrador.....	12
	Instalar o certificado auto-assinado ou pré-instalado para utilizadores de Windows® XP e Windows Server® 2003.....	14
	Importar e exportar o certificado e a chave privada.....	17
	Como importar o certificado auto-assinado, o certificado emitido por uma CA e a chave privada...	17
	Como exportar o certificado auto-assinado, o certificado emitido por uma CA e a chave privada...	17
	Importar e exportar um certificado CA.....	18
	Gerir vários certificados.....	19
3	Gerir a máquina de rede de modo seguro utilizado SSL/TLS	20
	Gestão segura utilizando a gestão baseada na web (web browser).....	20
4	Imprimir documentos em segurança com SSL	21
	Imprimir documentos em segurança com IPPS para Windows®.....	21
	Windows® XP e Windows Server® 2003.....	21
	Windows Vista®, Windows® 7 e Windows Server® 2008.....	23
5	Enviar ou receber (nos modelos DCP e MFC) um e-mail com segurança	25
	Configuração utilizando a gestão baseada na web (browser web).....	25
	Enviar ou receber (nos modelos DCP e MFC) um e-mail com segurança utilizando SSL/TLS.....	26
6	Resolução de problemas	27
	Descrição geral.....	27
	Identificar o problema.....	27
	Imprimir a Página de Definições da Impressora (para o modelo HL-5450DN(T)).....	29
	Imprimir o Relatório da Configuração de Rede (em outros modelos).....	29
	Termos e conceitos de redes.....	31
	Descrição técnica do SSL.....	31
	Termos de redes.....	32

Descrição geral

Secure Socket Layer (SSL) é um método eficaz para proteger os dados que são transmitidos em redes locais e não locais. A protecção é conseguida com encriptação dos dados transmitidos, por exemplo um trabalho de impressão, pelo que alguém que tente capturá-lo não conseguirá lê-lo porque os dados estão encriptados.

Pode ser configurado tanto em redes com fios como em redes sem fios e funciona em conjunto com outros métodos de segurança, como as chaves WPA e as firewalls.

Breve história do SSL

O SSL foi criado inicialmente com o objectivo de proteger informação em trânsito na web, especialmente os dados transmitidos entre browsers e servidores da web. Por exemplo, quando utiliza o Internet Explorer® para aceder ao seu banco pela Internet e vê https:// e o pequeno cadeado no web browser, isso significa que está a utilizar SSL. Posteriormente, o sistema foi alargado a outras aplicações como Telnet, impressoras e software de FTP para se tornar uma solução universal para segurança online. As intenções da concepção original ainda são utilizadas por muitos retalhistas e bancos online para proteger dados delicados, como números de cartão de crédito, registos de clientes, etc.

O SSL utiliza níveis extremamente elevados de encriptação e merece a confiança de bancos de todo o mundo pela baixa probabilidade de violação.

Benefícios do SSL

O único benefício de utilizar SSL nos equipamentos Brother é dar segurança à impressão numa rede IP, impedindo que utilizadores não autorizados possam ler os dados que são enviados para o equipamento. O seu principal argumento de venda é o facto de poder ser utilizado para imprimir dados confidenciais com segurança. Por exemplo, um departamento de RH de uma grande empresa pode imprimir recibos de vencimento com frequência. Sem a encriptação, os dados desses recibos de vencimento poderiam ser lidos por outros utilizadores da rede. Mas com o SSL, qualquer pessoa que tente capturar os dados verá apenas uma página de código confuso e não o recibo de vencimento real.

Utilizar certificados para a segurança de dispositivos

A sua máquina Brother suporta a utilização de vários certificados de segurança, o que permite uma gestão, autenticação e comunicação seguras com a máquina. Com a máquina, podem ser utilizadas as funcionalidades de certificado de segurança seguintes. Para imprimir um documento ou utilizar a Gestão baseada na web (web browser) com segurança através de SSL, tem de instalar o certificado no seu computador. Consulte *Instalação do Certificado Digital* >> página 4.

- Comunicação SSL/TLS
- Comunicação SSL para SMTP/POP3

A máquina Brother suporta os certificados seguintes.

- Certificado pré-instalado

O equipamento tem um certificado auto-assinado pré-instalado.

Ao utilizar este certificado, pode utilizar facilmente a comunicação SSL/TLS sem criar ou instalar um certificado. Se pretender utilizar a função Google Cloud Print do equipamento, pode utilizar este certificado pré-instalado para configurar as definições do Google Cloud Print com segurança. Para obter mais informação sobre o Google Cloud Print, visite o Brother Solutions Center em <http://solutions.brother.com/> e clique na ligação Manuais da página do seu modelo para transferir o Guia de Instalação do "Google Cloud Print".



Nota

O certificado auto-assinado pré-instalado não consegue proteger as suas comunicações contra spoofing. Recomendamos que utilize um certificado que seja emitido por uma organização de confiança para obter mais segurança.

- Certificado auto-assinado

Este servidor de impressão emite o seu próprio certificado. Ao utilizar este certificado, pode utilizar facilmente a comunicação SSL/TLS sem ter um certificado de uma CA. (Consulte *Criar um certificado auto-assinado* >> página 6.)

- Certificado de uma CA

Existem dois métodos para instalar um certificado de uma CA. Se já tem um certificado de uma CA ou se pretender utilizar um certificado de uma CA externa de confiança:

- Quando utilizar um CSR (Certificate Signing Request - Pedido de Assinatura de Certificado) a partir deste servidor de impressão. (Consulte *Criar um CSR (Certificate Signing Request)* >> página 7.)
- Quando importar um certificado e uma chave privada. (Consulte *Importar e exportar o certificado e a chave privada* >> página 17.)

■ Certificado CA

Se utilizar um certificado CA que identifique a própria CA (autoridade de certificados), tem de importar o certificado CA a partir da própria CA antes de efectuar a configuração. (Consulte *Importar e exportar um certificado CA* >> página 18.)



Nota

- Se for utilizar a comunicação SSL/TLS, recomendamos que primeiro contacte o administrador do sistema.
 - Se repuser as predefinições de fábrica do servidor de impressão, o certificado e a chave privada instalados serão eliminados. Se quiser manter o mesmo certificado e a chave privada depois de reiniciar o servidor de impressão, exporte-os antes de reiniciar e reinstale-os mais tarde. (Consulte *Como importar o certificado auto-assinado, o certificado emitido por uma CA e a chave privada* >> página 17.)
-

Instalação do Certificado Digital

A impressão através de uma rede segura e a gestão segura através da Gestão baseada na web (web browser) requerem a instalação de um certificado digital tanto no equipamento como no dispositivo que envia os dados para o equipamento, por exemplo um computador. O equipamento tem um certificado pré-instalado. Para configurar o certificado, o utilizador tem de aceder remotamente ao equipamento através de um web browser utilizando o respectivo endereço IP.



Nota

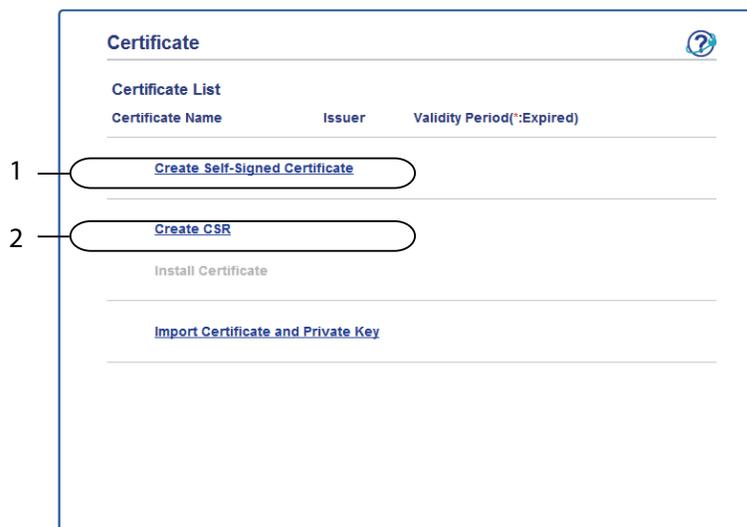
Recomendamos o Windows® Internet Explorer® 7.0/8.0 ou o Firefox® 3.6 para Windows® e o Safari 4.0/5.0 para Macintosh. Certifique-se de que activa as opções de JavaScript e Cookies em qualquer um dos browsers utilizados. Se utilizar um browser diferente, certifique-se de que é compatível com HTTP 1.0 e HTTP 1.1.

- 1 Abra o seu web browser.
- 2 Escreva “http://endereço IP do equipamento/” na barra de endereço do seu browser (em que “endereço IP do equipamento” é o endereço IP do equipamento ou o nome do servidor de impressão).
 - Por exemplo: http://192.168.1.2/
- 3 Por predefinição, não é necessária nenhuma palavra-passe. Se tiver definido uma palavra-passe anteriormente, introduza-a e prima .
- 4 Clique em **Network** (Rede).
- 5 Clique em **Security** (Segurança).
- 6 Clique em **Certificate** (Certificado).

7 Pode configurar as definições do certificado.

Para criar um certificado auto-assinado utilizando a Gestão baseada na web, vá para *Criar um certificado auto-assinado* >> página 6.

Para criar um CSR (Certificate Signing Request - pedido de assinatura de certificado), vá para *Criar um CSR (Certificate Signing Request)* >> página 7.



1 Como criar e instalar um certificado auto-assinado

2 Para utilizar um certificado de uma Autoridade de Certificados (CA)



Nota

- As funções que aparecem a cinzento e sem ligação indicam que não estão disponíveis.
- Para obter mais informações sobre a configuração, consulte a ajuda da gestão baseada na web.

Criar um certificado auto-assinado

- 1 Clique em **Create Self-Signed Certificate** (Criar certificado auto-assinado).
- 2 Introduza um **Common Name** (Nome comum) e uma **Valid Date** (Data válida).



Nota

- O comprimento de **Common Name** (Nome comum) tem de ser inferior a 64 caracteres. Introduza um identificador, como um endereço IP, nome do nó ou nome do domínio, a utilizar quando aceder a esta máquina através da comunicação SSL/TLS. Por predefinição, é apresentado o nome do nó.
 - Aparecerá um aviso se utilizar o protocolo IPPS ou HTTPS e introduzir no URL um nome diferente do **Common Name** (Nome comum) que foi utilizado para o certificado auto-assinado.
-
- 3 Pode seleccionar as definições **Public Key Algorithm** (Algoritmo de chave pública) e **Digest Algorithm** (Algoritmo de resumo) na lista pendente. As configurações predefinidas são **RSA(2048bit)** (RSA (2048 bits)) para **Public Key Algorithm** (Algoritmo de chave pública) e **SHA256** para **Digest Algorithm** (Algoritmo de resumo).
 - 4 Clique em **Submit** (Submeter).
 - 5 O certificado auto-assinado foi criado e guardado na memória do equipamento com sucesso.

Criar um CSR (Certificate Signing Request)

Um CSR (pedido de assinatura de certificado) é um pedido que é enviado a uma CA para autenticação das credenciais contidas no certificado.



Nota

Recomendamos que o certificado raiz da CA seja instalado no computador antes de criar o CSR.

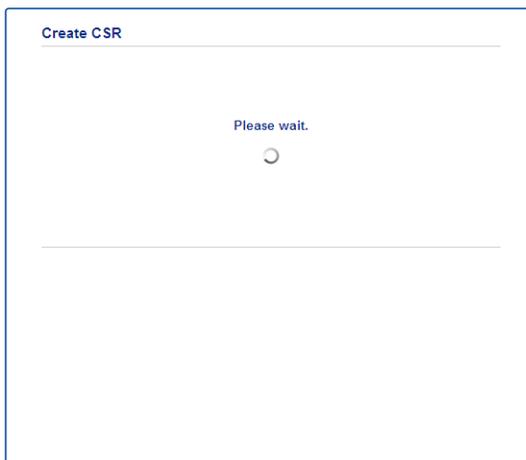
- 1 Clique em **Create CSR** (Criar CSR).
- 2 Introduza um **Common Name** (Nome comum) e os seus dados, como **Organization** (Organização). Terá de indicar os dados da sua empresa para que a CA possa confirmar a sua identidade e atestá-la perante o mundo.



Nota

- O comprimento de **Common Name** (Nome comum) tem de ser inferior a 64 caracteres. Introduza um identificador, como um endereço IP, nome do nó ou nome do domínio, a utilizar quando aceder a esta máquina através da comunicação SSL/TLS. Por predefinição, é apresentado o nome do nó. O **Common Name** (Nome comum) é necessário.
- Aparecerá um aviso se introduzir no URL um nome diferente do nome comum que foi utilizado para o certificado.
- O comprimento de **Organization** (Organização), de **Organization Unit** (Unidade da organização), de **City/Locality** (Cidade/Localidade) e de **State/Province** (Estado/Província) tem de ser inferior a 64 caracteres.
- O **Country/Region** (País/Região) deve ser um código de país ISO 3166 composto por dois caracteres.
- Se estiver a configurar uma extensão de certificado X.509v3, seleccione a caixa de verificação **Configure extended partition** (Configurar partição aumentada) e, em seguida, seleccione **Auto (Register IPv4)** (Auto (Registar IPv4)) ou **Manual**.

- 3 Pode seleccionar as definições **Public Key Algorithm** (Algoritmo de chave pública) e **Digest Algorithm** (Algoritmo de resumo) na lista pendente. As configurações predefinidas são **RSA(2048bit)** (RSA (2048 bits)) para **Public Key Algorithm** (Algoritmo de chave pública) e **SHA256** para **Digest Algorithm** (Algoritmo de resumo).
- 4 Clique em **Submit** (Submeter). Aparecerá o seguinte ecrã.



- 5 Após um momento, ser-lhe-á apresentado o certificado, que pode ser guardado num ficheiro pequeno ou copiado e colado directamente num formulário de CSR que a Autoridade de Certificados disponibiliza. Clique em **Save** (Guardar) para guardar o ficheiro CSR no seu computador.



Nota

Siga a política da sua CA em relação ao método de envio de um CSR para a CA.

- 6 O CSR é criado. Para saber como instalar o certificado no seu equipamento, vá para *Como instalar o certificado na máquina* >> página 9.

Como instalar o certificado na máquina

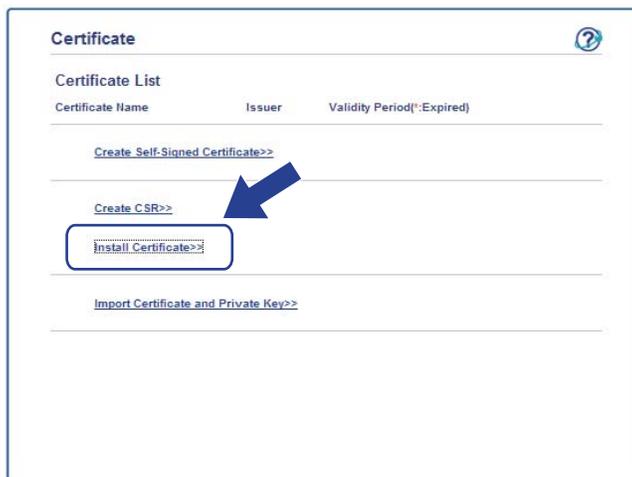
Quando receber o certificado de uma CA, execute os passos seguintes para o instalar no servidor de impressão.



Nota

Só é possível instalar um certificado emitido com o CSR desta máquina. Quando pretender criar outro CSR, verifique se o certificado está instalado antes de criar outro CSR. Crie outro CSR depois de instalar o certificado na máquina. Caso contrário, o CSR que criou antes da instalação será inválido.

- 1 Clique em **Install Certificate** (Instalar certificado) na página **Certificate** (Certificado).

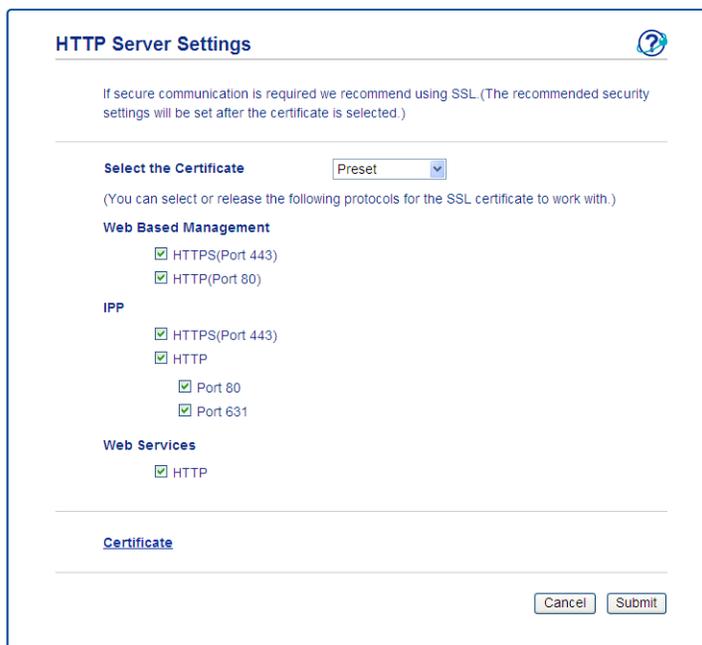


- 2 Especifique o ficheiro do certificado que foi emitido por uma CA e, em seguida, clique em **Submit** (Submeter).
- 3 Neste momento, o certificado foi criado e guardado na memória do seu equipamento com sucesso. Para utilizar a comunicação SSL/TLS, é necessário instalar o certificado raiz da CA no computador. Para obter informações sobre a instalação, contacte o administrador da rede. Concluiu a configuração do certificado digital. Se pretender enviar ou receber um e-mail utilizando SSL, consulte *Enviar ou receber (nos modelos DCP e MFC) um e-mail com segurança* >> página 25 para ver os passos de configuração necessários.

Escolher o certificado

Após instalar o certificado, siga estes passos para escolher o certificado que pretende utilizar.

- 1 Clique em **Network** (Rede).
- 2 Clique em **Protocol** (Protocolo).
- 3 Clique em **HTTP Server Settings** (Definições do servidor HTTP) e escolha o certificado na lista pendente **Select the Certificate** (Seleccione o certificado).



The screenshot shows the 'HTTP Server Settings' configuration window. At the top, there is a title bar with a help icon. Below the title, a message states: 'If secure communication is required we recommend using SSL. (The recommended security settings will be set after the certificate is selected.)'. A section titled 'Select the Certificate' contains a dropdown menu currently set to 'Preset'. Below this, a note says '(You can select or release the following protocols for the SSL certificate to work with.)'. The window is divided into three sections: 'Web Based Management' with checkboxes for 'HTTPS(Port 443)' and 'HTTP(Port 80)'; 'IPP' with checkboxes for 'HTTPS(Port 443)', 'HTTP', 'Port 80', and 'Port 631'; and 'Web Services' with a checkbox for 'HTTP'. At the bottom, there is a 'Certificate' section with a blank area and 'Cancel' and 'Submit' buttons.



Nota

- Se aparecer a seguinte caixa de diálogo, a Brother recomenda que desactive os protocolos Telnet, FTP e TFTP, bem como a gestão através da rede se utilizar uma versão antiga do BRAdmin Professional (2.8 ou inferior) para garantir uma comunicação segura. Se os activar, a autenticação de utilizadores não será segura.

Protocol(Low security)

It is recommended to disable the protocols for high security communication.
To disable the protocol, uncheck the protocol.

Telnet
 FTP(Including Scan to FTP)
 TFTP

BRAdmin uses SNMP.
When SNMP is used, it is designed to use "SNMPv3 read-write access" for high security.
If you do not use, uncheck the protocol.

SNMP

Cancel Submit

- Para modelos DCP e MFC:
Se desactivar o protocolo FTP, a função Digitalizar para FTP será desactivada.

- 4 Clique em **Submit** (Submeter).

Instalar o certificado auto-assinado ou pré-instalado em Windows Vista®, Windows® 7 e Windows Server® 2008 para utilizadores que tenham direitos de administrador

Nota

- Os passos seguintes destinam-se ao Windows® Internet Explorer®. Se utilizar outro web browser, siga a ajuda do próprio web browser.
- É necessário que tenha direitos de administrador para instalar o certificado auto-assinado ou pré-instalado.

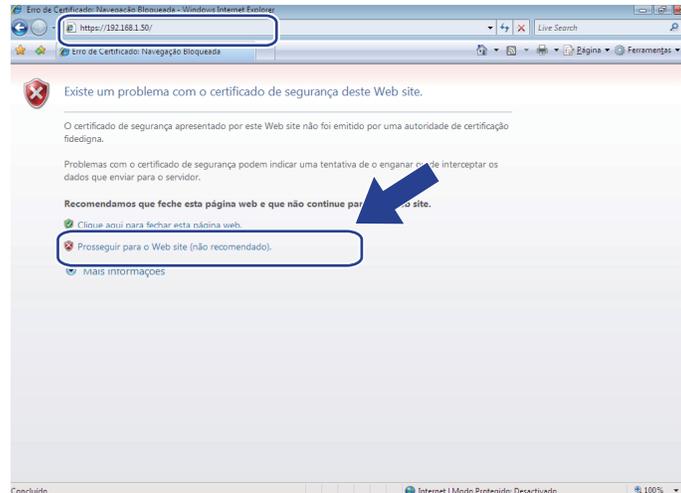
- 1 Clique no botão  e em **Todos os programas**.
- 2 Clique com o botão direito do rato em **Internet Explorer** e depois clique em **Executar como administrador**.



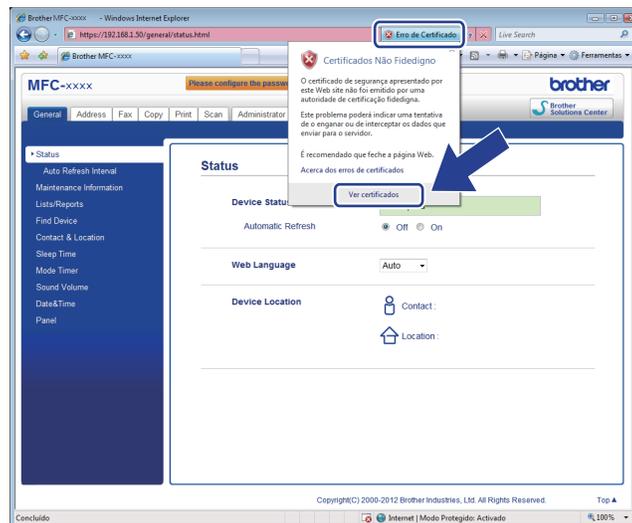
Nota

Se o ecrã **Controlo de Conta de Utilizador** aparecer,
(Windows Vista®) Clique em **Continuar (Permitir)**.
(Windows® 7) Clique em **Sim**.

- 3 Escreva “https://endereço IP da máquina/” no browser para aceder ao seu equipamento (em que “endereço IP da máquina” corresponde ao endereço IP ou ao nome do nó da máquina, que atribuiu ao certificado).
Em seguida, clique em **Prosseguir para o Web site (não recomendado)..**



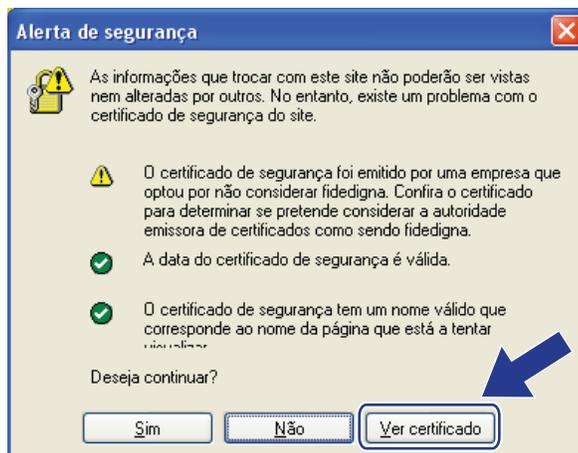
- 4 Clique em **Erro de Certificado** e em **Ver certificados**. Em relação às instruções restantes, execute os passos a partir do passo 4 na *Instalar o certificado auto-assinado ou pré-instalado para utilizadores de Windows® XP e Windows Server® 2003* >> página 14.



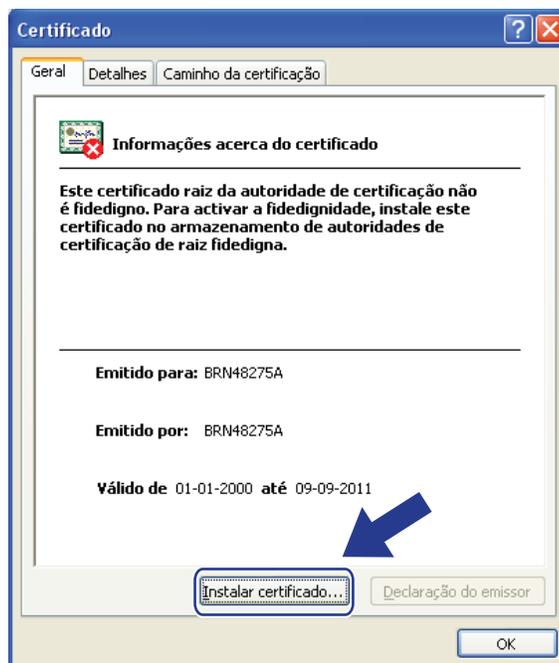
Instalar o certificado auto-assinado ou pré-instalado para utilizadores de Windows® XP e Windows Server® 2003

2

- 1 Abra o seu web browser.
- 2 Escreva “https://endereço IP da máquina/” no browser para aceder ao seu equipamento (em que “endereço IP da máquina” corresponde ao endereço IP ou ao nome do nó da máquina, que atribuiu ao certificado).
- 3 Quando surgir a caixa de diálogo de aviso de segurança, efectue uma destas acções:
 - Clique em **Prosseguir para o Web site (não recomendado)**.. Clique em **Erro de Certificado** e em **Ver certificados**.
 - Se aparecer a caixa de diálogo seguinte, clique em **Ver certificado**.



- 4 Clique em **Instalar certificado...** no separador **Geral**.



5 Quando aparecer **Assistente para importar certificados**, clique em **Seguinte**.



6 Tem de especificar uma localização para instalar o certificado. Recomendamos que escolha **Colocar todos os certificados no seguinte arquivo** e depois clique em **Procurar...**



7 Seleccione **Autoridades de certificação de raiz fidedigna** e clique em **OK**.



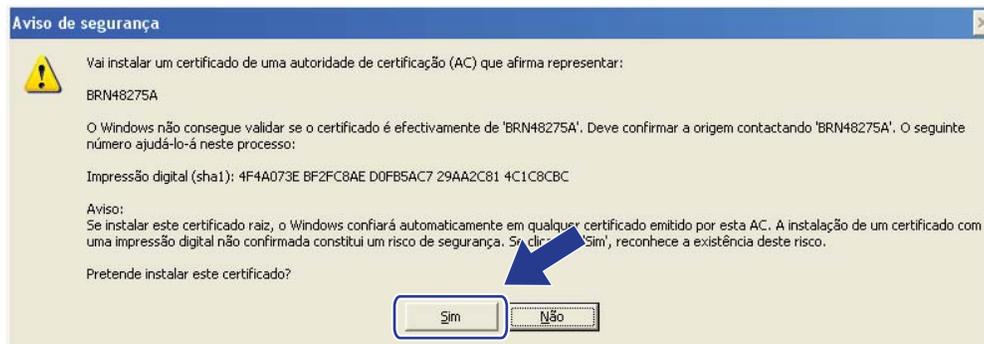
8 Clique em **Seguinte**.



9 No ecrã seguinte, clique em **Concluir**.

10 De seguida, ser-lhe-á pedido que instale o certificado. Efectue uma das seguintes operações:

- Se estiver a instalar o certificado auto-assinado, confirme a impressão digital (polegar) e clique em **Sim**.
- Se estiver a instalar o certificado pré-instalado, clique em **Sim**.



Nota

- No caso do certificado auto-assinado, a impressão digital (polegar) é impressa no Relatório da Configuração de Rede.

Para saber como imprimir o Relatório da Configuração de Rede, consulte *Imprimir a Página de Definições da Impressora (para o modelo HL-5450DN(T))* >> página 29 *Imprimir o Relatório da Configuração de Rede (em outros modelos)* >> página 29.

- No caso do certificado pré-instalado, a impressão digital não é impressa no Relatório da Configuração de Rede.

- 11 Clique em **OK**.
- 12 O certificado auto-assinado ou o certificado pré-instalado está agora instalado no computador e a comunicação SSL/TLS está disponível.

É necessário executar estas operações em cada computador que queira utilizar para imprimir. Mas, uma vez instalado o certificado, não voltará a ser necessário repetir estes passos, excepto se o certificado for alterado.

Importar e exportar o certificado e a chave privada

Pode guardar o certificado e a chave privada na máquina e geri-los através de importação e exportação.

Como importar o certificado auto-assinado, o certificado emitido por uma CA e a chave privada

- 1 Clique em **Import Certificate and Private Key** (Importar certificado e chave privada) na página **Certificate** (Certificado).
- 2 Especifique o ficheiro que pretende importar.
- 3 Introduza a palavra-passe se o ficheiro estiver encriptado e clique em **Submit** (Submeter).
- 4 O certificado e a chave privada foram importados para a máquina com sucesso.

Como exportar o certificado auto-assinado, o certificado emitido por uma CA e a chave privada

- 1 Clique em **Export** (Exportar) apresentado com **Certificate List** (Lista de certificados) na página **Certificate** (Certificado).
- 2 Introduza uma palavra-passe se quiser encriptar o ficheiro.



Nota

Se utilizar uma palavra-passe em branco, a saída não é encriptada.

- 3 Volte a introduzir a palavra-passe para confirmar e clique em **Submit** (Submeter).
- 4 Especifique a localização onde pretende guardar o ficheiro.
- 5 O certificado e a chave privada foram exportados para o computador.

Importar e exportar um certificado CA

Pode guardar um certificado CA na máquina através de importação e exportação.

Como importar um certificado CA

- 1 Clique em **CA Certificate** (Certificado CA) na página **Security** (Segurança).
- 2 Clique em **Import CA Certificate** (Importar certificado CA) e escolha o certificado. Clique em **Submit** (Submeter).

Como exportar um certificado CA

- 1 Clique em **CA Certificate** (Certificado CA) na página **Security** (Segurança).
- 2 Seleccione o certificado que pretende exportar e clique em **Export** (Exportar). Clique em **Submit** (Submeter).
- 3 Clique em **Save** (Guardar) e escolha a pasta destino.
- 4 Escolha o destino onde pretende guardar o certificado exportado e guarde o certificado.

Gerir vários certificados

A função de gestão de vários certificados permite gerir cada um dos certificados instalados utilizando a Gestão baseada na web. Após a instalação dos certificados, pode ver os certificados instalados na página **Certificate** (Certificado) e visualizar o seu conteúdo, apagar ou exportar o certificado. Para obter mais informações sobre como aceder à página **Certificate** (Certificado), consulte *Instalação do Certificado Digital* >> página 4.

■ Para modelos de impressora

O equipamento Brother permite guardar até três certificados auto-assinados ou até três certificados emitidos por uma CA. Os certificados guardados podem ser utilizados no protocolo HTTPS/IPPS ou na autenticação IEEE 802.1x.

■ Para modelos DCP e MFC

O equipamento Brother permite guardar até quatro certificados auto-assinados ou até quatro certificados emitidos por uma CA. Os certificados guardados podem ser utilizados no protocolo HTTPS/IPPS, na autenticação IEEE 802.1x ou em PDF Assinado.

Também pode guardar até quatro certificados CA para utilizar a autenticação IEEE 802.1x e SSL para SMTP/POP3.

Recomendamos que guarde menos um certificado e que mantenha o último livre para lidar com a expiração dos certificados. Por exemplo, se pretender guardar um certificado CA, guarde três certificados e deixe um espaço de armazenamento de reserva. No caso de nova emissão do certificado, por exemplo, quando este expirar, pode importar um novo certificado para o espaço de reserva e apagar o certificado expirado para evitar falhas de configuração.



Nota

- Quando utilizar o protocolo HTTPS/IPPS, IEEE 802.1x ou PDF Assinado (no caso dos modelos DCP e MFC), tem de seleccionar o certificado que está a utilizar.
- Quando utilizar SSL para comunicações SMTP/POP3 (para os modelos DCP e MFC), não é necessário escolher o certificado. O certificado necessário será escolhido automaticamente.

Para gerir de forma segura a sua máquina de rede, tem de utilizar os utilitários de gestão com protocolos de segurança.

Gestão segura utilizando a gestão baseada na web (web browser)

Recomendamos que utilize o protocolo HTTPS para uma gestão segura. Para utilizar estes protocolo, são necessárias as seguintes definições da máquina.



Nota

- Por predefinição, o protocolo HTTPS está ativado.
Pode alterar as definições do protocolo HTTPS e o certificado a utilizar no ecrã da Gestão baseada na Web clicando em **Network** (Rede), **Protocol** (Protocolo) e **HTTP Server Settings** (Definições do servidor HTTP).
- Também é necessário instalar no computador o certificado que instalou no equipamento. Consulte *Instalar o certificado auto-assinado ou pré-instalado em Windows Vista[®], Windows[®] 7 e Windows Server[®] 2008 para utilizadores que tenham direitos de administrador* >> página 12 ou *Instalar o certificado auto-assinado ou pré-instalado para utilizadores de Windows[®] XP e Windows Server[®] 2003* >> página 14.

- 1 Abra o seu web browser.
- 2 Digite “https://endereço IP do equipamento/” no seu browser. (Se utilizar o certificado que criou, digite “https://nome comum/” no seu browser. “nome comum” é o nome comum que atribuiu ao certificado, como um endereço IP, nome do nó ou nome do domínio. Para saber como atribuir um nome comum ao certificado, consulte *Utilizar certificados para a segurança de dispositivos* >> página 2.)
 - Por exemplo:
https://192.168.1.2/ (se o nome comum for o endereço IP da máquina)
- 3 Por predefinição, não é necessária nenhuma palavra-passe. Introduza uma palavra-passe, se tiver definido uma, e prima

Imprimir documentos em segurança com IPPS para Windows[®]

Recomendamos que utilize o protocolo IPPS para uma gestão segura. Para utilizar o protocolo IPPS, são necessárias as seguintes definições da máquina.



Nota

- A comunicação através de IPPS não consegue impedir o acesso não autorizado ao servidor de impressão.
- Também é necessário instalar no computador o certificado que instalou no equipamento. Consulte *Instalar o certificado auto-assinado ou pré-instalado em Windows Vista[®], Windows[®] 7 e Windows Server[®] 2008 para utilizadores que tenham direitos de administrador* >> página 12 ou *Instalar o certificado auto-assinado ou pré-instalado para utilizadores de Windows[®] XP e Windows Server[®] 2003* >> página 14.
- O protocolo IPPS tem de estar activado. A configuração predefinida é Activado. Pode alterar as definições do protocolo IPPS e o certificado a utilizar no ecrã da Gestão baseada na Web clicando em **Network** (Rede), **Protocol** (Protocolo) e **HTTP Server Settings** (Definições do servidor HTTP).

Windows[®] XP e Windows Server[®] 2003

- 1 Clique em **Iniciar** e seleccione **Impressoras e faxes**.
- 2 Clique em **Adicionar uma impressora** para abrir o **Assistente para adicionar impressoras**.
- 3 Clique em **Seguinte** quando aparecer o ecrã **Bem-vindo ao 'Assistente para adicionar impressoras'**.
- 4 Seleccione **Uma impressora de rede ou uma impressora ligada a outro computador**.
- 5 Clique em **Seguinte**.
- 6 Seleccione **Ligar a uma impressora na Internet ou numa rede empresarial ou doméstica** e introduza o seguinte no campo do URL:
"https://endereço IP do equipamento/ipp" (em que "endereço IP do equipamento" corresponde ao endereço IP do equipamento ou ao nome do nó).



Nota

- É importante que utilize “https://” e não “http://” - caso contrário, a impressão sobre IPP não será segura.
- Se tiver editado o ficheiro hosts no seu computador ou estiver a utilizar um DNS (Domain Name System), também pode introduzir o nome DNS do servidor de impressão. Dado que o servidor de impressão suporta TCP/IP e nomes NetBIOS, também pode introduzir o nome NetBIOS do servidor de impressão. Pode ver o nome NetBIOS no relatório de configurações de rede. (Para saber como imprimir o Relatório da Configuração de Rede, consulte *Imprimir a Página de Definições da Impressora (para o modelo HL-5450DN(T))* >> página 29 ou *Imprimir o Relatório da Configuração de Rede (em outros modelos)* >> página 29.) O nome NetBIOS atribuído é composto pelos primeiros 15 caracteres no nome do nó e aparece, por predefinição, como “BRNxxxxxxxxxxxx” numa rede com fios ou “BRWxxxxxxxxxxxx” numa rede sem fios. (“xxxxxxxxxxxx” é o endereço MAC/endereço Ethernet da máquina.)

- 7 Quando clicar em **Seguinte**, o Windows® XP e o Windows Server® 2003 estabelecem uma ligação ao URL que especificou.
- Se o controlador da impressora já estiver instalado:
Verá o ecrã de selecção de impressora no **Assistente para adicionar impressoras**.
Vá para o passo 11.
 - Se o controlador da impressora NÃO estiver instalado:
Uma das vantagens do protocolo de impressão IPP é o facto de ele determinar o nome do modelo de impressora quando comunica com ela. Após uma comunicação com sucesso, o nome do modelo da impressora aparecerá automaticamente. Isto significa que não é necessário dizer ao Windows® XP e ao Windows Server® 2003 qual é o tipo de controlador da impressora que deverá ser utilizado.
Vá para o passo 8.



Nota

Se o controlador da impressora que pretende instalar não tiver um Certificado Digital, verá uma mensagem de aviso. Clique em **Continuar na mesma** para continuar a instalação.

- 8 Clique em **Disco**. De seguida, ser-lhe-á pedido que introduza o disco do controlador.
- 9 Clique em **Procurar** e seleccione o controlador da impressora Brother correcto, que se encontra no CD-ROM ou partilha de rede.
Clique em **OK**.
- 10 Clique em **OK**.
- 11 Seleccione a máquina e clique em **OK**.
- 12 Marque **Sim** se pretender utilizar este equipamento como impressora predefinida. Clique em **Seguinte**.
- 13 Clique em **Concluir** e o equipamento fica configurado e pronto para imprimir. Para testar a ligação à impressora, imprima uma página de teste.

Windows Vista[®], Windows[®] 7 e Windows Server[®] 2008

- 1 (Windows Vista[®])
Clique no botão , **Painel de controlo, Hardware e Som** e depois em **Impressoras**.
(Windows[®] 7)
Clique em  e, em seguida, clique em **Dispositivos e Impressoras**.
(Windows Server[®] 2008)
Clique em **Iniciar, Painel de controlo, Hardware e Som** e depois em **Impressoras**.
- 2 Clique em **Adicionar uma impressora**.
- 3 Seleccione **Adicionar uma impressora da rede, sem fios ou Bluetooth**.
- 4 Clique em **A impressora que pretendo não se encontra listada**.
- 5 Seleccione **Seleccionar uma impressora partilhada pelo nome** e introduza o seguinte no campo do URL: "https://endereço IP do equipamento/ipp" (em que "endereço IP do equipamento" corresponde ao endereço IP do equipamento ou ao nome do nó).

Nota

- É importante que utilize "https://" e não "http://" - caso contrário, a impressão sobre IPP não será segura.
- Se tiver editado o ficheiro hosts no seu computador ou estiver a utilizar um DNS (Domain Name System), também pode introduzir o nome DNS do servidor de impressão. Dado que o servidor de impressão suporta TCP/IP e nomes NetBIOS, também pode introduzir o nome NetBIOS do servidor de impressão. Pode ver o nome NetBIOS no relatório de configurações de rede. (Para saber como imprimir o Relatório da Configuração de Rede, consulte *Imprimir a Página de Definições da Impressora (para o modelo HL-5450DN(T))* >> página 29 ou *Imprimir o Relatório da Configuração de Rede (em outros modelos)* >> página 29.) O nome NetBIOS atribuído é composto pelos primeiros 15 caracteres no nome do nó e aparece, por predefinição, como "BRNxxxxxxxxxxxx" numa rede com fios ou "BRWxxxxxxxxxxxx" numa rede sem fios. ("xxxxxxxxxxxx" é o endereço MAC/endereço Ethernet da máquina.)

- 6 Quando clicar em **Seguinte**, o Windows Vista[®] e o Windows Server[®] 2008 estabelecem uma ligação ao URL que especificou.
 - Se o controlador da impressora já estiver instalado:
Verá o ecrã de selecção de impressora no Assistente para adicionar impressoras. Clique em **OK**.
Se já tiver um controlador da impressora apropriado instalado no computador, o Windows Vista[®] e o Windows Server[®] 2008 utilizam automaticamente esse controlador. Neste caso, ser-lhe-á simplesmente perguntado se deseja que o controlador seja a impressora predefinida e o Assistente de instalação do controlador termina. Neste momento, já pode imprimir.
Vá para o passo 11.

- Se o controlador da impressora **NÃO** estiver instalado:

Uma das vantagens do protocolo de impressão IPP é o facto de ele determinar o nome do modelo de impressora quando comunica com ela. Após uma comunicação com sucesso, o nome do modelo da impressora aparecerá automaticamente. Isto significa que não é necessário dizer ao Windows Vista® e ao Windows Server® 2008 qual é o tipo de controlador da impressora que deverá ser utilizado.

Vá para o passo 7.

- 7 Se o seu equipamento não aparecer na lista de impressoras suportadas, clique em **Disco**. De seguida, ser-lhe-á pedido que introduza o disco do controlador.
- 8 Clique em **Procurar** e seleccione o controlador da impressora Brother correcto, que se encontra no CD-ROM ou partilha de rede. Clique em **Abrir**.
- 9 Clique em **OK**.
- 10 Especifique o nome do modelo do equipamento. Clique em **OK**.



Nota

- Quando aparecer a caixa de diálogo do Controlo de Conta de Utilizador, clique em **Continuar**.
 - Se o controlador da impressora que pretende instalar não tiver um Certificado Digital, verá uma mensagem de aviso. Clique em **Instalar este software de controlador mesmo assim** para continuar a instalação. O **Assistente para adicionar impressoras** termina em seguida.
- 11 Verá o ecrã **Escrever um nome de impressora** no assistente **Adicionar Impressora**. Marque a caixa de verificação **Predefinir impressora** se pretender utilizar este equipamento como impressora predefinida e clique em **Seguinte**.
 - 12 Para testar a ligação à impressora, clique em **Imprimir uma página de teste** e depois em **Concluir**. O equipamento está agora configurado e pronto para imprimir.

Configuração utilizando a gestão baseada na web (browser web)

Pode configurar o envio de e-mail seguro com a autenticação de utilizadores ou o envio e a recepção (nos modelos DCP e MFC) de e-mail utilizando SSL/TLS no ecrã da Gestão baseada na web.

- 1 Abra o seu web browser.
- 2 Escreva “http://endereço IP do equipamento/” no browser (em que “endereço IP do equipamento” corresponde ao endereço IP do equipamento).
 - Por exemplo:
http://192.168.1.2/
- 3 Por predefinição, não é necessária nenhuma palavra-passe. Introduza uma palavra-passe, se tiver definido uma, e prima .
- 4 Clique em **Network** (Rede).
- 5 Clique em **Protocol** (Protocolo).
- 6 Clique em **Advanced Setting** (Definição avançada) de **POP3/SMTP** e certifique-se de que o estado de **POP3/SMTP** é **Enabled** (Activar).
- 7 Pode configurar as definições de **POP3/SMTP** nesta página.



Nota

- Para obter mais informações, consulte a ajuda da gestão baseada na web.
 - Após a configuração, também pode confirmar se as definições de e-mail estão correctas enviando um e-mail de teste.
 - Se não souber as definições do servidor POP3/SMTP, contacte o administrador de sistema ou o fornecedor de serviços de Internet (ISP) para mais informações.
-
- 8 Após a configuração, clique em **Submit** (Submeter). Aparece o ecrã **Test E-mail Send Configuration** (Testar a configuração de envio de e-mail) ou **Test E-mail Send/Receive Configuration** (Testar a configuração de envio/recepção de e-mail).
 - 9 Siga as instruções apresentadas no ecrã se quiser testar as definições actuais.

Enviar ou receber (nos modelos DCP e MFC) um e-mail com segurança utilizando SSL/TLS

Este equipamento suporta os métodos SSL/TLS para enviar ou receber (nos modelos DCP e MFC) um e-mail através de um servidor de e-mail que exija uma comunicação SSL/TLS segura. Para enviar ou receber e-mail através de um servidor de e-mail que utilize a comunicação SSL/TLS, tem de configurar correctamente SMTP sobre SSL/TLS ou POP3 sobre SSL/TLS.

Verificar certificado de servidor

- Se seleccionar SSL ou TLS para **SMTP over SSL/TLS** (SMTP sobre SSL/TLS) ou **POP3 over SSL/TLS** (POP3 sobre SSL/TLS), a caixa **Verify Server Certificate** (Verificar certificado do servidor) irá ficar automaticamente seleccionada para verificar o Certificado do Servidor.
 - Antes de verificar o Certificado do Servidor, tem de importar o certificado CA emitido pela autoridade de certificados que assinou o Certificado do Servidor. Contacte o administrador da rede ou o ISP (fornecedor de serviços de Internet) para saber se é necessário importar um certificado CA. Para importar o certificado, consulte *Importar e exportar um certificado CA* >> página 18.
 - Se não necessitar de verificar o Certificado do Servidor, desactive **Verify Server Certificate** (Verificar certificado do servidor).

Número da porta

- Se seleccionar SSL ou TLS, o valor de **SMTP Port** (Porta SMTP) ou **POP3 Port** (Porta POP3) será alterado para corresponder ao protocolo. Se pretender alterar manualmente o número da porta, introduza o número da porta depois de seleccionar **SMTP over SSL/TLS** (SMTP sobre SSL/TLS) ou **POP3 over SSL/TLS** (POP3 sobre SSL/TLS).
- Tem de configurar o método de comunicação POP3/SMTP para corresponder ao servidor de E-mail. Para obter mais informações sobre as definições do servidor de E-mail, contacte o administrador de rede ou o fornecedor de serviços de Internet (ISP). Na maioria dos casos, os serviços de webmail seguros necessitam das seguintes definições:
 - **SMTP**
 - **Porta SMTP:** 587
 - **Método de autenticação de servidor SMTP:** SMTP-AUTH
 - **SMTP over SSL/TLS:** TLS
 - **POP3**
 - **Porta POP3:** 995
 - **POP3 over SSL/TLS:** SSL

Descrição geral

Este capítulo explica como resolver problemas de rede típicos com que poderá deparar-se ao utilizar o equipamento Brother. Se, após a leitura deste capítulo, não conseguir resolver o seu problema, visite o Brother Solutions Center em: (<http://solutions.brother.com/>).

Visite o Brother Solutions Center em (<http://solutions.brother.com/>) e clique em Manuais na página do modelo para transferir os outros manuais.

Identificar o problema

Antes de ler este capítulo, certifique-se de que os itens que se seguem estão configurados.

Verifique o seguinte:
O cabo de alimentação está devidamente ligado e a máquina Brother está ligada.
Os materiais de protecção foram todos retirados da máquina.
Os cartuchos de toner e a unidade do tambor estão instalados correctamente.
As tampas frontal e traseira estão totalmente fechadas.
O papel está introduzido correctamente na gaveta.
O equipamento está ligado correctamente à rede.

Aceda à página que contém a solução a partir das listas que se seguem

- Não consigo imprimir o documento pela Internet com IPPS.
Consulte *Não consigo imprimir o documento pela Internet com IPPS.* >> página 28.
- Quero verificar se os meus dispositivos de rede estão a funcionar correctamente.
Consulte *Quero verificar se os meus dispositivos de rede estão a funcionar correctamente.* >> página 28.

Não consigo imprimir o documento pela Internet com IPPS.

Questão	Solução
Não consigo comunicar com o meu equipamento Brother utilizando SSL.	<ul style="list-style-type: none"> ■ Obtenha um certificado válido e volte a instalá-lo no equipamento e no computador. ■ Certifique-se que a configuração da porta no equipamento está correcta. Pode confirmar a configuração da porta do equipamento no ecrã da Gestão baseada na web clicando em Network (Rede), Protocol (Protocolo) e HTTP Server Settings (Definições do servidor HTTP).

Quero verificar se os meus dispositivos de rede estão a funcionar correctamente.

Questão	Solução
O seu equipamento Brother está ligado?	Certifique-se de que confirmou todos os pontos de <i>Verifique o seguinte</i> : >> página 27.
Onde posso encontrar as minhas definições de rede do equipamento Brother, como o endereço IP?	Imprima o relatório de configurações de rede. Consulte <i>Imprimir a Página de Definições da Impressora (para o modelo HL-5450DN(T))</i> >> página 29 ou <i>Imprimir o Relatório da Configuração de Rede (em outros modelos)</i> >> página 29.

Imprimir a Página de Definições da Impressora (para o modelo HL-5450DN(T))



Nota

Nome do nó: o nome do nó aparece no relatório de configurações de rede. A predefinição do nome de nó é "BRNxxxxxxxxxxxx". ("xxxxxxxxxxxx" é o endereço MAC/endereço Ethernet da máquina.)

A Página de Definições da Impressora é um relatório que lista todas as definições actuais da impressora, incluindo as configurações do servidor de impressão de rede.

Pode imprimir a Página de Definições da Impressora utilizando o botão **Go** do equipamento.

- 1 Certifique-se de que a tampa dianteira está fechada e que o cabo de alimentação está ligado.
- 2 Ligue o equipamento e aguarde que fique no estado Pronto.
- 3 Prima **Go** três vezes no espaço de 2 segundos. O equipamento imprime o Página de Definições da Impressora actual.

Imprimir o Relatório da Configuração de Rede (em outros modelos)



Nota

Nome do nó: o nome do nó aparece no relatório de configurações de rede. O nome de nó predefinido é "BRNxxxxxxxxxxxx" para uma rede com fios ou "BRWxxxxxxxxxxxx" para uma rede sem fios. ("xxxxxxxxxxxx" é o endereço MAC/endereço Ethernet da máquina.)

O relatório de configurações de rede imprime uma lista de todas as configurações actuais da rede, incluindo as definições do servidor de impressão de rede.

Para HL-5470DW(T) e HL-6180DW(T)

- 1 Prima **▲** ou **▼** para seleccionar `Info.` aparelho.
Prima **OK**.
- 2 Prima **▲** ou **▼** para seleccionar `Imprimir DefRede`.
Prima **OK**.

Para DCP-8110DN, DCP-8150DN, DCP-8155DN, MFC-8510DN, MFC-8710DW e MFC-8910DW

- 1 Prima **Menu**.
- 2 (Modelos MFC) Prima ▲ ou ▼ para seleccionar **Impr. relat.**
(Modelos DCP) Prima ▲ ou ▼ para seleccionar **Info. aparelho.**
Prima **OK**.
- 3 Prima ▲ ou ▼ para seleccionar **Config de Rede.**
Prima **OK**.
- 4 Prima **Iniciar**.

Para DCP-8250DN e MFC-8950DW(T)

- 1 Prima **Menu**.
- 2 Prima ▲ ou ▼ para ver **Impr. relat e**, em seguida, prima **Impr. relat.**
- 3 Prima **Config de Rede**.
- 4 Prima **Iniciar**.



Nota

Se o **IP Address** aparecer no relatório de configurações da rede como **0.0.0.0**, aguarde um minuto e tente novamente.

Termos e conceitos de redes

Descrição técnica do SSL

O SSL (Secure Socket Layer) é um método para proteger dados na camada de transporte transmitidos numa rede local ou não local através do protocolo IPP (Internet Printing Protocol), para evitar que possam ser lidos por utilizadores não autorizados.

Isto é conseguido através da utilização de protocolos de autenticação na forma de chaves digitais, das quais existem 2 tipos:

- Chave pública – conhecida por todos os que imprimem.
- Chave privada – conhecida apenas pelo equipamento que faz a descriptação dos pacotes e os torna de novo legíveis pelo equipamento.

A chave pública utiliza encriptação de 1.024 ou 2.048 bits e encontra-se dentro de um certificado digital. Estes certificados podem ser auto-assinados ou aprovados por uma Autoridade de Certificados (CA).

Para começar, existem três chaves diferentes: Privada, Pública e Partilhada.

A chave Privada, conhecida apenas pelo equipamento, está associada à chave Pública mas não se encontra no certificado digital dos clientes (remetentes). Quando o utilizador estabelece a ligação pela primeira vez, o equipamento envia a chave Pública com o certificado. O PC cliente confia que a chave Pública provém do equipamento com o certificado. O cliente gera a chave Partilhada, codifica-a com a chave Pública e envia-a para o equipamento. O equipamento codifica a chave Partilhada com a chave Privada. Agora, o equipamento e o cliente partilham a chave Partilhada com segurança e estabelecem uma ligação segura para transferência de dados de impressão.

Os dados de impressão são codificados e decodificados com a chave Partilhada.

O SSL não impede o acesso aos pacotes por parte de utilizadores não autorizados, mas torna-os ilegíveis sem a chave Privada, que só é conhecida pelo equipamento.

Pode ser configurado tanto em redes com fios como em redes sem fios e funciona em conjunto com outros métodos de segurança, como as chaves WPA e as firewalls, mediante configuração adequada.

Termos de redes

■ SSL (Secure Socket Layer)

Protocolo de comunicação de segurança que encripta dados para impedir ameaças à segurança.

■ IPP (Internet Printing Protocol)

O IPP é um protocolo de impressão standard que é utilizado para gerir e administrar trabalhos de impressão. Pode ser utilizado localmente e também a nível global, permitindo que uma pessoa possa imprimir no mesmo equipamento a partir de qualquer sítio do mundo.

■ IPPS

A versão do protocolo de impressão Internet Printing Protocol (IPP Versão 1.0) que utiliza o SSL.

■ HTTPS

A versão do protocolo da Internet HTTP (Hyper Text Transfer Protocol) que utiliza o SSL.

■ CA (Certificate Authority - Autoridade de Certificados)

Uma CA é uma entidade que emite certificados digitais (sobretudo certificados X.509) e que atesta a ligação entre os itens de dados num certificado.

■ CSR (Certificate Signing Request - Pedido de Assinatura de Certificado)

Um CSR é uma mensagem enviada por um requerente para uma CA para pedir a emissão de um certificado. O CSR contém informações que identificam o requerente, a chave pública criada pelo requerente e a assinatura digital do requerente.

■ Certificado

Um certificado é a informação que junta uma chave pública e uma identidade. O certificado pode ser utilizado para verificar se uma chave pública pertence a um indivíduo. O formato é definido pelo padrão x.509.

■ Criptosistema de chave pública

Um criptosistema de chave pública é um subdomínio moderno da criptografia no qual os algoritmos utilizam um par de chaves (uma chave pública e uma chave privada) e utilizam um componente diferente do par para diferentes passos do algoritmo.

■ Criptosistema de chave partilhada

Um criptosistema de chave partilhada é um subdomínio da criptografia que lida com algoritmos que utilizam a mesma chave para dois passos diferentes do algoritmo (como encriptação e desencriptação).